UNIVERSIDADE FEDERAL DE SERGIPE
CENTRO DE CIÊNCIAS SOCIAIS APLICADAS
DEPARTAMENTO DE RELAÇÕES INTERNACIONAIS

ELIS REGINA DE OLIVEIRA MARTINS

O SISTEMA DE INTELIGÊNCIA BRASILEIRO NO CONTEXTO DO VAZAMENTO DE DADOS OCORRIDO DURANTE O MANDATO PRESIDENCIAL DE DILMA ROUSSEFF NO PERÍODO ENTRE 2013-2015

São Cristóvão/SE
2025

ELIS REGINA DE OLIVEIRA MARTINS

O SISTEMA DE INTELIGÊNCIA BRASILEIRO NO CONTEXTO DO VAZAMENTO DE DADOS OCORRIDO DURANTE O MANDATO PRESIDENCIAL DE DILMA ROUSSEFF NO PERÍODO ENTRE 2013-2015

Trabalho de Conclusão Curso II apresentado ao Departamento de Relações Internacionais como requisito para obtenção do título de Bacharel em Relações Internacionais.

Orientadora: Profa. Dra. Bárbara Vasconcellos de Carvalho Motta.

São Cristóvão/SE

2025

TERMO DE APROVAÇÃO

ELIS REGINA DE OLIVEIRA MARTINS

O SISTEMA DE INTELIGÊNCIA BRASILEIRO NO CONTEXTO DO VAZAMENTO DE DADOS OCORRIDO DURANTE O MANDATO PRESIDENCIAL DE DILMA ROUSSEFF NO PERÍODO ENTRE 2013-2015

Trabalho de Conclusão Curso II apresentado ao Departamento de Relações Internacionais como requisito para obtenção do título de Bacharel em Relações Internacionais.

Orientadora: Profa. Dra. Bárbara Vasconcellos de Carvalho Motta.

BANCA EXAMINADORA

Professora Dra. Bárbara Vasconcellos de Carvalho Motta

Orientadora - Universidade Federal de Sergipe

Professor Dr. Rodrigo Barros de Albuquerque

Examinador Interno - Universidade Federal de Sergipe

Professor Dr. David Paulo Succi Junior

Examinador Externo - Instituto de Políticas Públicas e Relações Internacionais

Nota: _____

São Cristóvão, ___ de _____ 2025.

“Agulha no palheiro”

(Glenn Greenwald, 2013)

AGRADECIMENTOS

Agradeço primeiramente a Deus, pelo dom da vida e por permitir eu chegar aonde cheguei. Sem Deus não sou absolutamente nada e foi por meio do seu amor, que ao enviar Jesus, eu pudesse ter uma esperança verdadeira e sentido de vida.

Graças à confiança e suporte total da minha família, eu estou finalizando com êxito esse capítulo da minha vida. Papai Sérgio, mamãe Elaine e irmã Elisama, obrigada do fundo do meu ser pelo amor, carinho, suporte, ensinamentos, conselhos, palavras de incentivo e também às vezes, puxão de orelha. Tudo o que fizeram, contribuiu para que eu pudesse atingir mais esse alvo.

Ao amor da minha vida, anjo e Dragão Guerreiro Gabriel, o qual também está nessa jornada de término de TCC, obrigada por ser quem é, pelas sábias palavras, pelo companheirismo e por podermos dividir juntos as lamúrias do TCC um com o outro, fazendo jus o que diz em Gálatas no capítulo 6, "levai as cargas uns dos outros… ". Sem você, essa jornada teria sido mais árdua. Como sempre lhe disse, estamos mais perto do final dessa fase do que do começo. Gratidão do fundo do meu coração por tudo!

Aos caros amigos, demais familiares e conhecidos, obrigada a todos por não desistirem de mim e estarem comigo, cada qual de maneira única e especial, nesse percurso.

Agradeço a todos os professores, profissionais e colegas do curso, que cada qual a sua maneira, contribuíram para o meu crescimento acadêmico, desenvolvimento profissional e pessoal. A CORI, pela qual tive o privilégio de poder participar e me envolver, desde praticamente o início até o término da graduação, obrigada pelas experiências e amizades. À Reina, melhor empresa júnior do Brasil, a qual tive a honra de poder fazer parte e contribuir de alguma forma a sua trajetória, bem como à do Reinaldo, com seus queridos e maravilhosos membros, obrigada por tudo.

Agradeço à minha orientadora, a professora Dra. Bárbara Motta, por não desistir de mim e ter me auxiliado com muita paciência, durante todo o processo de elaboração do TCC. Desejo sucesso e muitas conquistas à sua história de vida.

Enfim, aqui chegamos! Espero que a minha passagem no curso de RI na UFS tenha sido de alguma forma contribuinte. De qualquer modo, não me vejo onde estou sem por aqui ter trilhado.

Ao departamento de Relações Internacionais e à UFS, "*fluendo crescit*".

RESUMO

Este trabalho busca compreender o papel da inteligência brasileira no âmbito nacional e internacional. Para tanto, um dos casos mais notáveis em que o Brasil esteve no centro de tal debate - o caso do vazamento de dados ainda nos anos do governo da presidente Dilma Rousseff, principalmente o primeiro de 2013- vai ser utilizado para exemplificar o quanto e como o papel efetivo (ou não), sobretudo do Sistema Brasileiro de Inteligência (SISBIN) por meio da Agência Brasileira de Inteligência (ABIN), contribuiu para refletir as vulnerabilidades, desafios e possíveis aprendizados desse notável episódio na Segurança do Sistema de Inteligência do governo brasileiro. Outrossim, será posto em pauta também os mecanismos de resposta e defesa do Estado brasileiro diante de tal conjuntura. Para tanto, esta pesquisa contará com as contribuições de bibliografia especializada no campo da inteligência para melhor elucidar tal dilema. Logo, alguns conceitos como vazamento de dados, espionagem, segurança, Sisbin, governo brasileiro, Abin, contrainteligência, segurança cibernética, entre outros, serão apresentados e debatidos ao decorrer desse estudo. Ao final, se apresentará os resultados obtidos, com possíveis conjecturas à temática abordada.

Palavras-chave: Inteligência; Vazamento de dados; Contrainteligência; Governo brasileiro; Segurança cibernética.

ABSTRACT

This paper seeks to understand the role of Brazilian intelligence at both national and international levels. To this end, one of the most remarkable cases in which Brazil was at the center of such a debate—the data leak case during the years of President Dilma Rousseff's administration, mainly the first from 2013—will be used to exemplify how and to what extent the effective role (or lack thereof) of the Brazilian Intelligence System (SISBIN), through the Brazilian Intelligence Agency (ABIN), contributed to reflecting on the vulnerabilities, challenges, and possible lessons from this notable episode in the security of the Brazilian government's intelligence system. Furthermore, the Brazilian State response and defense mechanisms in the face of such a situation will also be put on the agenda. Therefore, this research will draw on specialized bibliography in the field of intelligence to better elucidate this dilemma. Consequently, some concepts such as data leak, espionage, security, Sisbin, Brazilian government, Abin, counterintelligence, cyber security among others, will be presented and discussed throughout this study. In the end, the results obtained will be presented with possible conjectures on the topic addressed.

Keywords: Intelligence; Data Leak; Counterintelligence; Brazilian Government; Cyber Security.

LISTA DE ILUSTRAÇÕES

LISTA DE ABREVIATURAS E SIGLAS

ABIN	Agência Brasileira de Inteligência
AI	*Artificial Intelligence*
AI - 5	Ato Institucional nº 5
BBC	*British Broadcast Corporation*
CCAI	Comissão de Controle da Atividade de Inteligência
CDN	Conselho de Defesa Nacional
Cepesc	Centro de Pesquisa e Desenvolvimento para Segurança das Comunicações
CFI	Centro Federal de Inteligência
CGU	Controladoria Geral da União
CIA	*Central Intelligence Agency*
CISET-PR	Controle Interno da Presidência da República
DESPS	Delegacia Especial de Segurança Pública e Social
DFSP	Departamento Federal de Segurança Pública
DHS	*Department of Homeland Security*
DOI-CODIs	Centros de Operações de Defesa Interna e Destacamentos de Operações Internas
ESG	Escola Superior de Guerra
EsNI	Escola Nacional de Informações
EUA	Estados Unidos da América
FHC	Fernando Henrique Cardoso
GSI	Gabinete Institucional de Segurança

HUMINT	*Human Intelligence*
IA	Inteligência Artificial
IC	Infraestruturas Críticas
IMINT	*Imagery Intelligence*
ITU	*International Communications Union*
JCI	Junta Coordenadora de Informações
LGPD	Lei Geral de Proteção de Dados
MASINT	*Measurement and Signature Intelligence*
NSA	*National Security Agency*
OCDE	Organização para a Cooperação e Desenvolvimento Econômico
OIGs	Organizações Intergovernamentais
ONGs	Organizações Não Governamentais
OSINT	*Open Source Intelligence*
OTAN	Organização do Tratado do Atlântico Norte
PNI	Política Nacional de Inteligência
PNPC	Programa Nacional de Proteção do Conhecimento Sensível
PRISM	*Planning Tool for Resource Integration, Synchronization, and Management*
RBI	Revista Brasileira de Inteligência
RI	Relações Internacionais
SAE	Secretaria de Assuntos Estratégicos
SADEN	Secretaria de Assuntos de Defesa Nacional

SFICI	Serviço Federal de Informações e Contrainformações
SG-CSN	Secretaria Geral do Conselho de Segurança Nacional
SI	Serviços de Inteligência
SIC	Segurança da Informação e Comunicações
SIGINT	*Signals Intelligence*
SNI	Serviço Nacional de Informações
SISBIN	Sistema Brasileiro de Inteligência
SISNI	Sistema Nacional de Informações
SISSEGIN	Sistema de Segurança Interna
SSI	Departamento de Inteligência em Subsecretaria de Inteligência
TICs	Tecnologias da Informação e Comunicação

SUMÁRIO

1 INTRODUÇÃO

A delação de Edward Snowden em 2013, um dos ex-agentes da *National Security Agency (NSA)* e da *Central Intelligence Agency (CIA)*, acerca das atividades que os EUA vinham operando em estadunidenses, Estados não aliados e também aliados, chocou o mundo na época gerando uma trama de consequências, ações, represálias, decisões e impactos no sistema internacional. Esse dilema se insere no escopo principal deste trabalho, a saber o caso do vazamento de dados, visto que o Brasil foi um dos alvos nessa espionagem, que ficou conhecida como espionagem industrial/comercial/cibernética. Ao implementar essa atividade, os EUA recorreram à maior rede de comunicação mundial, a Internet, para acessar informações privadas e de interesse de outros Estados. Essa ação resultou na violação da privacidade de atores estatais e na exposição de infraestruturas críticas governamentais de diversos países - aliados e não aliados - com destaque para o Brasil.

O presente trabalho, cuja pergunta de pesquisa é "Como o Sistema de Segurança de Inteligência Brasileiro lidou com o dilema do vazamento de dados durante o mandato da Presidente Dilma Rousseff no período entre 2013-2015?", busca analisar e compreender melhor a atuação do sistema de inteligência brasileiro, dentro da perspectiva do caso em questão. Para tanto, uma análise voltada para compreender alguns conceitos principais, como Segurança e Inteligência e em seguida Segurança da Inteligência, serão melhor observados, usando-se as suas três teorias basilares de Relações Internacionais (RI) a saber, o realismo, liberalismo e construtivismo, para enxergar como a Segurança é concebida, e somente então meditar com Pontes (2015), como o caso pode ser analisado a partir de uma concepção em que aceita um misto dessas três vertentes. Dessa forma, a segurança envolvendo o vazamento de dados, dentro da perspectiva brasileira, tende a estar atrelada ao grupo dos "ampliadores", devido ao fato desse grupo conceber a segurança como algo que vai além da visão mais tradicionalista, ou seja, que envolve diversos atores, para além dos militares, como Estados, empresas, organizações, indivíduos entre outros.

No primeiro capítulo, ao conceituar a Segurança, se faz necessário entender outro conceito de suma importância para este trabalho de forma geral, a Inteligência. A inteligência, voltada para a perspectiva desse trabalho, tem um caráter mais relacionado às "atividades fundamentais de qualquer Estado (...), e é a partir de dados de Inteligência que o Estado planeja e executa políticas públicas de defesa nacional,

segurança pública e relações exteriores" (Ivanissevic, 2013, p. 6). Ademais, conforme será historicamente explicado, dentro da literatura brasileira, esse conceito no século XX ganhou outro nome, informação, e só tornou-se "inteligência" de fato, dado o término da ditadura. Após compreender melhor esses conceitos separadamente, a critério do princípio da especificidade, os dois -segurança e inteligência- são aproximados, e após isso, adquirem um novo sentido, se tornando a "segurança da inteligência" ou "*Security Intelligence*", a qual consoante Marco Aurélio Cepik (2003, p. 249), adquirem papéis simétricos e dependem entre si.

Nesse sentido, se faz necessário analisar esta temática sob a lente da Segurança Internacional com o intuito de melhor observar como o Brasil se comportou diante de tal vulnerabilidade e a maneira através da qual reagiu posteriormente tanto para dirimir o desconforto internacional levantado, quanto para melhorar seu aparato de segurança em matéria de inteligência. Logo, este trabalho tem por premissa buscar utilizar contribuições de diversos autores de dentro e fora do campo das Relações Internacionais, em particular voltados para a Segurança, para melhor compreender o papel da inteligência e seus impactos na atuação nacional e internacional brasileira.

Ainda em relação aos conceitos supracitados e ao escopo deste trabalho, outros conceitos essenciais, que serão também abordados são a contrainteligência e a segurança cibernética. A contrainteligência é, segundo a Agência Brasileira de Inteligência (ABIN), a operação que tem o intuito de assegurar a segurança nacional, agindo através da detecção, prevenção, neutralização, capacitação, sensibilização, orientação e obstrução de Inteligência ou espionagem incondizente com o governo brasileiro (Brasil, 2020d). Dessa forma, ela está presente em diversas instituições governamentais e se configura como a área responsável por dirimir as vulnerabilidades e ameaças possíveis. Outrossim, parte da literatura brasileira compreende a contrainteligência com duas frentes, tendo a parte da segurança orgânica, voltada para a cibersegurança e a segurança ativa, voltada para a contraespionagem (Baptistella e Vianna, 2022).

Entre os espaços existentes, o espaço cibernético, também chamado ciberespaço, abarca o mundo das máquinas computacionais e o fenômeno que se aprimorou com a globalização, a saber, a *internet*. A segurança cibernética, por sua vez, está concomitantemente atrelada ao surgimento, aprimoramento e alcance das chamadas novas Tecnologias da Informação e Comunicação (TICs), ou seja, tudo que for de caráter comunicacional e tecnológico ou científico, são TICs. Dentre os exemplos,

cita-se a economia, a medicina, o comércio eletrônico, o próprio desenvolvimento científico e tecnológico dos equipamentos, e principalmente, a *internet*, o ponto de base para as TICs. Particularmente no Brasil, entende-se segurança cibernética como o meio de garantir o funcionamento da sociedade da informação de um dado Estado, com suas respectivas infraestruturas críticas (como energia, transporte, defesa, saúde, telecomunicações *etc*) dentro do espaço cibernético (Mandarino, 2009, p. 25-29). Ademais, vale ressaltar que a institucionalização do Marco Civil da *Internet* só se deu por volta de 2013, graças ao incentivo, conforme será melhor elucidado posteriormente, dos fatos do vazamento de dados.

Nessa feita, no segundo capítulo, busca-se primariamente entender do ponto de vista histórico como se deu a formação do Sistema de Inteligência Brasileiro para posteriormente melhor compreender como é a atuação dessa atividade nos moldes nacionais. Os acontecimentos que abalaram o mundo, como a I Guerra Mundial (1914-1918), II Guerra Mundial (1939-1945) e posteriormente a Guerra Fria (1945-1991), causaram impactos marcantes em diversas frentes no mundo todo. Um desses impactos contribuiu para a formação da atividade de inteligência do Brasil, como uma forma do país se posicionar frente às transformações internacionais. Nessa feita, o Brasil deu seus primeiros passos da atividade de inteligência, com a Inspetoria de Investigação e Segurança Pública, com funcionamento inicial datado ainda em 1920. Ao longo do século XX e início do século XXI, com as transformações externas e internas, o Brasil passou por diversas alterações no que diz respeito à configuração da atividade de Inteligência. Contudo, chegou finalmente ao que prevalece até os dias atuais, no Sistema Brasileiro de Inteligência (SISBIN), tendo a Agência Brasileira de Inteligência (ABIN) como seu órgão central (Brandão e Quadrat, 2024).

Uma das observações mais interessantes nesse período de consolidação do sistema de Inteligência no âmbito nacional diz respeito à própria terminologia[1] do que se conhece hoje como inteligência, pois antes da ditadura tal atividade ganhou a terminologia de “informação”. Como forma de dissociar as atividades “de inteligência” praticadas nesse período sombrio da história, foi que, pouco tempo após o fim da

[1] Diferentemente dos modelos anglo-saxões e de muitos modelos latino-americanos, o Brasil adotou a expressão informações para referir-se ao que a teoria política define como órgãos de inteligência. Esta expressão passa a ser utilizada no país apenas a partir de 1990, quando o desgaste produzido por esses órgãos durante a ditadura militar, em função da violência por eles desenvolvida, faz que adotem o termo inteligência como forma de se deslocarem dessa memória de violência. Dessa maneira, quando estivermos nos referindo a órgãos ou ao sistema responsável pela produção de conhecimento no país no período anterior a 1990, usaremos a expressão informações e, posterior a 1990, inteligência (Brandão e Quadrat, 2024).

ditadura, a atividade em questão passou a ser concebida como “inteligência”, se associando a denominação já comumente usada na maioria dos outros países. Afinal, “inteligência não é apenas segurança nem meramente informação, mas sim a busca e análise de informações necessárias para vencer um conflito entre vontades antagônicas” (Brandão e Cepik, 2003, p. 110).

Em adição a isso, as atividades de inteligência no Brasil enquanto política pública apresentam como premissa o reconhecimento que as ameaças podem causar nas infraestruturas críticas do governo. Logo, fatores como corrupção, terrorismo, ataques cibernéticos, espionagem, ações contrárias a soberania nacional, eventos críticos, entre outros (Aquino, 2024, p. 190), são considerados ameaçadores à segurança das instituições, sociedade e ao próprio Estado. Para além das infraestruturas críticas mencionadas, o governo também reconhece a segurança cibernética com “infraestrutura crítica da informação”, ou seja, desde o fenômeno da *internet*, avanços científicos, computacionais, tecnológicos e o mais recente, *boom* da Inteligência Artificial (IA), têm contribuído para que os ataques cibernéticos estivessem cada vez mais em local de prioridade dentro das agendas dos Estados (Canongia e Mandarino, 2009; Ferreira e Rodrigues, 2024). Assim, é incontestável o quanto a segurança cibernética, adjunto da contrainteligência, se mostram como conceitos fundamentais para a compreensão do caso em voga e principalmente para compreender os seus impactos na sociedade de modo geral.

No terceiro e último capítulo desta monografia se analisa de maneira mais pontual o emblemático caso do vazamento de dados ocorrido entre 2013-2015, durante o mandato presidencial de Dilma Vana Rousseff no Brasil, o qual teve seu epítome com as delações feitas voluntariamente por Snowden em um quarto de hotel, em Hong Kong, em meados de junho de 2013, diante dos repórteres Ewen MacAskill, Glenn Greenwald e da documentarista Laura Poitras. O vídeo divulgado em todos os canais televisivos na época, de denominação “Delator PRISM[2]”, tinha cerca de 12 minutos e, nele, Snowden respondia perguntas feitas por Greenwald enquanto MacAskill escrevia as respostas e Poitras o filmava.

> A história era um duplo constrangimento para a Casa Branca. Primeiro, os EUA haviam reclamado insistentemente de ciberataques invasivos e

[2] Planning Tool for Resource Integration, Synchronization, and Management; airview e PRISM, programas utilizados pelos EUA para espionar dados de usuários do mundo, para ver se há alguma ligação criminosa (particularmente associada ao terrorismo). No entanto, no caso dos EUA, ambos os programas têm respaldo legal no Ato Patriótico. Todavia, há um processo para que haja essa permissibilidade, algo que os EUA estava negligenciando (...). (Spaniol, 2015)

> prejudiciais de Pequim, dirigidos contra a infraestrutura militar norte-americana, o Pentágono e outros alvos. Essas queixas agora pareciam distintamente hipócritas; os EUA estavam fazendo exatamente o mesmo (...) (Harding, 2014, p. 117).

Conforme o desenrolar do caso, ficou claro que,

> Além de colocar escutas nas lideranças democraticamente eleitas do Brasil, a NSA, de forma secreta, havia direcionado sua atenção para a Petrobras, estatal do petróleo e empresa mais importante do país. A Petrobras é uma das trinta maiores empresas do mundo. Majoritariamente controlada pelo Estado, é uma importante fonte de receitas para o governo brasileiro. Está iniciando a exploração de novos, diversos e gigantescos campos de petróleo, na região de alta profundidade no Atlântico, conhecida como "Pré-sal"(Harding, 2014, p. 221).

Consoante isso, o Brasil precisou se posicionar e tomar algumas medidas, visto que tinha sido um dos alvos principais da espionagem estadunidense. Como o caso impactou a privacidade, a soberania e algumas das infraestruturas críticas do país, e acabou por colocar em xeque a relação do Brasil com o país espião, uma das ações mais importantes que o Brasil teve na época foi levar o caso à Organização das Nações Unidas (ONU), em setembro do mesmo ano, e apresentar o marco civil para a governança e uso da *internet*, doravante, Marco Civil da *Internet*, com o objetivo de proteger e preservar todos os usuários dessa rede mundial. Além do mais, o acontecimento em questão contribuiu para que um debate interno fosse levantado acerca do quanto (e se) o Brasil está protegido de ataques similares, fazendo com que diversos atores, órgãos e instituições do governo se pronunciassem, cada qual com uma perspectiva e posição particular.

Há pouco tempo, em um evento da ABIN que ocorreu em junho de 2024, cujo debate foi sobre "A Atividade de Inteligência e o parlamento brasileiro na defesa da soberania nacional", Cepik, enquanto o atual diretor-adjunto da ABIN, em uma das suas falas finais ressaltou que "as universidades e a inteligência precisam produzir conhecimento independente e livre para assessorar adequadamente e construir um país e uma nação soberanos" (Brasil, 2023a). Assim, quanto ao procedimento metodológico, ao retomar a pergunta de pesquisa desta monografia, "Como o Sistema de Segurança de Inteligência Brasileiro lidou com o dilema do vazamento de dados durante o mandato da Presidente Dilma Rousseff no período entre 2013-2015?", reconhece-se a utilização da revisão bibliográfica, análise de conteúdo, pesquisa de natureza qualitativa e cunho bibliográfico para discutir o vazamento de dados, compreender o papel das instituições mais proeminentes em matéria de segurança e de inteligência do Brasil, dentre eles o

próprio SISBIN e a ABIN, e para articular os conceitos mais relevantes, os acontecimentos, principalmente durante e após aos fatos.

Após essas ponderações, evidencia-se que o presente trabalho de conclusão de curso pode contribuir consideravelmente para as Relações Internacionais, visto que utiliza alguns conceitos do campo em questão, pouco explorados em conjunto no curso, ao mesmo tempo que os analisa no escopo deste trabalho inserindo-os dentro das agendas internacionais vigentes, realçando, assim, o papel e contribuições desta ciência na sociedade atual.

2 INTELIGÊNCIA E SEGURANÇA DA INTELIGÊNCIA

O campo das Relações Internacionais aborda um conjunto de teorias, temas e assuntos dentre os quais em sua maioria estão voltados para discutir os acontecimentos e dinâmicas dentro da esfera global. Uma das áreas centrais desse campo é a segurança internacional, um ramo na qual as três teorias basilares das Relações Internacionais contemporâneas como um todo, a saber, Realismo, Liberalismo e Construtivismo, possuem perspectivas diversas entre si. Portanto, faz-se necessário para o escopo deste presente trabalho, compreender a priori esse conceito da segurança tão fundamental dentro da própria Relações Internacionais para posteriormente inseri-lo mais objetivamente ao caso estudado. De antemão, em um olhar mais amplo, dentre as várias possíveis compreensões acerca da segurança, esse conceito dentro da perspectiva das Relações Internacionais, está relacionado "à segurança dos estados, de seus cidadãos e à sua própria vivência" (Pontes, 2015, p. 9).

Todavia, vale ressaltar que há diversas formas de conceber e compreender a segurança, dado a sua dimensão e natureza, logo, se faz necessário entender isso de antemão para se chegar a um possível conceito. Nesse viés, fica evidente nos materiais acadêmicos, que o conceito teve uma eclosão e um crescente aprimoramento ao longo do tempo e principalmente, após o fim da Guerra Fria (1945-1991). Ou seja, é notório segundo o arcabouço teórico das Relações Internacionais, o quanto o termo em questão saiu de "uma agenda tradicional" e realista, para um âmbito no qual se abarca "questões não tão tradicionais" (Pontes, 2015, p. 10). De acordo com Pontes (2015, p. 11), conforme abordado por Wolfers (1952), "segurança é um conceito crucial nas Relações Internacionais, mas também pode ser de natureza extremamente subjetiva" (Pontes, 2015, p. 11).

Segundo a vertente realista das Relações Internacionais, a segurança está atrelada à garantia da segurança nacional. Dado o contexto do período, ou seja, os primeiros anos da Guerra Fria e o ainda recente término da II Guerra Mundial (1939-1945), os interesses nacionais dos Estados estavam no centro das preocupações, tanto no quesito militar como político. Logo, a segurança do Estado se configurava como bem primário e, portanto, de grande interesse nacional. Por conseguinte, fica subentendido nessa vertente que ao securitizar o Estado, se seguraria também a segurança de seus cidadãos. Hans Morgenthau (1993, p. 3), em seu livro *Politics among Nations: the struggle for power and Peace* (Política entre as nações: a luta pelo

Poder e pela Paz), aponta que os estadistas têm como premissa a busca pelo poder para garantir os interesses nacionais, e dessa forma, a segurança é constituída enquanto um elemento resultante do poder. Ou seja, os Estados, enquanto atores únicos, têm "seus interesses e políticas nacionais guiados pelo desejo de poder absoluto" (Pontes, 2015, p. 12). Dentro da conjuntura do Sistema Internacional da época, "a segurança era vista então como seguro ou proteção contra invasões e baseava-se na existência de capacidades técnicas e militares" (Pontes, 2015, p. 12).

Além da relação de poder e segurança, de acordo com alguns estudiosos, a segurança também pode ser caracterizada como "ausência de ameaças"; ou ainda, segundo Baldwin (1997), como a diminuição da probabilidade da ameaça. No entanto, para detalhar melhor e para inserir em um contexto mais atual, a segurança teria duas especificações segundo Baldwin (1997, p. 26) sendo:

> a) Segurança para quem? Isso significa quem é o objeto de referência, ou quem deveria se sentir seguro. Seria o indivíduo, e se assim fosse, seriam alguns ou a maioria deles? Ou seria o estado, o sistema internacional, e assim por diante?
> b) Segurança para quais valores? Já que segurança não é um valor absoluto, ela precisa ser contrabalançada por outros valores fundamentais, como bem-estar econômico, liberdade, integridade territorial e conservação ambiental, por exemplo.

Para melhor explicar a Segurança, a perspectiva realista chega à conclusão de que essas especificações apresentadas por Baldwin, podem ser complementadas a outras tipificações como: " 'quanta segurança', segurança 'relativas a quais ameaças', 'de que forma', 'com que custo', e 'em que período' " (Pontes, 2015, p. 13-14).

A abordagem liberal das Relações Internacionais, apesar de consentir com o conceito anárquico e com o reconhecimento dos interesses individuais dos Estados tal como a vertente realista, acredita que os Estados podem colaborar entre si para lidar com questões de cunho internacional. Além disso, reconhecem que outros atores, como corporações transnacionais, grupos de *advocacy*, Organizações Intergovernamentais (OIGs), Organizações Não-Governamentais (ONGs), podem também atuar no sistema internacional. No entanto, o liberalismo deixa claro que o poder nacional de um dado Estado, bem como seus atores domésticos, tende a direcionar a atuação da política externa. Nessa perspectiva, o liberalismo defende que os Estados vão utilizar a anarquia a seu favor, promovendo a cooperação entre eles, usando as instituições governamentais de maneira a promover bem-estar, cooperação, segurança e equilíbrio no Sistema Internacional (Pontes, 2015, p. 15-16). No tocante à segurança, a teoria liberal vê que

essa vai além dos aspectos militares; ou seja, conceituar segurança voltado principalmente para o aspecto militar, conforme aponta Richard Ullman (2011, p. 11),

> expressa uma imagem totalmente falsa da realidade. Essa falsa imagem é duplamente enganosa e, por isso, duplamente perigosa. Primeiro, ela faz com que os estados se concentrem em ameaças militares e ignorem outros perigos talvez até piores, reduzindo assim a segurança total. E segundo, contribui para uma militarização invasiva nas relações internacionais que, a longo prazo, vai só reforçar a segurança global.

De fato, a Guerra Fria contribuiu demasiadamente para a definição do que vem a ser segurança, entretanto, após o fim deste conflito, ela se tornou uma prioridade, pois a partir daquele momento a segurança tinha que lidar, para além da segurança nacional e do sistema internacional, com a segurança de grupos e indivíduos; a segurança política, econômica, social, ambiental e humana. Em consonância a isso, Buzan em seu excerto *People, States and Fear: An Agenda for International Security Studies em The Post-Cold War Era* (1991) pondera que a segurança abrange cinco dimensões, são elas: segurança militar, política, econômica, ambiental e social. Buzan complementa que a segurança não deve ser analisada de forma isolada e vê no Estado o denominador basilar da segurança, enfatizando assim, ainda que indiretamente, o papel crucial que a segurança nacional possui, para garantir a segurança internacional (Buzan, 1991).

Mediante o marco temporal de fim da Guerra Fria, o mundo, bem como as pautas e agendas dos atores internacionais se desenvolveram, e, concomitantemente, o conceito de segurança, que por sua vez acabou se tornando mais amplo, incorporando pautas mais recentes e correntes, conforme pontuado por Brauch (2011, p. 63):

> O conceito de ameaça como base para o planejamento militar e para legitimação de programas militares – pelo menos entre os países da OTAN – mudou muito depois de 1990. Com a ampliação do conceito de segurança da tradicional segurança militar e diplomática para suas novas dimensões econômicas, sociais e ambientais, o conceito de ameaça também se expandiu para se aplicar a uma série de novas ameaças não só ao 'estado' como também a outras referências dos novos conceitos de segurança, englobando desde segurança de seres humanos a segurança global.

Dessa forma, pode-se compreender que a segurança não seria necessariamente um fim a ser atingido, mas um resultado mediante as ameaças e vulnerabilidades existentes entre os atores dentro do sistema anárquico, chegando a assimilar o conceito em questão com a sua origem latina, "*securitas*, que se refere à tranquilidade e despreocupação" (Liotta; Owen, 2006 *apud* Pontes, 2015, p. 17).

A abordagem construtivista, por sua vez, pondera que o entendimento de segurança é construído de modo intersubjetivo. Nessa lógica, elementos imateriais

como tradição, culturas, percepção, visão de mundo e crenças podem influenciar na interpretação das ameaças, perigos e riscos a serem constatados por um dado Estado. Assim, a segurança estaria relacionada a uma questão de concepção da identidade, e por conseguinte, ao construirmos nossa relação, podemos "compartilhar interesses, preferências, valores, crenças e compromissos" (Pontes, 2015, p. 19). Nessa visão construtivista, as identidades determinam o caráter da relação de um ator com o mundo. Em outras palavras, segundo Agius (2013, p. 88), a "segurança advém da cooperação para conseguir segurança sem que outros tenham de ser privados dela".

A partir da visão dos construtivistas do terceiro mundo, segundo Amitav Acharya (2011), e consoante (Pontes, 2015, p. 20), boa parte dos conflitos que tangem a questão da segurança se origina "em condições regionais locais, não em transformações no sistema internacional". Ademais, há uma certa predominância de conflitos nos países em desenvolvimento em que elementos como "a escassez de recursos, a superpopulação, o subdesenvolvimento, e a degradação ambiental" (Acharya, 2011, p. 54) contribuem significativamente para uma maior insegurança. Os realistas, em contrapartida, preferem enfatizar o papel da força e da atividade militar como componentes essenciais para a definição da segurança. Invariavelmente, para compreendermos a segurança é necessário olhar e considerar suas múltiplas dimensões. Em síntese, conforme ressaltou o renomado Kofi Annan em 1995, "não haverá desenvolvimento sem segurança e não haverá segurança sem desenvolvimento" (Annan, 2005).

Mediante as teorias, debates e perspectivas analisadas até aqui, reconhece-se a área da Segurança como no centro das Relações Internacionais, e para buscar responder à pergunta "o que são estudos em segurança?", será necessário retomar o cenário e objeto posto em voga. Todavia, apesar das forças militares e a proteção e expansão do Estado terem um papel ainda fundamental para a compreensão do que é segurança, com o evoluir dos tempos, esse conceito vem sendo cada vez mais aprimorado. Conforme cita David Mutimer (2013, p. 69): "uma vez que se questiona o objeto referente da segurança, deve-se questionar também a natureza e o âmbito da segurança e, por via de consequência, dos estudos em segurança". Em outras palavras, o conceito de segurança pode perpassar por questões que dizem respeito a ameaças territoriais e militares, como também, abranger outros tópicos, como atividades criminosas transnacionais (a própria ameaça cibernética, por exemplo), meio-ambiente, terrorismo, comércio internacional, desenvolvimento, armas, pobreza, destruição em massa, *etc*.

Em síntese, há três grandes grupos quando se trata da segurança conforme o estudo de Pontes, um primeiro, mais tradicionalista, por assim dizer, prefere deixar a definição mais intacta, abarcando os conceitos iniciais do viés militar. Um segundo grupo, que defende uma reforma modesta da área de segurança. E um terceiro grupo, o qual mistura os pensamentos das três correntes das Relações Internacionais, e contesta o primeiro, ao defender que a segurança deve abranger, para além do quesito militar, outros aspectos como as questões criminosas, ambientais, econômicas, grupos terroristas, organizações internacionais, movimentos sociais, empresas privadas, entre infinitas outras, eles são chamados de "alargadores" (Pontes, 2015, p. 24). A critério de particularização, este trabalho tenderá a atrelar a esse último grupo ao ponderar a segurança envolvendo o escândalo da espionagem estadunidense e sobretudo o vazamento de dados que chocaram o mundo ao qual o Brasil esteve intrinsecamente no epicentro do debate, entre os anos de 2013-2015. Por fim, consoante a interpretação de um dos mais influentes especialistas em matéria de Inteligência do Brasil, Marco Cepik, ressalta que:

> Segurança seria então uma condição relativa de proteção na qual se é capaz de neutralizar ameaças discerníveis contra a existência de alguém ou de alguma coisa com razoável expectativa de sucesso. Em termos organizacionais, segurança é obtida através de padrões e medidas de proteção para conjuntos definidos de informações, sistemas, instalações, comunicações, pessoal, equipamentos ou operações (Cepik, 2002, p. 138)

Posto o breve esclarecimento do que é segurança dentro do campo das Relações Internacionais, faz-se necessário tensionar e aproximar o debate da segurança para o conceito de inteligência, ou melhor, para o que é denominado "Segurança da Inteligência". Os autores que focalizam no estudo dessa vertente tendem a ver o debate de "*Security Intelligence*" como áreas inicialmente separadas que, ao se juntarem, dependem e têm funções simétricas (Cepik, 2003, p. 57). Portanto, inteligência, à priori, em seu sentido amplo, se resume em informação ou conhecimento (Cepik, 2003, p. 24-248), e independentemente, essa atividade é capaz de auxiliar nas tomadas de decisões de um governo, e na atuação das organizações, instituições, dos gestores entre outros. Em seu sentido restrito por sua vez, inteligência "é a coleta de informações sem o consentimento, a cooperação ou mesmo o conhecimento por parte dos alvos da ação. Nesta acepção, inteligência é o mesmo que segredo ou informação secreta" (Shulsky, 1995, p. 26 *apud* Cepik, 20003, p. 249). Outrossim,

> inteligência lida com o estudo do "outro" e procura elucidar situações nas quais as informações mais relevantes são potencialmente manipuladas ou escondidas, em que há um esforço organizado por parte de um adversário

> para desinformar, tornar turvo o entendimento e negar conhecimento. Os chamados serviços de inteligência de segurança (security intelligence) têm alguns alvos puramente domésticos, mas até mesmo esses compartilham a condição de "outro" aos olhos do arcabouço constitucional e da ordem política constituída (Cepik, 2003, p. 253).

Além disso, a inteligência se divide em categorias e em "operações". As primeiras são utilizadas quando o assunto é obtenção, análise e disseminação das informações de inteligência; são elas: inteligência política; inteligência militar; inteligência científica/tecnológica; inteligência econômica e inteligência sociológica. Já as operações são utilizadas a depender do seu aspecto, podendo esse ser: "transnacional (terrorismo, crime organizado *etc*); regional (África Austral, UE *etc*); nacional (EUA, China *etc*) ou subnacional (máfias criminosas, grupos de milícia armados, *etc*)" (Cepik, 2003, p. 255).

Ainda sobre inteligência, há oficialmente três fontes de Inteligência de acordo com a literatura, a saber: *Humint* (*Human Intelligence, tradicional*), *Sigint* (*Signals Intelligence*, mais utilizada durante a II Guerra Mundial e Guerra Fria) e *Imint* (*Imagery Intelligence*, mais recente, pós Guerra Fria). Há também uma outra fonte, mais vigente, chamada *Masin*t (*Measurement and Signature Intelligence*), a qual coleta assinaturas de certos equipamentos e dados geofísicos adjunto a uma outra variedade de fontes, para posteriormente fazer uma análise de tais coletas. Outrossim, as grandes potências possuem a chamada vigilância espacial, a qual emprega sistemas de inteligência terrestres e espaciais para monitorar suas áreas no espaço. Além disso, tem a *Osint* (*Open source Intelligenc*e, a qual se desenvolveu com o avanço da globalização e da *internet)*, na qual há programas responsáveis por circular e coletar informações entre os países que a possui. Outro ponto complementar à compreensão de inteligência diz respeito ao seu ciclo, o qual costuma ser de coleta, análise das informações e então a disseminação dessas informações para os usuários finais, os quais tendem a ser, em sua maioria, os tomadores de decisão (Cepik, 2003, p. 249-250).

Para o Sistema de Inteligência Brasileiro (SISBIN) por sua vez, em consonância com a Lei 9.883/1999, entende-se inteligência como:

> atividade que objetiva a obtenção, análise e disseminação de conhecimentos dentro e fora do território nacional sobre fatos e situações de imediata ou potencial influência sobre o processo decisório e a ação governamental e sobre a salvaguarda e a segurança da sociedade e do Estado (BRASIL, 1999a).

As atividades de inteligência no Brasil tendem a classificar as informações em aspectos militares, táticos, geral, diplomático, político, econômico, social, biográfico, científico, tecnológico e baseado em comunicações por transportes; ou seja, sua atuação não é similar às da polícia. Todavia, a inteligência tem algumas fases a serem atingidas antes de utilizar essa informação para tomar alguma decisão, como a necessidade do conhecimento, coleta de dados disponíveis e não disponíveis, processamento desses dados, disseminação do conhecimento ao usuário e por fim, a tomada de decisão (Brasil, 2005b).

Nessa perspectiva, Miranda Filho ressalta que "o Serviço de Inteligência pode atuar como mais um órgão de segurança, especializado em antiterrorismo, por exemplo, ou até liderando o processo de estimativas de risco" (Miranda Filho, 2012, p. 86) como acontece em alguns outros países. No Brasil, por exemplo, a Agência Brasileira de Inteligência (ABIN) segundo Miranda Filho, tem um programa chamado: Programa Nacional de Proteção do Conhecimento Sensível (PNPC) que atua na "proteção e salvaguarda de conhecimentos sensíveis de interesse da sociedade e do Estado Brasileiros (Miranda Filho, 2012, p. 86).

A breve sintetização do conceito de inteligência e sua relação com a Segurança se mostram imprescindíveis para compreender a maneira que tais conceitos estão intimamente relacionados ao objeto de estudo deste trabalho. Nesse sentido, conforme será abordado em maiores detalhes no decorrer dos capítulos, o Brasil, por ocasião do vazamento de dados realizado por Edward Snowden, percebeu que a sua segurança estava abalada e sua inteligência posta em cheque, em virtude da espionagem acometida a figuras centrais e chaves do Estado, dentre eles, a própria então presidente, Dilma Rousseff. Consoante isso, outros conceitos fundamentais para a compreensão do Sistema de Inteligência brasileiro serão analisados, partindo de uma perspectiva mais geral em direção à especificidade do caso.

Além disso, Fábio Miranda Filho (2012), em seu artigo "O papel do Serviço de Inteligência na Segurança das infraestruturas críticas", publicado na Revista Brasileira de Inteligência (RBI), concorda indiretamente com a ONU ao reforçar que "cabe ao Estado, por meio de sua estrutura técnica e de Segurança, incluindo a Inteligência, liderar um programa de proteção" (Miranda Filho, 2012, p. 80). Miranda Filho vai enfatizar ao decorrer de todo o seu artigo, um conceito chamado "Infraestruturas Críticas (IC)", para melhor explicitar essa relação do Estado com a Segurança e a Inteligência, ou aos "serviços de inteligência" de maneira mais precisa. Segundo o

Gabinete de Segurança Institucional, “infraestruturas críticas são instalações, serviços, bens e sistemas cuja interrupção ou destruição, provoque sério impacto social, ambiental, econômico, político, internacional ou à segurança do Estado e a sociedade” (Brasil, 2023b). Nesse viés, nota-se que o escopo deste trabalho, o sistema de inteligência brasileiro, se relaciona também com o conceito trazido por Miranda Filho acerca das infraestruturas críticas (IC). Logo, proteger uma significa proteger a outra também.

Cepik (2002) aponta que o conceito da Segurança está estritamente relacionado com outros conceitos, dentre eles segredo e ameaças. Em uma perspectiva mais nacional, Cepik conceitua esse formato de segurança como “uma condição relativa de proteção coletiva e individual dos membros de uma sociedade contra ameaças à sua sobrevivência e autonomia” (Cepik, 2002, p. 139). Em complemento a isso, Cepik (2002, p. 139) ressalta que boa parte dos

> “ordenamentos constitucionais contemporâneos reconhece a agressão militar, a espionagem, as operações encobertas, a invasão territorial e o bloqueio econômico como ameaças externas vitais, capazes de engendrar respostas dissuasórias proporcionais por parte dos Estados ameaçados.”

Além do mais, pode-se acrescentar aqui conceitos como terrorismo, narcotráfico e crime organizado (Cepik, 2002, p. 139). Dessa forma, pode-se aferir que tanto Miranda Filho (2012) quanto Cepik (2002), reconhecem e dão ênfase ao papel da Segurança para um Estado, especialmente quando o assunto é uso da inteligência como meio de se assegurar a sua própria estabilidade no âmbito nacional e em suas infraestruturas críticas e também, a paz no Sistema Internacional.

2.1 Contrainteligência e Segurança Cibernética

Segundo a Agência Brasileira de Inteligência (ABIN), contrainteligência pode ser conceituada como “a atividade que objetiva prevenir, detectar, obstruir e neutralizar a Inteligência adversa e as ações que constituam ameaça à salvaguarda de dados, conhecimentos, pessoas, áreas e instalações de interesse da sociedade e do Estado” (Brasil, 2020d). Dessa forma, a contrainteligência é a principal responsável por assegurar os interesses nacionais, bem como a segurança nacional, dirimindo ou impedindo os impactos da espionagem (que não sejam coniventes com o governo brasileiro), sabotagem, ameaças terroristas e vazamento de dados ou informações. Por

ter uma grande importância na inteligência brasileira, a contrainteligência, ou melhor, os integrantes e atores envolvidos nela, estão presentes em diversas áreas e instituições do Brasil, ou seja, não estão vinculados apenas à ABIN ou ao Sisbin, pois quanto mais frentes envolvidas nesse front, maior a efetividade da operação de contrainteligência em relação aos interesses nacionais (Brasil, 2020d).

No Brasil, a metodologia de atuação da contrainteligência é composta por: prevenção, ação que busca evitar o agrave, através de capacitações, orientações, sensibilização e até mesmo dando suporte às instituições sob alerta; detecção, medida que percebe a tentativa de ameaça à áreas chaves que compõe a segurança nacional, por meio de recursos humanos e tecnológicos com o intuito de fazer fracassar as ameaças; identificação, ação que determina a autoria da atividade antagonista; obstrução, atividade que impede ou dificulta o prosseguimento da atividade inimiga, desconhecida ou indesejada; neutralização, prática que paralisa os efeitos e suas consequências. Todas essas medidas são configuradas como essenciais e basilares para a contrainteligência ter um papel efetivo para com os interesses sociais e nacionais. Ademais, é papel da contrainteligência preservar o aprendizado da atividade de inteligência e também de entidades públicas, privadas e nacionais (Brasil, 2020d).

Além disso, parte da literatura brasileira sobre contrainteligência tende a dividir esse segmento em dois, sendo: segurança orgânica e segurança ativa. No primeiro, o enfoque está em proteger o setor de instalações, pessoal, documentos, e tecnologia de informação voltados para a área de segurança cibernética (*cyber security*). O segundo, por sua vez, diz respeito à atuação da contraespionagem, contra sabotagem, desinformação, contrapropaganda e contraterrorismo. Ainda, a segurança orgânica atua na obstrução e prevenção, enquanto a segurança ativa atua na neutralização e detecção. De qualquer modo, ambas as frentes têm um objetivo comum: o de salvaguardar os interesses do Estado, dirimindo suas vulnerabilidades diante de ameaças inimigas internas e externas (Baptistella e Vianna, 2022).

Ademais, a contrainteligência pode ser compreendida como "a atividade neutralizadora da inteligência antagônica" (Kamakawa, 2022, p. 540). De acordo com Paula *et al* (2012, p. 126),

> Percebe-se que "inteligência" vai muito além das atividades de Estado e de Governo, envolvendo um conjunto de ações interligadas que tem como propósito a busca da certeza e verdade sobre fatos que possam, direta ou indiretamente, afetar a vida das pessoas, da sociedade e do próprio governo, principalmente no sentido de se evitarem situações de crise ou de riscos reais ou potenciais. Assim, analisando o histórico do serviço de inteligência no

> Brasil, e a constância nessas atividades, percebe-se que o conceito de inteligência está diretamente associado à obtenção, utilização e gestão de informação. E o conceito de contrainteligência com o sigilo da informação que se possui, isto é, de impedir que outros possam obter e utilizar essas mesmas informações.

Ademais, Joanisval Brito Gonçalves, de acordo com a Escola Superior de Guerra (ESG), relata que contrainteligência, além de ser um aspecto da inteligência, conforme já supracitado, abrange certas medidas que buscam neutralizar a eficiência de serviços de inteligência adversos, ao mesmo tempo que tenta "salvaguardar os segredos da segurança nacional, bem como identificar as agressões à população (Gonçalves, 2018, p. 60)".

Em suma, entende-se que os Serviços de Inteligência (SI) estrangeiros vão atuar por meio da contrainteligência. A ABIN, posto isso, delimitou uma diretoria para atuar nesse ramo da inteligência, através da operabilidade em quatro áreas, como: proteção de documentos e conformidade; proteção na gestão de pessoas; proteção física e do ambiente, e proteção de sistemas de informação e continuidade (Oliveira, 2012, p. 69). Logo, a contrainteligência é indissociável da inteligência (Gonçalves, 2018, p. 60) e adquire um papel fundamental para reforçar a segurança da inteligência em um dado Estado. Desta feita, observa-se que perante o caso emblemático do vazamento de dados ocorridos durante o mandato de Dilma Rousseff, a contrainteligência brasileira aparentou vulnerável ou insuficiente ao cumprir com seus pressupostos básicos. Em outras palavras,

> "é neste cenário que ações de contrainteligência são mais importantes. Desde o nível estratégico, passando pelo tático e operacional, os processos, pessoas e tecnologias devem ser acompanhados, visando identificar indicadores de comprometimento" (Baptistella e Vianna, 2022).

A esfera da segurança cibernética tem cada vez mais se tornado pauta corrente nas agendas internacionais, conforme se aumenta a presença e acessibilidade das novas Tecnologias da Informação e Comunicação (TICs) nos mais diversos espaços da sociedade, a saber, educação (principalmente à distância), comércio eletrônico, atendimento médico à distância, economia, desenvolvimento tecnológico e científico. Nesta feita, o rápido desenvolvimento e alcance das TICs e, em particular, o caráter da "qualidade, da integridade, da confiabilidade e da segurança" da denominada *internet*, rede mundial que se coloca como base para as TICs, têm contribuído para que algumas problemáticas surgissem ao longo do seu desenvolvimento. Nessa perspectiva, é notório, por outro lado, o quanto o avanço positivo das TICs contribui para uma

melhoria em diversos setores da sociedade, sobretudo nos países em desenvolvimento (Canongia e Mandarino, 2009, p. 22). Nesse cenário, o *National Counterintelligence and Security Center* (2022, p. 2) define ameaças cibernéticas como:

> Foreign Intelligence Entities conduct cyber operations to penetrate our public and private sectors in the pursuit of policy and military insights, sensitive research, intellectual property, trade secrets, and personally identifiable information (PII). FIE cyber activities present both CI and security threats.

Nesse sentido, se faz importante conceituar como a literatura e perspectiva brasileira conceitua segurança cibernética e como ela está relacionada à contrainteligência e à própria segurança como um todo.

Vale reiterar uma informação recorrente acerca dos espaços existentes no universo, há o espaço físico, o qual se conhece muito bem, e há o espaço cibernético, também denominado ciberespaço, o qual abrange o universo dos computadores e do fenômeno da *internet*. O ciberespaço vem sendo pauta corrente de inúmeros debates, discussões, estudos, pesquisas e análises. A partir disso, existe a denominada defesa cibernética. Enquanto a segurança cibernética tem um enfoque na "prevenção e repressão", a defesa cibernética atua nas "ações operacionais de combates ofensivos" (Canongia; Mandarino, 2009, p. 26). O conceito de segurança cibernética no Brasil, embora novo, tem cada vez mais se desenvolvido de modo que a seguinte conceituação é frequentemente utilizada: "segurança cibernética é entendida como a arte de assegurar a existência e a continuidade da Sociedade da Informação de uma Nação, garantindo e protegendo, no Espaço cibernético, seus ativos de informação e suas infraestruturas críticas" (Mandarino, 2009, p. 29). Em complemento a isso, o termo originário de Segurança cibernética, *cybersecurity* do inglês, apresenta algumas características particulares, que valem a pena serem pontuadas. O primeiro fato a ser pontuado, originário do *Department of Homeland Security* (DHS), entende *cybersecurity* como

> "a prevenção aos danos causados pelo uso não autorizado da informação eletrônica e de sistemas de comunicações e respectiva informação neles contida, visando assegurar a confidencialidade, integridade, e disponibilidade, incluindo, também, ações para restaurar a informação eletrônica e os sistemas de comunicações no caso de um ataque terrorista ou de um desastre natural (National Infrastructure Protection Plan. Partnering to enhance protection and resiliency. DHS, . p.12 apud Canongia e Mandarino, 2009, p.26).

Já o segundo ponto, trazido da International Communications Union (ITU), compreende *cybersecurity* como meio que promove

> "proteção contra acesso, manipulação, e destruição não autorizada de recursos críticos e bens. Tais recursos e bens variam e dependem do nível de desenvolvimento dos países. Dependem, também, do que cada país considera

> como sendo recurso crítico, os esforços que podem e estão dispostos a realizar, bem como da avaliação do risco que estão dispostos a aceitar em conseqüência das inadequadas medidas de segurança cibernética. Adicionalmente, para certo número de países desenvolvidos, há outras ameaças tais como fraude, proteção do consumidor, e privacidade, as quais consideram também como soluções da cybersecurity, forma de proteger e manter a integridade das infraestruturas críticas nos setores financeiro, de saúde, da energia, do transporte, das telecomunicação, da defesa, e de outros. (ITU Global Cybersecurity Agenda - GCA. . Framework for International Cooperation in Cybersecurity. ITU, 2007, p. 10 apud Canongia; Mandarino, 2009, p. 26)".

Além disso, os países que fazem parte da Organização para a Cooperação e o Desenvolvimento (OCDE), dentre eles os EUA, acordaram no que tange segurança na Sociedade da Informação com os seguintes princípios: 1. Sensibilização sobre riscos; 2. Responsabilidade; 3. Resposta; 4. Ética; 5. Democracia; 6. Avaliação de riscos; 7. Concepção; 8. Gestão da Segurança e 9. Reavaliação. Embora o Brasil esteja no processo de adesão à OCDE, os seus membros, em sua maioria, os países de primeiro mundo, têm premissas e obrigações a serem seguidas, como os princípios supracitados. Logo, à vista do caso deste trabalho, os EUA acabaram por infringir determinados princípios da Segurança cibernética em relação ao Brasil. Outrossim, em uma dada reunião sobre cultura de Segurança, promovida pela OCDE, colocou-se em evidência que: (...) as questões de segurança devem ser objeto de preocupação e responsabilidade de todos os atores, seja governamental, empresarial, e de outros (pesquisa e terceiro setor)" (Canongia; Mandarino, 2009, p. 24).

Deste modo, a segurança cibernética é relevante pois se estabelece enquanto parte da função estratégica de governo de um dado Estado e se mostra essencial para "manutenção e preservação das infraestruturas críticas, como saúde, energia, defesa, transporte, telecomunicações, da própria informação, entre outras (Canongia; Mandarino, 2009, p. 25)". Sob tal perspectiva, o governo federal brasileiro considera segurança cibernética como "infraestrutura crítica da informação" a qual tem impacto direto na segurança da sociedade e também do Estado (Canongia; Mandarino, 2009, p. 27), sobretudo, devido ao fato das atividades governamentais e empresariais estarem em crescente migração para o ambiente virtual. Dessa forma, surge um novo conceito, a ciber-resiliência, com o intuito de promover um alinhamento entre os envolvidos, buscando aumentar a confiança no sistema, com a parceria da "prevenção, absorção, recuperação e adaptação após emergências". Em suma, (Desolda *et al*, 2021 *apud* Georg *et al,* 2022, p. 604) "a segurança cibernética envolve segurança, salvaguardas, políticas,

diretrizes, abordagens de gerenciamento de riscos, boas práticas, ferramentas com foco na proteção do ambiente cibernético e nos ativos de risco".

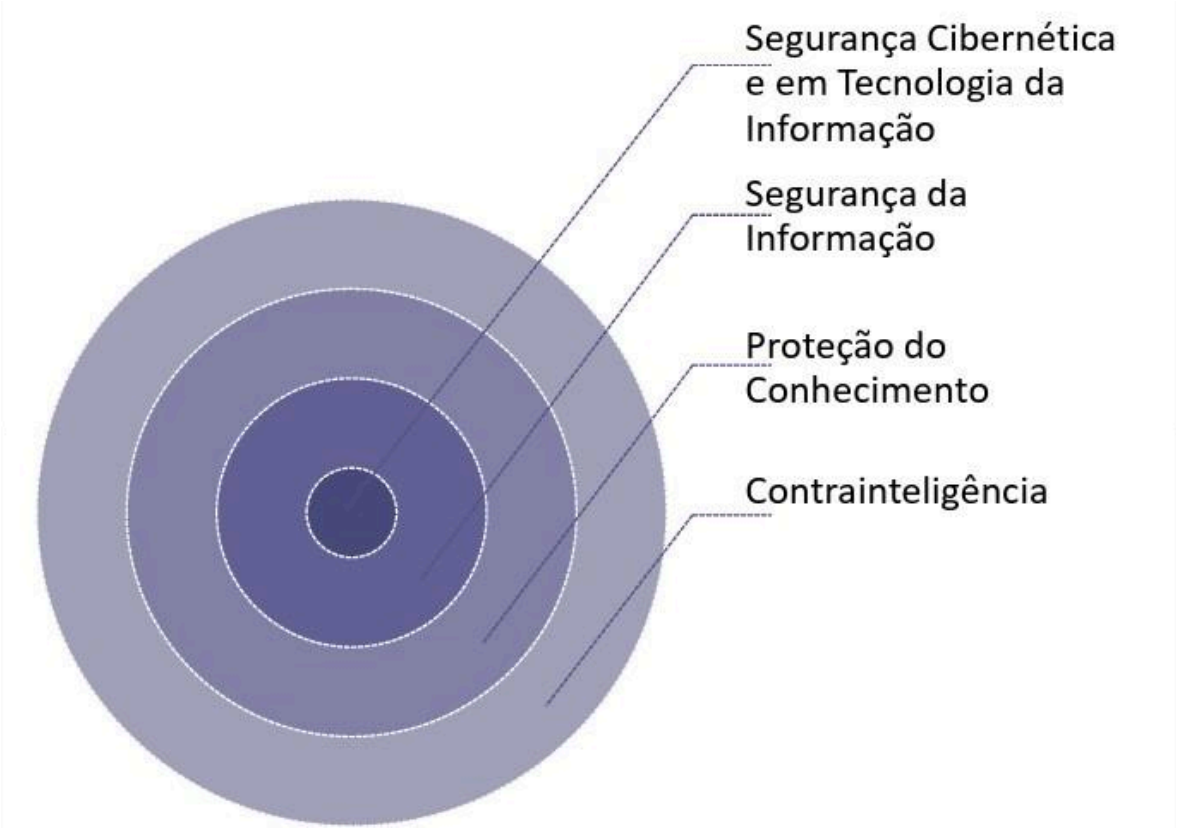
A relação da segurança cibernética com o setor público brasileiro apresenta de antemão um desafio na sua própria estrutura, visto que não há um órgão específico que cuida de todas as nuances e frentes que abrangem a segurança cibernética. Logo, áreas relacionadas à segurança cibernética, como Segurança da Informação e Comunicações (SIC) e Segurança dos ativos de informação críticos, tendem a ficar em uma situação crítica e suscetível a vulnerabilidades, devido aos desafios inerentes a sua estrutura e formação dentro do contexto brasileiro (Brasil, 2015c).

A institucionalização da Segurança cibernética teve um impulso a partir de alguns eventos, dentre eles, a aprovação do Marco Civil da *Internet* em 2013, o qual por sua vez foi motivado pelo vazamento de dados ocorridos entre 2013-2015. Se por um lado a contrainteligência, função essa indissociável da inteligência (Gonçalves, 2018), ao ser posta em prática pelo Estado, vai atuar em todos os níveis necessários (estratégico, tático, operacional, processos, pessoas e tecnologia) para garantir a segurança da inteligência, por outro, a segurança cibernética vai atuar em complemento à contrainteligência, assegurando as estruturas críticas do Estado, as quais apresentam impacto direto à sociedade como um todo (Canongia; Mandarino, 2009). Em complemento a isso, Georg (*et al*, 2022), sobre o tema da segurança cibernética, aponta que os ataques a órgãos públicos serão cada vez mais intensos e sofisticados. Embora o objetivo de ambas contrainteligência e segurança cibernética seja de salvaguardar os interesses do Estado, dirimindo suas vulnerabilidades diante de ameaças inimigas internas e externas (Baptistella;Vianna, 2022), o fato do Brasil ainda estar em processo de melhor estruturar um órgão voltado apenas para a segurança cibernética reforça o quão imprescindível é a atuação da contrainteligência para garantir a segurança da inteligência como um todo, dentro do Estado brasileiro.

Outrossim, o Brasil divulgou um documento E-Ciber em 2020, por meio do Decreto nº 10/222, o qual representa um marco positivo, embora carente de melhorias, no que diz respeito à matéria de Segurança Cibernética. Esse documento tem como intuito, entre outros, apresentar à sociedade brasileira uma orientação acerca da atividade cibernética no país. Ou seja, a atuação da atividade de segurança deve estar situada para além da tecnologia de informação apenas, pois esse representa um dos viés de inúmeros outros que podem inferir no campo da segurança da inteligência, sendo assim, *cyber security* e contrainteligência, se mostram cruciais e necessárias para

contribuir para uma maior segurança de fato, nos serviços de inteligência. A Figura 1 abaixo, mostra como os conceitos apresentados estão organizados:

Figura 1 - Organização dos Conceitos



Fonte: Alvares, 2024.

3 O SISTEMA DE INTELIGÊNCIA BRASILEIRO

O Sistema de Inteligência Brasileiro, formalmente constituído em meados do século XX, foi fortemente influenciado pelos acontecimentos internacionais, como I Guerra Mundial, II Guerra Mundial e Guerra Fria, os quais fizeram com que o Brasil se posicionasse e tomasse algumas medidas. A literatura pertinente ao debate de inteligência, inicialmente pontua que antes da década de 90, no Brasil, o que se entende hoje como atividade de inteligência e espionagem era denominada como informação, ou ainda, como atividades de informações. Porém, devido aos acontecimentos durante a Ditadura Militar, e a infeliz relação dos órgãos de informação em auxílio à repressão, somente a partir de 1990 adotou-se o termo inteligência, como forma de se distanciar da violência realizada por parte governo, apresentando uma nova roupagem às atividades de informações (Brandão e Quadrat, 2024, p. 108). No entanto, conforme (Pinheiro, 2012), pontua em seu excerto,

> mudar o nome de informação para inteligência não é suficiente para se ter legitimidade. É preciso institucionalizar o setor de inteligência e a competência desse órgão através da força de seu quadrante: política externa, defesa, segurança e controle, e não mais uma função de repressão interna.

Embora o processo de formalização do sistema de inteligência brasileiro tenha ocorrido no século XX, relatos e materiais históricos datam a existência de atividades secretas desde o Brasil Colônia. Foi nesse mesmo período histórico que foi criado o Regulamento Paranhos, elaborado por José Paranhos, popularmente conhecido como o visconde do Rio Branco, com o intuito de reestruturar a então Secretaria de Estado de Negócios Estrangeiros, o qual continha prescrição normativa quanto à salvaguarda de material confidencial (Araújo, 2004).

O Brasil ainda durante a Primeira República (1889-1930), precisamente durante a presidência de Epitácio Pessoa (1919-1922), criou a Inspetoria de Investigação e Segurança Pública, a qual teve seu funcionamento inicial somente em 1920. Essa estrutura civil tinha duas fontes, uma social e outra política. A primeira, atuava na coibição dos movimentos dos trabalhadores, também na crescente imigração de estrangeiros em grande escala, na contenção de membros ligados ao Partido Comunista e a Anarquia. Já a frente política, encarregava-se de promover equilíbrio ao governo, ao buscar conter os antagonismos provenientes das oligarquias que também queriam tomar o poder. Do ponto de vista histórico, criou-se, em 1946, o Serviço Federal de Informações e Contrainformações (SFICI), através do Decreto nº 9.775-A enquanto

Eurico G. Dutra era presidente. Todavia, a institucionalização do órgão só ocorreu 10 anos depois, em 1956, durante o mandato de Juscelino Kubitschek, e por forte influência estadunidense, visto que os EUA precisavam de aliados na América, ao mesmo tempo que buscavam dirimir a propagação do socialismo e comunismo no mundo e, principalmente, em sua própria região de domínio (Brandão e Quadrat, 2024, p. 109).

Embora a criação da SFICI tenha ocorrido durante o mandato de Dutra em 1946, foi somente após o Decreto nº 44.489-A, em 1958, durante o governo JK que o órgão em questão foi estruturado para coordenar as atividades de informações no Brasil e assuntos pertinentes à segurança nacional. O SFICI tinha um papel importante e equivalente ao da Forças Armadas, dos representantes dos Estados–Maiores e das Seções de Segurança dos Ministérios Civis, instituições essas que compunham a Junta Coordenadora de Informações (JCI). O orçamento do SFICI provinha da Secretaria Geral do Conselho de Segurança Nacional e,

> Na visão da época, a formação do SFICI veio preencher uma lacuna, pois até então não havia um órgão central de informações no âmbito federal que assessorasse diretamente a Presidência da República. No entanto, o que ocorreu na prática foi a construção de uma agência que viria a desempenhar um papel ativo no golpe militar de 31 de março de 1964 (Brandão e Quadrat, 2024, p. 110).

Quando Artur Bernardes assumiu a presidência, em 1922, transformou a Inspetoria de Investigação e Segurança Pública na 4ª Delegacia Auxiliar, a qual atuava de maneira similar à Inspetoria. Cerca de 5 anos depois, o setor militar criou o Conselho de Defesa Nacional (CDN), cujas funções eram basicamente "estudar e coordenar dados sobre todas as questões de ordem financeira, econômica, bélica e moral, relativas à defesa da Pátria" (Antunes, 2002, p. 43).

A estrutura de informações no Brasil teve uma relação próxima com a violência política desde os seus anos iniciais, dado as particularidades da época. Essa violência aumentou de maneira bastante considerável desde os anos 30, a partir da ascensão de Getúlio Vargas. Algumas mudanças ocorridas durante a era Vargas foram a formação da Delegacia Especial de Segurança Pública e Social (DESPS), cuja atuação pressionou para a sua própria extinção. Ao extinguir a DESPS, Vargas deu origem ao Departamento Federal de Segurança Pública (DFSP), o qual adquiriu todas as responsabilidades e direitos concernentes às informações do Estado desde 1920. Com o advento da II Guerra Mundial, o setor de Informações do Brasil passou a atuar em duas frentes, uma

militar sob a supervisão da Secretaria Geral do Conselho de Segurança Nacional (SG-CSN) e a outra frente, civil, que tinha foco no DFSP. Com a transferência da capital do Rio de Janeiro para Brasília (1960), os militares optaram por transferir todo o acervo sobre Informações do DFSP para as Forças Armadas (Brandão e Quadrat, 2024, p. 109-110).

Consoante esse breve relato histórico, nota-se que a atividade de inteligência no Brasil, desde os seus primórdios, esteve intrinsecamente relacionada à máquina pública, seja em seu surgimento e estruturação, ou até mesmo no ataque aos Direitos Humanos, durante o regime militar. Desde o SFICI observa-se uma busca e interesse do governo em aprimorar suas atividades de informações, visto que era ofertado cursos no Brasil, pela Escola Superior de Guerra (ESG), e era incentivado não só a inserção das mulheres, mas também a parceria e o intercâmbio no exterior para obter conhecimento e aperfeiçoamento interno, nas frentes tecnológicas e nos equipamentos, e manter os contatos e proximidade com o exterior, principalmente dos EUA, Inglaterra e França. Outrossim, esse intercâmbio fez com que o Brasil se aproximasse de seus vizinhos, principalmente dos países do Cone Sul, aproximação essa que se mostrou bastante vantajosa, visto que boa parte dos países da América do Sul estavam enfrentando questões similares, a saber, ditaduras e golpes (Brandão e Quadrat, 2024, p. 111). Além de que, hoje de maneira mais irrisória, porém, antes do fim das ditaduras na região, os países do Cone Sul, viam a atividade de inteligência, com suspeitas, devido ao "alto grau de autonomia, poder e capacidade operacional" que essas instituições tinham nesse período (Oliveira, 1999, p. 19).

Em virtude das duras críticas ao SFICI por questões estruturais e orçamentárias, e a deposição do presidente João Goulart em 1964, os militares que já estavam tomando o poder e reestruturando as instituições, acharam por bem dissolver a SFICI e dar aval de criação ao Serviço Nacional de Informações (SNI). O general, político e geopolítico brasileiro, Golbery do Couto e Silva, em 1955 propôs em seu livro "Planejamento Estratégico" a criação do SNI. Todavia, somente 11 anos depois, em 1964, através da lei nº 4.341, que ocorreu a sua implementação de fato. Propositadamente, Golbery tornou-se o primeiro chefe e principal responsável por toda a estruturação do SNI. Dessa forma,

> o SNI era a estrutura central do Sistema Nacional de Informações, o SISNI, e responsável pela criação do Plano Nacional de Informações (PNI). Com isso, surgiu nos anos seguintes uma complexa e gigante estrutura que coordenava

> as atividades de informações e a repressão aos opositores do regime (Brandão e Quadrat, 2024, p. 112).

Todos os âmbitos do governo (federal, estadual e municipal) tinham ou criaram no decorrer da ditadura órgãos responsáveis pela informação e contrainformação do Brasil, sendo todos integrados ao SISNI.

Em caráter de soma ao SNI, o Sistema de Segurança Interna (SISSEGIN) foi criado em 1970, sob a administração do Ministro do Exército, Orlando Geisel, durante o mandato de Médici. Os documentos denominados, Diretriz para a Política de Segurança Interna e Plano de Segurança Interna, foram elaborados para tratar da perseguição dos opositores ao sistema político. Essa estrutura, após a instituição do Ato Institucional nº 5 (AI 5), de 1968, coordenou os Centros de Operações de Defesa Interna e Destacamentos de Operações Internas, também denominados, DOI-CODIs. Esses centros e destacamentos foram os de principal destaque quanto aos "principais casos de mortes e desaparecimentos forçados no anos 1970 no país" (Brandão; Quadrat, 2024, p. 113). Diferentemente do SFICI, pelo fato do chefe do SNI ser um ministro, o SNI, mesmo não sendo um ministério de fato, não teve problemas orçamentários, seu orçamento inclusive, era um dos maiores na época. Logo após algumas mudanças, o SNI passou a ter bastante autonomia e forte atuação graças ao número de pessoas que atuavam em Brasília na Agência Central e nas agências subordinadas dos estados. Além disso, o SNI também se encarregou de especializar os militares e civis que atuariam nas informações (Brandão e Quadrat, 2024, p. 114-115).

Em 1971, a Escola Nacional de Informações (EsNI) foi criada por meio do decreto nº 68.448 com o objetivo de "preparar civis e militares para o atendimento das necessidades e informações e contrainformações do Sistema Nacional de Informações (...)" (Decreto nº 68.448 *apud* Brandão e Quadrat, 2024, p. 115). Ainda, a EsNI tinha a intenção de tomar para si o monopólio da formação dos profissionais do ramo das informações, se diferenciando da ESG no ponto de buscar ofertar atividades mais práticas. A EsNI, nesse e em outros aspectos, acabou ganhando desenvoltura devido ao momento o qual o país estava passando; em outras palavras, os interessados estavam buscando mais ação do que aulas teóricas. A construção da EsNI contou com o máximo sigilo dos profissionais envolvidos e uma inauguração discreta. A EsNI tinha uma estrutura bastante sólida e bem preparada para atender os objetivos propostos e também aos civis e militares ingressantes, tanto nacionais bem como estrangeiros, inclusive,

mulheres também eram integradas, um fato inovador para a época (Brandão e Quadrat, 2024, p. 116-118).

Devido à forte ligação do SNI com a repressão durante a ditadura, seu fim se iniciou em 1987 e se consolidou no início da década de 90, com um novo modelo de governo. Dentre os inúmeros argumentos que justificam a sua dissolução, como questões estruturais e conforme os registros dos documentos, a nova era da Democracia, fizeram com que os representantes eleitos, políticos e a nova configuração governamental, chegassem à conclusão de que o SNI não era mais necessário (Brandão e Quadrat, 2024, p. 119-124). Com a posse de Fernando Collor de Melo na presidência deu-se a reorganização de fato do sistema de inteligência brasileiro como um todo, com os adventos iniciais da extinção do SNI e da Secretaria de Assuntos de Defesa Nacional (SADEN), através da medida provisória nº 150. Por outro lado, essa mesma medida deu origem à Secretaria de Assuntos Estratégicos (SAE), a qual tinha um modesto Departamento de Inteligência. Todavia, o poder executivo propôs, em 1991, ao Congresso, um projeto de Lei nº 1862, voltado para a criação de um órgão federal de inteligência, com foco na atividade para o exterior, ou seja,

> sua atividade compreenderia a execução de ações direcionadas para a obtenção de dados e a avaliação de situações externas que pudessem implicar ameaças externas, veladas ou dissimuladas, e que fossem capazes de dificultar ou impedir a consecução dos interesses estratégicos do Brasil na cena internacional (Lei nº 1862 apud Brandão e Quadrat, 2024, p. 126).

Entretanto, devido às dificuldades do governo Collor em lidar com os militares, esta lei foi extinguida e a atividade de inteligência retirada da SAE, além de ampliada a participação militar na esfera da inteligência através da criação do Centro Federal de Inteligência (CFI). Todavia, essa ação de Collor foi considerada tardia e, somada aos fatores que ocasionaram em seu impeachment, contribui para que o executivo removesse este ponto da pauta política. Com a saída de Collor, Itamar Franco assumiu o poder e fez com que o cargo de secretário da SAE se tornasse ministro, transformando o Departamento de Inteligência em Subsecretaria de Inteligência (SSI) (Brandão e Quadrat, 2024, p. 126-128).

Em contrapartida, o período pós-ditadura é visto como um período bastante delicado para a atividade de inteligência, pois havia, em primeiro lugar, o desprezo por parte da sociedade, devido à estreita relação desse ramo com alguns conflitos da ditadura; em segundo, a permanente força militar dentro desse setor; e em terceiro, a negligência existente entre as políticas voltadas para um regime democrático e as

relações de poder internacionais, visando o bom desenvolvimento das áreas de atuação do Estado Nacional. Com a posse em 1994 de Fernando Henrique Cardoso (FHC), houve a Medida Provisória nº 813 em 1995, a qual propunha uma reorganização da presidência da República, e dentre as propostas, estava a criação do que viria a ser a Agência Brasileira de Inteligência (ABIN). A forma de criar um órgão por meio de uma medida provisória foi criticada e o FHC teve que redirecionar essa iniciativa para um debate público. Esse debate ocorreu em 1996, na Câmara dos Deputados, e foi organizado pela CDN. Entre as intempéries, o referido marco legal só foi aprovado em 1998, após a reeleição de FHC (Brandão e Quadrat, 2024, p. 128-130).

Dada a dificuldade de implementar mudanças ou melhorias nas áreas de segurança e defesa, sobretudo em um país que havia acabado de sair de uma ditadura e que ainda possuía urgência em relação a questões básicas, como saúde, moradia, educação entre outros, mostrar que o setor de inteligência era também prioritário para a própria sociedade civil acabava sendo moroso.

O processo de criação do Sistema Brasileiro de Inteligência (SISBIN) bem como da Agência Brasileira de Inteligência (ABIN) se iniciou ainda em meados de 1996, porém só foi formalmente consolidado através da Lei nº 9.883, após aprovação do Congresso Nacional e validação de FHC, então presidente na época. A referida Lei definiu a atividade de inteligência como

> a atividade que objetiva a obtenção, análise e disseminação de conhecimentos dentro e fora do território nacional sobre fatos e situações de imediata ou potencial influência sobre o processo decisório e a ação governamental e sobre a salvaguarda e a segurança da sociedade e do Estado (Lei nº 9.883, art. 1, parágrafo 2º).

Nessa feita, a ABIN e o SISBIN são duplamente importantes, e ambos são supervisionados pela própria ABIN. O artigo 1º da lei determina os fundamentos, objetivos e demais observações sobre a estruturação e princípios que regem o SISBIN. O artigo 2º da lei pontua que todos que fazem parte da relações exteriores, defesa externa, segurança interna e outros membros da Federação também poderiam integrar o SISBIN. Ademais, a referida lei proíbe veementemente o uso indevido da atividade de inteligência de maneira similar ao que aconteceu durante a ditadura. Como também, restringe o uso desta para fins estritamente particulares, oriundo principalmente das autoridades e dirigentes do SISBIN (Brandão e Quadrat, 2024, p. 131). É portanto competência da ABIN,

> Art. 3º Fica criada a Agência Brasileira de Inteligência - ABIN, órgão da Presidência da República, que, na posição de órgão central do Sistema Brasileiro de Inteligência, terá a seu cargo planejar, executar, coordenar, supervisionar e controlar as atividades de inteligência do País, obedecidas à política e às diretrizes superiormente traçadas nos termos desta Lei (Vide Medida Provisória nº 1.999-17, de 2000; Lei nº 9.883, art. 3º).

Outrossim, embora a iniciativa de FHC de melhor estruturar as atividades de inteligência no país tenha sido genuína, essa tentativa foi marcada por alguns impasses e percalços. Um desses pontos foi a própria Comissão de Controle da Atividade de Inteligência (CCAI), a qual tomou forma somente em 2013, contando com seis membros representantes da Câmara e seis do Senado. Essa comissão é fundamental, pois cabe a ela concordar ou não com a indicação do presidente da ABIN, realizada pelo presidente da República; cabe a ela também acessar de maneira irrestrita todas as informações pertinentes aos órgãos que compõem o SISBIN. Na prática, porém, observa-se que a referida comissão tem um papel de maior enfoque na ABIN do que em relação ao SISBIN (Brandão e Quadrat, 2024, p. 133).

Dessarte, observa-se que a ABIN é uma instituição expoente quando o assunto é inteligência e espionagem no Brasil. A ABIN além de ser órgão central do SISBIN, é a principal responsável de informar à Presidência da República, com informações, estratégias, análises, *etc*, que auxiliem no processo de tomada de decisão (Cartilha da ABIN, 2024). O SISBIN por sua vez, se configura como o principal responsável por "integrar as ações de planejamento e execução da Atividade de Inteligência" no Brasil (Brasil, 2023c, p. 5), e ele tem em sua composição: "Centros de Inteligência, ministérios, secretarias e agências da Administração Pública Federal (Brasil, 2023c, p. 5)". A ABIN enquanto órgão apartidário, apolítico e permanente, tem como principais fundamentos que a norteiam: "a preservação da soberania nacional, a defesa do Estado Democrático de Direito e a dignidade da pessoa humana" (Brasil, 2023c, p. 6). Isto posto, o principal instrumento norteador da Atividade de Inteligência no Brasil é representado pela Política Nacional de Inteligência (PNI), a qual "define os parâmetros e limites da Atividade de Inteligência e estabelece seus pressupostos, objetivos, instrumentos e diretrizes para atuação" (Brasil, 2023c, p. 16). Além do mais, o PNI apresenta ameaças mais relevantes as quais tem capacidade de expor em risco o Estado e a integridade da sociedade brasileira.

Atualmente a ABIN, se submete a certos mecanismos do governo federal para cumprir de maneira efetiva com a Atividade de Inteligência, a saber: Comissão Mista de Controle das Atividades de Inteligência (CCAI) do Congresso Nacional; Tribunal de

Contas da União (TCU); Secretaria de Controle Interno da Presidência da República (CISET/PR) e Controladoria-Geral da União (CGU) (Brasil, 2023c, p. 29). Conforme já sumariamente abordado na introdução deste trabalho, os casos de vazamento de dados que aconteceram durante o mandato da presidente Dilma Rousseff, precisamente entre 2013-2015, podem ter contribuído para a criação não só da Lei do Marco civil da *Internet* (2013), LGPD, entre outras criações e acordos que vieram posteriormente a esse ocorrido, mas também, pode ter influenciado os decretos que se oficializaram em 2016 e 2017, sendo primeiro o "Decreto nº 8793, de 29 de junho de 2016, que instituiu a Política Nacional de Inteligência e em segundo, o Decreto de 15 de dezembro de 2017, que instituiu a Estratégia Nacional de Inteligência" (Brasil, 2023c, p. 16).

Um ponto que merece destaque, seria que o então diretor do Centro de Pesquisa e Desenvolvimento para Segurança das Comunicações (Cepesc) da ABIN, Otávio da Silva, ainda em 2008, cerca de 5 anos antes do escopo deste trabalho, reiterou "que a Abin não realiza nenhum tipo de escuta telefônica e não tem competência nem equipamentos para realizar esse tipo de procedimento". Entretanto, a Polícia Federal é capaz de tal atividade (Brasil, 2008).

Se por um lado a Lei 9.883 se mostrou bastante pertinente dada a situação de prévia desorganização do Sistema de Inteligência como um todo, por outro, algumas questões foram relegadas ou postas em segundo plano. Entre 2000 e 2014, o número de órgãos vinculados ao SISBIN cresceu, porém, o estabelecimento sobre a Atividade de Inteligência foi motivo de bastante discussão e desorganização do SISBIN (Cepik, 2022, p. 91-109). Apesar disso,

> houve crises, fracassos e denúncias que atingiram o setor de inteligência na fase de maior expansão sob o regime democrático da Constituição Federal de 1988. Basta lembrar das crises desencadeadas pela Operação Satiagraha e pela revelação dos documentos que comprovavam a espionagem do governo americano contra a Presidência da República e a Petrobras (caso Snowden) (Brandão e Quadrat, 2024, p. 135).

Com a aprovação e divulgação da Doutrina da atividade de Inteligência em 2023, a sua atuação foi fundamentada e organizada levando em consideração a ética, princípios, valores, democracia entre outros, buscando dirimir as vulnerabilidades até então existentes (Brandão e Quadrat, 2024, p. 95).

Assim, após essa retomada histórica da formação do Sistema de Inteligência brasileiro, observa-se que não é recente que se tenta buscar a melhor maneira de consolidar e estruturar as atividades de inteligência no Brasil. O trajeto dessa longa jornada contribuiu para que a ABIN completasse 25 anos de relativa estabilidade, apesar dos desafios e problemas enfrentados. O SISBIN, em conjunto com a ABIN, tem se mantido ao longo desses anos, apesar de diversas questões e das trocas de governos, fatores esses que no século XX contribuíram para a inconstância e má estruturação e funcionamento da atividade de inteligência. Ao buscar compreender a atuação do Brasil, entre 2013 a 2015, perante o vazamento de dados realizado por Snowden foi necessário compreender a formação desse sistema de inteligência, para melhor averiguar como e o porquê a atuação do Sistema de Inteligência Brasileiro foi da maneira que ocorreu no período mencionado.

3.1 A Atividade de Inteligência no Brasil

Partindo da premissa de que a atividade de inteligência no Brasil é uma política pública, ou seja, a qual tem todas as fases que a tornam política pública, a saber, construção de agenda, formulação e implementação da política e avaliação (Howlett: Ramesh, 2003), é necessário buscar compreender melhor como o assessoramento, contribuições, críticas, falhas, desafios, desvios e questionamentos tornam a atividade de inteligência no Brasil, ou sua correspondente, a ABIN, na agência que é hoje. A virada de chave a qual define a Política de Inteligência num dado Estado, começa a partir do reconhecimento do fator ameaça, tais como eventos críticos ou situações que mostram a necessidade do aparato da inteligência, na segurança da população e das instituições, sobretudo governamentais, que regem aquela região (Aquino, 2024, p. 180-182).

Afinal, como mensurar se a política pública tão restrita como o é a atividade de inteligência está sendo eficiente? Basicamente, observa-se a maneira pela qual a agência ou os atores envolvidos lidam com as dinâmicas e dilemas em meio ao mundo político ao qual estão inseridas, como segredo estatal, democracia, segurança estatal, direito ao acesso à informação, segurança individual *etc*. No entanto, devido à característica particular de sigilo das atividades de inteligência, o enfoque é voltado para os indicadores de legitimidade, efetividade e eficiência da atuação (Trevisan; Van Bellen *apud* Aquino, 2024, p. 184), consoante Cepik, 2003:

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

A seguinte tendência é notória na atividade de Inteligência do Brasil, sobretudo na ABIN,

> a efetividade da política pública de Inteligência, ou seja, a capacidade de atingir os resultados pretendidos, é geralmente mal dimensionada, pois, por definição, os sucessos de uma agência de inteligência frequentemente precisam ser mantidos em segredo, enquanto as falhas são alvo de escrutínio público, midiático e político. Assim, poucas referências existem sobre o assessoramento bem-sucedido resultante da Atividade de Inteligência. Normalmente, são falhas que chegam ao conhecimento público e motivam questionamentos políticos, investigações e reforma de sistemas e instituições dedicados à Atividade de Inteligência (George; Bruce, 2008 apud Aquino, 2024, p. 197).

No Brasil, houve a fixação do Decreto nº 8.793, em 2016, da Política Nacional de Inteligência (PNI), ou seja, desde a consolidação da ABIN, somente em 2016, foi criada uma normativa nacional para a atividade de inteligência. Nele,

> são expressos os principais conceitos, pressupostos, valores e instrumentos da política pública de Inteligência. Destaca a função do SISBIN como arranjo institucional para a implementação da política, marcando a importância do planejamento integrado e do compartilhamento de dados. Os controles interno e externo da atividade foram também mencionados como importante elemento da política (Brasil, 2016).

Esse documento apresenta uma relação de itens que têm uma "potencial capacidade de pôr em perigo a integridade da sociedade e do Estado e a segurança nacional do Brasil" (Brasil, 2016 *apud* Aquino, 2024, p. 189). São alguns deles: interferência externa; espionagem; ataques cibernéticos; terrorismo; armas de destruição em massa; sabotagem; ações contrárias à soberania nacional; atividades ilegais; corrupção; criminalidade organizada; e ações contrárias ao Estado Democrático de Direito (Aquino, 2024, p. 190). Em outras palavras,

> "a atividade de inteligência no Brasil, sobretudo a ABIN, no seu papel de órgão central, tem como desafio prestar assessoramento a elevado número de potenciais usuários com necessidades informacionais diversas entre si, cuja prioridade de acompanhamento oscila conjunturalmente" (Aquino, 2024, p. 192).

Nessa feita, ao perpassar pela abordagem da inteligência enquanto uma política pública, faz-se necessário analisar como esse debate se encaixa, no contexto do ambiente cibernético, com suas respectivas ameaças à segurança. Como apresentado no

capítulo anterior, dentre as infraestruturas críticas reconhecidas pelo Estado brasileiro, tais como, "saúde, energia, defesa, transporte, telecomunicações, da própria informação entre outras (Canongia e Mandarino, 2009, p. 25), o governo federal também considera a segurança cibernética como "infraestrutura crítica da informação", pois essa política pública também apresenta impacto direto na segurança da sociedade e do Estado (Canongia e Mandarino, 2009, p. 27).

O espaço cibernético, portanto, particularmente após o fenômeno da *internet*, dos avanços tecnológicos, computacionais e mais recentemente, o *boom* das *AI's (artificial intelligence)*, tem contribuído para que a segurança cibernética seja uma prioridade dentre as políticas governamentais, visto que os ataques cibernéticos, os quais apresentam um desafio para a contrainteligência, podem afetar de maneira rápida e negativa o setor político, o sistema financeiro, entre inúmeros outros espaços da infraestrutura crítica governamental (Ferreira e Rodrigues, 2024, p. 257-258). O emblemático caso do vazamento de dados, ocorrido após a divulgação de Snowden em meados de 2013, pode ser considerado uma das ocorrências relacionadas ao espaço cibernético de natureza da área da Inteligência, que acabaram por afetar consideravelmente algumas infraestruturas críticas do governo brasileiro e até mesmo a relação do Brasil com os EUA (Fagundes *et al*., 2019).

Se por um lado o avanço tecnológico foi bem recepcionado e se mostrou favorável em vários aspectos, como já pontuado anteriormente (Canongia e Mandarino, 2009), por outro esse mesmo espaço pode ser utilizado para afetar a segurança de uma dada sociedade, Estado, setores e infraestruturas críticas de um dado governo. Pois o ciberespaço contribui para o anonimato, redução de riscos aos atacantes e amplificação do potencial de danos. Ou seja,

> a crescente possibilidade de anonimato no ciberespaço, combinada com a redução dos riscos para os atacantes, impulsiona ações maliciosas cada vez mais ousadas. No mundo digital, os ofensores operam com maior segurança, ocultando suas identidades e localizações, o que dificulta drasticamente o rastreamento e a retaliação imediata (Ferreira e Rodrigues, 2024, p. 257).

Nesse sentido, o meio digital contribui também, para que as consequências dos ataques sejam amplas, imediatas e quando de conhecimento do público, tome dimensões diversas, devido ao impacto que as mídias sociais possuem. Como exemplo, na época das delações de Snowden, a charge a seguir (Figura 2) foi uma das imagens que mais se popularizou, graças a atuação da mídia:

Figura 2 - Charge espionagem cometida ao governo de Dilma Rousseff

Fonte: Arruda, 2024

Logo, é notório o quanto a segurança cibernética, para além de ser uma política pública, deve ser considerada como "uma prioridade essencial para proteger a soberania nacional" (Ferreira e Rodrigues, 2024, p. 258). Visto que os fatores mencionados e a interconectividade das infraestruturas críticas, aumentam as vulnerabilidades da segurança e da manutenção da estabilidade política e econômica, se constituem desafios basilares da atividade de contrainteligência cibernética (Goldman e Maret, 2019 *apud* Ferreira e Rodrigues, 2024, p. 258), mostra-se assim, a necessidade de fortalecer a contrainteligência como um todo, como meio de mitigar cada vez mais, os iminentes ataques. Nesse sentido,

> a segurança cibernética e a contrainteligência precisam evoluir continuamente para acompanhar o ritmo das ameaças. Soluções que combinam criptografia avançada, algoritmos de detecção baseados em IA e desenvolvimento de padrões de segurança robustos tornam-se indispensáveis para proteger as informações sensíveis e resguardar a soberania dos Estados contra interesses adversos (Ferreira e Rodrigues, 2024, p. 258).

4 BRASIL E O VAZAMENTO DE DADOS

> O problema, porém, transcende o relacionamento bilateral de dois países. Afeta a própria comunidade internacional e dela exige resposta. As tecnologias de telecomunicação e informação não podem ser o novo campo de batalha entre os Estados. Este é o momento de criarmos as condições para evitar que o espaço cibernético seja instrumentalizado como arma de guerra, por meio da espionagem, da sabotagem, dos ataques contra sistemas e infraestrutura de outros países (Brasil, 2013).

Com essa fala, a presidente Dilma Rousseff, mediante ao recém acontecido caso do vazamento de dados em 2013, compareceu à 68º Assembleia Geral das Nações Unidas (AGNU) e, durante seu discurso, ressaltou em primeira mão, de maneira objetiva, como o ocorrido foi intransigente e desrespeitoso, e que, mediante isso, gostaria de propor algumas iniciativas para que a ONU, enquanto uma organização com capacidade de "desempenhar um papel de liderança no esforço de regular o comportamento dos Estados frente a essas tecnologias e a importância da *internet*, dessa rede social, para construção da democracia no mundo" (Brasil, 2013), pudesse de fato assim o agir. Nessa feita, o Brasil apresentou o marco civil para a governança e uso da *internet*, o qual ficou comumente conhecido como Marco Civil da *Internet*, com o intuito de preservar a proteção de todos os seus usuários.

O Brasil, alguns outros países da América Latina juntamente da China, Irã, Rússia e Paquistão, foram alvos da espionagem estadunidense durante anos, todavia, tal fato só tomou uma proporção considerável mediante a delação pública e inesperada de Edward Snowden, um ex-agente que prestava consultoria à NSA. Segundo ele, o Brasil ficou atrás somente do próprio EUA (Greenwald; Kaz; Casado, 2013 *apud* Spaniol, 2015). O documentário, Citizenfour (2014), produzido por Laura Poitras, a qual obteve acesso primário a Snowden e aos documentos juntamente de Ewen MacAskill e Glenn Greenwald, relata como Snowden obteve as provas da atuação das agências de espionagem estadunidense, bem como porque ele achou por bem divulgar tais provas supostamente sigilosas (Harding, 2014). Os EUA através de suas agências de espionagem, a saber, NSA e CIA, estavam não apenas infringindo a própria constituição do país ao espionar os cidadãos estadunidenses, como também, de acordo com Snowden, vinham espionando diversos países, aliados e não aliados. Dentre os não aliados, a justificativa amplamente utilizada e invariavelmente aceita era o terrorismo, mas e entre os aliados? Conforme as revelações, foi esclarecido que os EUA espionaram a América Latina não (apenas) para fim militar e de segurança no continente, mas, e

principalmente, em relação ao petróleo e à produção de energia (Documentário sobre Edward Snowden ganha prêmio internacional, 2014). Os arquivos ultrassecretos mostram a então presidente Dilma Rousseff, bem como seus assessores, sendo um dos alvos. Conforme o renomado repórter Glenn Greenwald apontou numa entrevista feita ao Fantástico:

> Os documentos mostram que foi feita espionagem de comunicações da presidente Dilma com seus principais assessores. Também é espionada a comunicação dos assessores entre eles e com terceiros. A apresentação secreta se chama "filtragem inteligente de dados: estudo de caso México e Brasil." Segundo a apresentação, o programa possibilita encontrar, sempre que quiser, uma "agulha no palheiro." O palheiro, no caso, é o volume imenso de dados a que a espionagem americana tem acesso todos os dias, espionando as redes de telefonia, internet, servidores de e-mail e redes sociais. A agulha é quem eles escolherem (Documentário sobre Edward Snowden ganha prêmio internacional, 2014).

Figura 3 - Snowden e o colunista Glenn Greenwald (Cena do documentário Citizenfour)

Fonte: Documentário sobre Snowden ganha prêmio internacional, 2014

Similarmente,

> arquivos fornecidos por Greenwald (...), mostravam que a NSA havia conseguido crackear a rede virtual privada da Petrobras, utilizando um programa secreto de codinome BLACKPEARL (Harding, 2014, p. 222).

Em um outro momento, o jornalista Greenwald complementa, em uma entrevista feita às Comissões do Senado e da Câmara, que o Brasil pode por meio de iniciativa do Congresso brasileiro descobrir as empresas nacionais que contribuíram para que a NSA

tivesse acesso por volta de 5 bilhões de dados e comunicações de empresas, cidadãos, bem como de atores e órgãos do governo brasileiro (Brasil, 2013).

Nessa feita, por conta de toda a repercussão gerada a partir das denúncias feitas por Snowden, e pelo fato de ter sua privacidade violada, bem como de outras figuras meritórias do governo, à exemplo dos outros integrantes, também alvos da espionagem, a presidente Dilma achou por bem cancelar, já às vésperas, o que seria a sua primeira visita oficial aos EUA (Canto, 2019, p. 6). Além do mais, a presidente Dilma viu a espionagem estadunidense "como uma violação escandalosa da soberania do Brasil" (Harding, 2014, p. 222). Ao tomar conhecimento da reação de Dilma, Obama tentou dissuadi-la da ideia, porém o fora em vão. O governo brasileiro declarou que "na falta de tempo para uma investigação oportuna [...] não há condições para que essa viagem seja feita" (Harding, 2014, p. 222).

O chefe de Estado, Luiz Inácio Lula da Silva, durante o seu mandato (2003-2011), adotou uma política a qual o aproximava mais dos países árabes, dentre eles o Irã, e ao fazer isso acabou por irritar Washington. Diferentemente do presidente anterior, Dilma buscou retomar a aproximação com os EUA, e chegou inclusive a receber o presidente Obama no Brasil. Conforme ficou esclarecido posteriormente,

> A NSA não tinha interesse nessas boas relações; os espiões norte-americanos estavam interessados no pensamento particular de Dilma. Um slide obtido pela Spiegel mostrava que analistas tinham obtido acesso a mensagens de Dilma. Fort Meade investigava "os métodos de comunicação e seletores associados da presidenta brasileira e de seus principais assessores", relatou a revista. A agência também havia descoberto outros "alvos de valor" dentro do círculo íntimo da presidenta (Harding, 2014, p. 221)

Nessa época, também, o então Ministro das Relações Exteriores do Brasil, Antonio Patriota, declarou que:

> O Governo brasileiro recebeu com grave preocupação a notícia de que as comunicações eletrônicas e telefônicas de cidadãos brasileiros estariam sendo objeto de espionagem por órgãos de inteligência norte-americanos. O Governo brasileiro solicitou esclarecimentos ao governo norte-americano por intermédio da Embaixada do Brasil em Washington, assim como ao Embaixador dos Estados Unidos no Brasil. O governo brasileiro promoverá no âmbito da União Internacional de Telecomunicações (UIT) em Genebra, o aperfeiçoamento de regras multilaterais sobre segurança das telecomunicações. Além disso, o Brasil lançará nas Nações Unidas iniciativas com o objetivo de proibir abusos e impedir a invasão da privacidade dos usuários das redes virtuais de comunicação, estabelecendo normas claras de comportamento dos Estados na área de informação e telecomunicações para garantir segurança cibernética que proteja os direitos dos cidadãos e preserve a soberania de todos os países (Governo brasileiro pede explicações aos EUA sobre espionagem, 2014).

Além dele, membros do Congresso Brasileiro e da Comissão Mista de Controle das Atividades de Inteligência[3], apresentaram seus respectivos pareceres perante o caso em questão. A deputada e vice-presidente da Comissão de Relações Exteriores, Perpétua Almeida, externou o seu desapontamento pelo fato da delação ter sido primariamente divulgada não pelo governo brasileiro ou órgãos responsáveis da Inteligência nacional, mas por terceiros:

> "Não podemos ser pegos de surpresa o tempo inteiro. Os ministros têm que prestar esclarecimentos ao Congresso. Temos que ter informações para poder ajudar a presidente Dilma, que está respaldada por seu Congresso. Os três Poderes têm que se unir porque, na minha opinião, isso é uma afronta à soberania do nosso país", disse a deputada (Brasil, 2013).

Para além das discussões correntes no âmbito nacional e internacional, o vazamento de dados abriu um debate sobre o quão preparado o Brasil estava quando o assunto era defender a si mesmo de ataques cibernéticos, visto que "são as falhas que chegam ao conhecimento público e motivam questionamentos políticos, investigações e reforma de sistemas e instituições dedicados à Atividade de Inteligência" (George e Bruce, 2008 *apud* Aquino, 2024, p. 197). Nesse sentido, se faz necessário buscar compreender como foi a atuação da ABIN, enquanto órgão responsável pela Inteligência e contrainteligência brasileira, e particularmente responsável pela Segurança cibernética como um todo, nesse período delicadamente crítico para o Brasil.

Ademais, do viés da Segurança e de Defesa cibernética do país, vale pontuar que a ABIN é apenas um entre os demais órgãos responsáveis desse setor, a saber, a Polícia Federal, o Ministério de Ciência e Tecnologia, o Departamento de Segurança da Informação e Comunicações do GSI e por fim, o Centro de Defesa Cibernética do Exército (CDCiber). Consoante a própria formação brasileira desse sistema, ou seja, de falta de "articulação institucionalizada", a dificuldade de lidar com o caso do vazamento de dados e a configuração em questão se mostrou quase palpável, o que fez com que fosse até mesmo considerado criar uma agência nacional de segurança cibernética (Moraes, 2013).

De acordo com os documentos divulgados, algumas infraestruturas críticas do governo, como o Ministério das Minas e Energia, a Petrobras e a presidente com os seus assessores, entre outros, foram alvos da espionagem estadunidense. Logo, consoante fala da presidente,

---

[3] Comissão integrada por deputados e senadores, constituída para tratar de matéria pertinente à competência do Congresso Nacional. Pode ter caráter permanente ou temporário (Brasil, 2013).

> Não se sustentam argumentos de que a interceptação ilegal de informações e dados destina-se a proteger as nações contra o terrorismo. O Brasil, senhor presidente, sabe proteger-se. Repudia, combate e não dá abrigo a grupos terroristas. Somos um país democrático, cercado de países democráticos, pacíficos e respeitosos do Direito Internacional. Vivemos em paz com os nossos vizinhos há mais de 140 anos. Como tantos outros latino-americanos, lutei contra o arbítrio e a censura e não posso deixar de defender de modo intransigente o direito à privacidade dos indivíduos e a soberania de meu país. Sem ele – direito à privacidade - não há verdadeira liberdade de expressão e opinião e, portanto, não há efetiva democracia. Sem respeito à soberania, não há base para o relacionamento entre as nações (Brasil, 2013).

Posto isso, algo que ficou em voga na época foi a prenúncia de uma possível "guerra cibernética", dado que de acordo com analistas e especialistas no assunto, ninguém está totalmente incólume da ação de Inteligência, seja ela legal, ilegal, interna ou externa. Conforme também ressaltado pelo consultor e pesquisador de segurança cibernética de órgãos governamentais, Adriano Cansiam, "como criamos dependência muito grande da rede, seja no comércio, no setor de serviços e entretenimento, se um ataque se prolongar, as consequências podem ser danosas (...), isso vai ser sentido em todo lado" (Moraes, 2013).

Outrossim, o Brasil, ainda durante o mandato da presidente Dilma Rousseff, em meados dos anos de 2015, esteve mais uma vez no epicentro de um ruído nacional e internacional, após o *WikiLeaks* divulgar uma lista de pessoas e locais brasileiros alvos da espionagem estadunidense desde as primeiras revelações feitas em 2013. Tal lista demonstrou que o telefone presidencial da ex-presidente Dilma juntamente de seus assessores de governo e cerca de 29 ministros e diplomatas brasileiros foram alvo da espionagem estadunidense (Lopes; Perfil, 2024). Desta vez, no entanto, a reação brasileira se mostrou mais branda em vista do primeiro vazamento de informações. Na primeira divulgação de espionagem acometida ao governo brasileiro ainda em 2013, a presidente Dilma Rousseff se mostrou mais descontente com o ocorrido e cancelou a sua primeira visita presidencial e oficial aos EUA (Canto, 2019, p. 6). Na segunda revelação feita em 2015 por Julian Assange, porta voz oficial do *WikiLeaks*, a presidente Dilma, já às vésperas novamente da sua visita oficial de fato aos EUA, procurou levar a circunstância de maneira mais pacífica, amigável e diplomática possível, demonstrando que tal situação era uma "questão do passado" (Lista revela 29 integrantes do governo Dilma espionados pelos EUA, 2015).

Assim, quando o *Wikileaks* e Edward Snowden fizeram as divulgações alarmantes sobre espionagens acometidas a alguns Estados aliados dos EUA, dentre eles o Brasil, diversas áreas do governo brasileiro se mostraram vulneráveis. Por

consequência, pode-se afirmar que algumas infraestruturas críticas do Brasil foram ameaçadas, pois tal dilema gerou um forte impacto nas esferas mencionadas anteriormente pelo GSI (Brasil, 2023b).

Consoante reflete Spaniol (2015), o Brasil foi sem dúvida um dos países mais vigiados, contando até mesmo com agentes da CIA e NSA em Brasília, responsáveis por coletar determinadas informações e passar aos EUA (Spaniol, 2015). O fator econômico, conforme pontua Greenwald se qualifica portanto como o motivo mais plausível pelos EUA para justificar tal atitude:

> Greenwald diz que os Interesses dos Estados Unidos nas Informações brasileiras são comerciais. O Brasil é rico em recursos naturais e isso gera muito dinheiro — pelas reservas de petróleo marinhas e do pré-sal, por exemplo. Ter acesso às informações antes que outros países pode favorecer (e muito) os investidores norte-americanos. Além disso, com esses dados a competição internacional também pode ser vencida mais facilmente (Hamann, 2013 *apud* Spaniol, 2015, p. 96).

Outrossim, Greenwald complementou, em entrevista ao Fantástico, que o Brasil possivelmente virou um dos alvos, após ter galgado uma posição bastante considerável dentro do cenário global, logo, isso pode ter contribuído para que os EUA se sentisse relativamente ameaçado e preocupado com a estabilidade da região de seu domínio. Afinal, o Brasil seria amigo, inimigo ou problema? (Entenda o caso de Edward Snowden que revelou espionagem dos EUA, 2013) Ou ainda, “aminimigo”? Em suma, uma das interpretações sobre o assunto concluiu que os EUA praticou a denominada espionagem industrial, algo praticado pelos russos e chineses e supostamente repudiado pelos EUA. A NSA chegou a declarar ao *Washington Post*: “o departamento não se envolve em espionagem econômica em qualquer domínio, incluindo o cibernético” (Harding, 2014, p. 222).

Ademais, conforme as fontes divulgaram, o Brasil foi espionado particularmente via *internet*, logo, tal evento “resultou em disputas junto ao governo norte-americano relacionadas ao setor de informática” (Canto, 2019, p. 5). Tal ação demonstra fortemente, conforme já pontuado por Miranda Filho (2012), que uma parte da infraestrutura crítica do governo brasileiro se colocou por diversos motivos em situação de vulnerabilidade. Conforme pontuado por Canto:

> Como fator agravante, a privatização das telecomunicações em 1990 acabaram por enfraquecer não só um setor estratégico do país mas a indústria nacional de produtos de comunicação e informática, facilitando a entrada de agentes estrangeiros nos meios de comunicação brasileiros, assim como o acesso a dados pessoais dos cidadãos (Canto, 2019, p. 5).

Nesse viés, além do fato de não haver uma legislação internacional específica

que regulamenta a espionagem e inteligência em si, como particularmente também a ciberespionagem, e o fato do Brasil ter terceirizado um dos seus serviços essenciais facilitou para que o caso tomasse as proporções que tomou, gerando impactos posteriores e inclusive no meio internacional. Em resposta, a chefe do Estado brasileiro na época tomou algumas medidas mediante a ascensão do escândalo, e reiterou "a necessidade do Brasil de se envolver mais em legislações, tecnologias e mecanismos que protegessem o país de interceptações ilegais (...)" (Canto, 2019, p. 6).

No tocante à vulnerabilidades da estrutura brasileira consoante a defesa cibernética, o general do Centro de Defesa Cibernética do Comando do Exército, José dos Santos, na época, afirmou que o problema e motivo principal, para o Brasil não ter se defendido conforme deveria, foi pelo fato da "dependência de tecnologia estrangeira", e ressaltou, que tal dilema não seria fácil e prontamente superado. O general salientou que a parceria do governo com empresas e até mesmo universidades, no intuito de aprimorar a defesa cibernética seria de grande valia. Por fim, ele defendeu a aprovação do Marco Civil da *Internet* como também "a criação de uma agência nacional de segurança cibernética para regular e coordenar o setor" (Brasil, 2013).

Em adicional a isso, Cepik, logo após a divulgação do caso, foi convidado para uma entrevista a respeito desse assunto. Na entrevista, entre outras questões, ele também enfatizou a importância e urgência do Brasil aprender com suas "vulnerabilidades, melhorar a proteção de conhecimentos sensíveis e infraestrutura críticas". E ao concluir ressaltou:

> Nesse sentido, além de cobrarmos explicações do governo norte-americano, é importante termos maior explicitação governamental acerca das missões, recursos, requisitos, qualidade analítica esperada e controles democráticos das providências de contrainteligência e segurança informacional dos órgãos responsáveis no Estado brasileiro (Ivanissevic, 2013, p. 8).

Em suma, aponta-se que "o caso Snowden serviu não só para uma mudança de estratégias e infraestrutura do ciberespaço brasileiro, mas também como um catalisador da elaboração e aprovação do Marco Civil da *Internet*" (Canto, 2019, p. 6-7). A reação do Brasil foi diversa, porém, o ministro da justiça na época, José Cardozo, ao reunir com a presidente Dilma, deixou claro que o governo brasileiro tomou as três medidas seguintes: convocação do embaixador norte americano no Brasil, Thomas Shannon; cobrou explicações formais dos EUA; e em terceiro, recorreu aos órgãos internacionais, como a ONU, para resolver a violação de direitos acerca da privacidade dos cidadãos, autoridades e órgãos do governo. Conforme fala de Dilma Rousseff na ONU:

> Estamos, senhor presidente, diante de um caso grave de violação dos direitos humanos e das liberdades civis; da invasão e captura de informações sigilosas relativas as atividades empresariais e, sobretudo, de desrespeito à soberania nacional do meu país. Fizemos saber ao governo norte-americano nosso protesto, exigindo explicações, desculpas e garantias de que tais procedimentos não se repetirão (Brasil, 2013).

Em resposta, e mediante uma visita do secretário de Estado dos EUA, John Kerry, para averiguar a espionagem e restabelecer as conexões entre ambos os países, o secretário em questão pontuou que iria buscar entrar num acordo com o Brasil, usando como premissa a busca pela segurança dos brasileiros e de demais pessoas do mundo. Em contrapartida, o chanceler brasileiro, Antonio Patriota, comentou:

> Enfrentamos hoje um novo tipo de desafio em nossa relação bilateral, um desafio relacionado à notícia de interceptações de comunicações eletrônicas e telefônicas de brasileiros. E caso as implicações desses desafios não sejam resolvidas de modo satisfatório, corre-se o risco de se projetar uma sombra de desconfiança sobre o nosso trabalho (Alcântara, 2013).

Patriota também ressaltou que se fazia mais do que

> "necessário descontinuar práticas atentatórias à soberania, à relação de confiança entre os Estados, e violatória das liberdades individuais que nossos países tanto prezam". "O que nós consideramos é que os EUA não encontrarão melhor parceiro no combate do terrorismo internacional, à medida que as parcerias sejam levadas a cabo de forma transparente (Alcântara, 2013).

O artigo Vigilância cibernética no Brasil: O caso Snowden sob o PRISMa de um insider, de Gills Vilar Lopes, em consonância com o livro do Jorge Bessa, O escândalo da espionagem no Brasil, sendo esse último divulgado em período recente ao vazamento de dados de 2013, aponta que o programa PRISM, vulgo "palheiro", conforme posto por Glenn Greenwald anteriormente, foi utilizado pela CIA e NSA, para filtrar dados via *internet*, através de grandes grupos dessa maior rede mundial, a saber, *Facebook*, *Microsoft*, *Apple* e *Google*. A espionagem em questão, ou precisamente, o seu escândalo, contribuiu para que diversos atores ficassem em situação desconfortável quando não vulnerável, e dessa feita, criar meios de se protegerem nos organismos internacionais e ainda, dar iniciativas a um mecanismo de proteção internacional, tal como o Brasil fez com o Marco Civil da *Internet* em 2013 (Canto, 2019, p. 6-7). Assim, "as atividades de Inteligência compreendem *método* para subsidiar o principal tomador de decisão do Estado nacional, razão porque é um instrumento, e não um fim em si mesmo" (Lopes, 2015, p. 263).

No livro *A arte da Guerra*, Sun Tzu (2016) argumenta acerca da espionagem que "os espiões são a essência da arte da Guerra (...)" (p. 76) e, por conseguinte, tal atividade se mostra imprescindível para o auxílio das tomadas de decisões conforme já

visto, como também, para atingir da melhor forma possível, os objetivos de interesses do Estado que pratica tal arte, por assim dizer. Nesse sentido, reitera-se que os EUA foram sagaz ao utilizar os programas airview e PRISM para atingir seus intentos, sejam eles meramente econômicos, comerciais, preventivo, rotineiro ou ainda de caráter à Guerra ao Terror, dado então, aos 2 anos do ataque às Torres Gêmeas, o qual ocorreu em setembro de 2011. Nesse sentido, "a espionagem provê informações valiosíssimas para os que tomam decisões estratégicas, não importando em que época vivam" (Lopes, 2015, p. 263). Em outras palavras, Sun Tzu reafirma, "sê sutil! sê sutil! E use espiões para toda a sorte de negócios" (2016, p. 75).

O autor Jorge Bessa, ex-oficial de Inteligência da ABIN, no terceiro capítulo de sua obra, complementa pontuando que os cabos de submarinos brasileiros, situados à costa brasileira, seriam de fato o motivo pelo qual os EUA investiram recursos e também perderam tempo, espionando a chefe do Estado brasileiro, seus assessores entre outros órgãos já mencionados da infraestrutura crítica brasileira, desvinculando assim, a premissa do terrorismo amplamente utilizada pelos EUA. Ademais, Jorge Bessa chama atenção do governo brasileiro ao contribuir com tal inferência, pois "a questão nos cabos submarinos que cruzam o país" deveria ser incrementada e olhada com mais atenção pelo governo local, sobretudo inserido à agenda estratégica de defesa nacional. Por fim, Jorge Bessa, no último capítulo de sua obra, reitera uma observação já pontuada anteriormente neste presente trabalho, que não é hora mais do governo brasileiro relegar a ameaça existente da inteligência externa, sobretudo cibernética e que, portanto, deve melhor se estruturar em todos os âmbitos possíveis, para minimizar suas vulnerabilidades ao mesmo tempo que busca se aprimorar na sua defesa de tais iminentes, e cada vez mais recorrente, ataques (Lopes, 2015, p. 264).

Uma medida prática para além do Marco Civil da *Internet,* o Brasil também, propôs criar ainda em 2014, um centro de certificação de equipamentos com o intuito de certificar certos equipamentos para evitar que espionagens, como as reveladas por Snowden, ocorram novamente, como também, poder melhor supervisionar as informações e a segurança no Brasil. Essa iniciativa foi encabeçada por Sinclair Mayer, Chefe do departamento de Ciência e Tecnologia do exército. Em complemento, Raphael Mandarino Junior, diretor do Departamento de Segurança da Informação e Comunicação (DSIC) do GSI, pontuou que o órgão registrava na época em média 2100 incidentes por hora nas redes de *internet* do governo e ressaltou que boa parte desses incidentes, eram tentativas de coleta de informações. Inclusive, alguns dos algoritmos

utilizados, na solução de tais incidentes, foram elaborados em conjunto com a Abin. Conforme ele próprio enfatizou, “há algoritmos usados há cerca de 12 anos sem que nunca tenham sido quebrados” (Brasil terá centro de certificação para evitar espionagem, 2013). Por fim, em relação a isso, consoante Otávio da Silva, diretor do Centro de Pesquisas e Desenvolvimento para Segurança das Comunicações da Abin,

> um dos algoritmos citados por Mandarino protege há três anos as comunicações do Estado brasileiro. "O domínio de tecnologias é a grande solução (para evitar problemas de monitoramentos indesejados de informações do Estado)" (Brasil terá centro de certificação para evitar espionagem, 2013)

5 CONSIDERAÇÕES FINAIS

Consoante todo o exposto, e a ordem dos fatos, é possível observar como este trabalho introduziu alguns conceitos principais e imprescindíveis para a compreensão do caso analisado. À priori, foi necessário conceituar o que as Relações Internacionais, ou precisamente, as três teorias basilares que norteiam essa área do saber -realismo, liberalismo e construtivismo- conceituam como Segurança. Posteriormente, é trazido pelo autor Marcos Degaut Pontes, como essas três teorias são classificadas em grupos, e como esse trabalho se enquadra dentro do terceiro grupo, os chamados "ampliadores/alargadores" (Pontes, 2015). Após isso, há a junção da segurança ao debate da Inteligência, concebendo na chamada "*Security Intelligence*" ou "Segurança da Inteligência", e de fato há uma aproximação, pois os autores que analisam essas duas áreas, inicialmente separadas, reconhecem a dependência e complementaridade existente entre elas (Cepik, 2003).

Tendo feito essa breve introdução, a inteligência, outro conceito tão importante quanto a Segurança, também é debatido. Marco Aurélio Cepik, um dos autores mais conceituados em matéria de Inteligência da atualidade brasileira, apresenta suas contribuições para a vertente em questão e ao apresentar sua conceituação, aqui de maneira objetiva como conhecimento ou informação, a complementa em momentos posteriores subdividindo-a em operações, categorias e em suas diversas fontes. Dentre as contribuições de Cepik, pontua-se que particularmente neste trabalho acadêmico, consoante os estudos e leituras realizados, o caso do vazamento de dados, se encaixa nas categorias de inteligência científica/tecnológica e de inteligência econômica. Quanto às operações, o caso em questão abarca os níveis transnacionais, visto que os EUA usou diversas vezes a premissa do terrorismo Como também, abrange o nível nacional, por conta do envolvimento de vários Estados e inclusive do próprio EUA. Por fim, no que tange às fontes, destaca-se a Osint, a qual está estritamente ligada à *internet* e logo, ao modelo que este caso se desenvolve (Cepik, 2003).

Mediante o apresentado, Miranda Filho (2012) introduz um conceito basilar, chamado infraestruturas críticas (IC). Conforme já visto, é tudo aquilo que tem capacidade de causar impacto considerável no âmbito político, econômico, internacional, social e na própria segurança. Logo, consoante esse autor, atuar para a proteção e salvaguarda da Segurança significa atuar na proteção das infraestruturas críticas e vice-versa. Em complemento a isso, Cepik (2003) ressalta portanto, que a

segurança está estritamente relacionada à existência de segredo e da ameaça, ou seja, para ele, os "ordenamentos constitucionais" são capazes de gerar respostas e de agir conforme o tanto que são ameaçados. Em suma, ambos os autores reconhecem a importância da inteligência como forma de assegurar a Segurança, voltando ao ponto anteriormente falado, que, ambas (Inteligência e Segurança) se complementam.

Posto isso, adentra-se num conceito de suma relevância para o escopo desse caso, que é a contrainteligência. Na qual, essa atividade é imprescindível para garantir a segurança, os interesses bem como, fazendo o possível para impedir ameaças, terrorismo, vazamento de dados ou informações, sabotagem entre outros, que tendem a ir contra o interesse nacional. Outrossim, dentre os segmentos da contrainteligência, a saber, o segmento da segurança ativa e segurança orgânica, pontua-se que o segmento da segurança orgânica, se mostrou mais vulnerável após as delações de Snowden, visto que foi justamente o setor de instalações, tecnologia da informação, pessoal, documentos entre outros, que tiveram sua proteção inviolada. Ou seja, a atuação de prevenção e obstrução, essas de responsabilidade do segmento da segurança orgânica, se mostraram por algum motivo insuficientes (Brasil, 2020d; Baptistella e Vianna, 2022).

Para além da contrainteligência, a segurança cibernética é um outro conceito que tem ganhado cada vez mais espaço nas agendas internacionais. Graças ao surgimento da *Internet* e crescente desenvolvimento das TICs, os setores desde os mais básicos e essenciais, até os de acesso privativo ou de figuras chaves governamentais, estão aderindo a uma senão as duas vertentes (Tics e *Internet*). Principalmente devido ao avanço tecnológico, visto que esse impacta consideravelmente a vida cotidiana da sociedade. Nesta feita, partindo da concepção do que vem a ser segurança cibernética para a perspectiva brasileira, nota-se que essa também falhou quando não protegeu suficientemente "o espaço cibernético brasileiro, os ativos de informação e suas infraestruturas críticas" (Mandarino, 2009, p. 29), das atividades de espionagem das agências estadunidenses, como da CIA e da NSA. Em adição, é levantado como questão que, a ausência de uma estrutura ou órgão capaz de cuidar de todas as nuances e frentes que essa área exige, seria um dos motivos que dificultaram a eficiência da segurança cibernética no contexto em análise. Todavia, conforme já pontuado, tal advento contribuiu fortemente para que o Brasil retomasse as prioridades nesse assunto (do ciberespaço brasileiro), dando origem assim ao Marco Civil da *Internet*, no mesmo ano do ocorrido (Canongia e Mandarino, 2009).

Feito isso, se viu a necessidade de apresentar como se dá o funcionamento do sistema de Inteligência do Brasil. Para melhor compreensão, decidiu-se que o mais ideal seria fazer uma retomada histórica de como foi esse processo de consolidação como um todo, desde o seu tenro início até o contexto atual. Para tanto, foi utilizado bibliografia que provesse esse arcabouço teórico desde o final do século XIX, período este que corresponde à Primeira República brasileira, perpassando pelo século XX e chegasse até o presente século. Disso, ressalta-se que o primeiro órgão de Inteligência que se considera como oficial, foi a Inspetoria de Investigação e Segurança Pública, fundada durante o mandato de Epitácio Pessoa em 1920. Após essa inspetoria, como a bibliografia mostra e o capítulo II deste trabalho, reconta, houve inúmeros acontecimentos de cunho social, político, internacional, econômico *etc*, que motivaram as inúmeras transformações pelas quais o sistema de inteligência brasileiro passou. Um dos fatos mais marcantes e contributivos para a consolidação desse sistema, foi a ditadura, pois ela atuou como um divisor de águas no que tange a estruturação das instituições governamentais, dentre elas, a da Inteligência. Contribuindo também para que o termo informação, frequentemente utilizado antes da ditadura, adquirisse por fim, a terminologia "inteligência", já utilizada em vários outros países. Para mais, no final da década de 90 é que se tem o início oficial do SISBIN e do órgão central responsável desde então, por "planejar, executar, coordenar, supervisionar e controlar as atividades de Inteligência no país" (Lei nº 9883, art. 3º; Brandão e Quadrat, 2024).

Adicionalmente, após entender como se deu a consolidação do sistema de inteligência, a critério de aprimoramento, se fez necessário buscar entender como ocorre a atividade em si dentro da conjuntura brasileira, particularmente enquanto política pública com impacto considerável às IC. Logo, consoante a literatura pertinente, é possível aferir que sem o fenômeno das ameaças que provocam reações e respostas do governo, o Brasil, difícil ou mais tardiamente teria tomado algumas medidas que tomou, para assegurar a segurança em termos de Inteligência no Estado. Certamente, o avanço das TICs contribuiu para uma estruturação e melhorias das IC do governo, todavia, por outro lado, deixou margem para que em algum dado momento, as mesmas infraestruturas se vissem em situação delicada, devido a problemas estruturais, políticos, orçamentários, dependência sobretudo tecnológica externa *etc*. Enfim, foi possível ressaltar o quanto priorizar a segurança cibernética, enquanto uma "infraestrutura crítica da informação" e política pública, se mostra crucial para dirimir as vulnerabilidades da

segurança de um dado Estado (Canongia e Mandarino, 2009; Aquino, 2024; Ferreira e Rodrigues, 2024).

A critério de especificidade, analisou-se de maneira mais precisa os acontecimentos do caso em voga, dando atenção particular a reação do governo brasileiro, mediante o ocorrido. Após a divulgação do caso, algumas medidas foram tomadas dada a urgência e impacto da delação. Cita-se de maneira objetiva e resumida algumas dessas, 1. o cancelamento da primeira visita oficial da presidente da República do Brasil aos EUA; convocação do embaixador norte americano no Brasil, Thomas Shannon, buscando por respostas oficiais e formais dele e do governo estadunidense; 2. movimentação no âmbito interno, para dirimir as consequências do dilema gerado, seja na priorização de medidas que regulamenta e reestrutura o funcionamento das áreas de inteligência, segurança e sobretudo de equipamentos de defesa nacional e das redes do espaço cibernético; 3. Promoção, discurso e aprovação do Marco Civil da *Internet* na legislação nacional e na ONU; 4. Retomada das relações com os EUA (Canto, 2019, Harding, 2014; Spaniol, 2015; Brasil, 2013).

Ao retomar a pergunta central deste trabalho, "Como o Sistema de Segurança de Inteligência Brasileiro lidou com o dilema do vazamento de dados durante o mandato da Presidente Dilma Rousseff no período entre 2013-2015?", se faz possível aferir que o campo acadêmico das Relações Internacionais, ou mais especificamente, alguns dos seus debates, se mostram imprescindíveis para a análise do conteúdo, pesquisa e para melhor elucidação do caso em questão. Portanto o emblemático caso do vazamento de dados ocorrido no período entre 2013-2015, durante o mandato de Dilma Vana Rousseff, se configura como o caso ideal, que ao articular os conceitos e bibliografia utilizados, pode contribuir para enfatizar as contribuições e o papel que as Relações Internacionais tem, sobretudo em assuntos de matéria de Segurança, Inteligência, relações políticas, questões estruturais e governamentais, e em assuntos de grande debate na agenda contemporânea internacional, como o é da Segurança Cibernética. Consoante todo o exposto, a presente monografia buscou na medida do possível, apresentar contribuições à ciência das Relações Internacionais, bem como utilizar seus pressupostos teóricos para compreender melhor o caso, ao mesmo tempo que introduziu alguns conceitos, à perspectiva do campo em questão. Nessa feita, acredita-se que o objetivo geral tenha sido atingido, se mantendo aberto a possíveis e novas contribuições, que venham complementar e aprimorar este estudo.

REFERÊNCIAS BIBLIOGRÁFICAS

AGÊNCIA BRASILEIRA DE INTELIGÊNCIA (ABIN). **Doutrina da Atividade de Inteligência**. Brasília, DF: ABIN, 2023. Disponível em: https://www.gov.br/abin/pt-br/centrais-de-conteudo/doutrina/Doutrina-da-Atividade-de-Inteligencia-2023. Acesso em: 14 mar. 2025.

ACHARYA, Amitav. The third world and security studies. *In* Christopher W. Hughes e Yew Meng Lai (org), **Security Studies**. Routledge, 2011. p. 52-63. Disponível em: https://yciss.info.yorku.ca/files/2012/06/OP28-Acharya.pdf. Acesso em: 12 fev. 2025.

AGIUS, Christine et al. Social constructivism. **Contemporary security studies**, v. 3, p. 87-103, 2013.

ALCÂNTARA, Diogo. **Apesar de pedido de Patriota, Kerry diz que EUA manterão espionagem.** Jornal de Notícias, 13 Ago. 2013. Disponível em: https://www.terra.com.br/amp/noticias/brasil/apesar-de-pedido-de-patriota-kerry-diz-que-eua-manterao-espionagem,8cf404f3a6870410VgnVCM4000009bcceb0aRCRD.html. Acesso em: 25, Mar. 2025.

ALVARES, Lillian. **Segurança cibernética, segurança da informação, proteção do conhecimento e contrainteligência**. Brasília: Universidade de Brasília, 2024. Disponível em: http://lillianalvares.fci.unb.br/phocadownload/GIGCIC/InteligenciaCompetitiva/Aula43Protecao.pdf. Acesso em: 10 fev. 2025.

ANNAN, Kofi. Larger Freedom: Towards Development, Security and Human Rights for All. **Report of the Secretary-General**, 2005. Disponível em:http://www.ohchr.org/Documents/ Publications/A.59.2005. Add.3.pdf. Acesso em: 10 fev. 2025.

AQUINO, Rodrigo de. A Inteligência como política pública: desafios para a ABIN. *In* ABIN (org.), **Desafios e perspectivas para a Agência Brasileira de Inteligência – Inteligência na Democracia,** Cap. 6. Disponível em: https://repositorio.enap.gov.br/bitstream/1/8217/1/ABIN_Inteligencia_na%20_Democracia.pdf . Acesso em: 20 fev. 2025.

ARAUJO, Raimundo Teixeira de. **História secreta dos serviços de inteligência.** São Luís: CEADERMA, 2004. 204 p.

ARRUDA, Giovana. Notícias. **Espionagem do governo brasileiro: relembre vazamentos famosos do *WikiLeaks*.** *UOL*, 27 jun. 2024. Disponível em: https://noticias.uol.com.br/internacional/ultimas-noticias/2024/06/27/espionagem-do-governo-brasileiro-relembre-vazamentos-famosos-do-wikileaks.htm?cmpid=copiaecola. Acesso em: 29 mar. 2025.

BAPTISTELLA, Luis Fernando; VIANNA, Nilson Rocha. A contrainteligência e a cyberspionagem. **Adepol MS,** 2022. Disponível em: <https://adepolms.org.br/a-contrainteligencia-e-a-cyberespionagem/> . Acesso em: 14 fev. 2025.

BALDWIN, David A. The Concept of Security. **Review of International Studie**s, n. 23, p. 5-26, 1997. Disponível em: https://dbaldwin.scholar.princeton.edu/sites/g/files/toruqf4596/files/dbaldwin/files/baldwin_1997_the_concept_of_security.pdf. Acesso em 14 de fev. 2025

BRANDÃO, Priscila; QUADRAT, Samantha. Uma era de transição: entre o SNI e a ABIN. *In:* AGÊNCIA BRASILEIRA DE INTELIGÊNCIA-ABIN (org). **Inteligência na democracia: desafios e perspectivas para a Agência Brasileira de Inteligência.** Brasília, DF: Editora Esint, 2024. p. 108. Disponível em: https://www.gov.br/abin/pt-br/centrais-de-conteudo/inteligencia-na-democracia/inteligencia-na-democracia-abin-2024.pdf. Acesso em: 22 mar. 2025.

BRANDÃO, Priscila Carlos e CEPIK, Marco. Brazil´s new intelligence system: an institutional assessment. **International Journal of Intelligence and Counterintelligence**, New York, v.16, n.03, p.110, 2003. Disponível em: https://www.researchgate.net/publication/233212809_Brazil's_New_Intelligence_System_An_Institutional_Assessment. Acesso em: 22 mar. 2025.

BRASIL. **Brasil pode descobrir quais empresas colaboraram com espionagem dos EUA, diz jornalista**. Agência Câmara de Notícias, 6 Ago. 2013. Disponível em: https://www.camara.leg.br/noticias/410791-brasil-pode-descobrir-quais-empresas-colaboraram-com-espionagem-dos-eua-diz-jornalista/. Acesso em: 20 mar. 2025.

BRASIL. **Diretor diz que Abin não realiza escutas telefônicas**. Agência Câmara de Notícias, 28 Fev. 2008. Disponível em: https://www.camara.leg.br/noticias/113895-diretor-diz-que-abin-nao-realiza-escutas-telefonicas/.

BRASIL. **Líder do governo propõe nota de repúdio aos EUA por espionagem a Dilma.** Agência Câmara de Notícias, 02 Fev. 2013. Disponível em: https://www.camara.leg.br/noticias/413494-lider-do-governo-propoe-nota-de-repudio-aos-eua-por-espionagem-a-dilma/.

BRASIL. **Fragilidade brasileira à espionagem não será superada de imediato, diz general**. Agência Câmara de Notícias, 02 Out. 2013. Disponível em: https://www.camara.leg.br/noticias/416660-fragilidade-brasileira-a-espionagem-nao-sera-superada-de-imediato-diz-general .

BRASIL**. Decreto n.º 8.793, de 29 de junho de 2016.** Fixa a Política Nacional de Inteligência. Brasília, DF: Presidência da República, 2016. Disponível em: https://www.planalto.gov.br/CCiViL_03/_Ato2015-2018/2016/Decreto/D8793.htm. Acesso em: 16 fev. 2025.

BRASIL**. Decreto n.º 68.448, de 31 de março de 1971.** Dispõe sobre a organização e funcionamento do Serviço Nacional de Informações (SNI). Diário Oficial da União, Brasília, DF, 1º abr. 1971. Disponível em: https://www2.camara.leg.br/legin/fed/decret/1970-1979/decreto-68448-31-marco-1971-456468-publicacaooriginal-1-pe.html. Acesso em: 16 fev. 2025.

BRASIL. **Lei nº 9.883, de 7 de dezembro de 1999. I**nstitui o Sistema Brasileiro de Inteligência, cria a Agência Brasileira de Inteligência - ABIN, e dá outras providências. Gov.br, Brasília, DF 1999. Disponível em: <https://www.planalto.gov.br/ccivil_03/leis/l9883.htm>. Acesso em: 12 fev. 2025.

BRASIL**. Projeto de Lei n.º 1.862, de 1991.** Dispõe sobre a criação e organização do Sistema Brasileiro de Inteligência e dá outras providências. Diário da Câmara dos Deputados, Brasília, DF, 1991.

BRASIL**.** Presidente da República. **Discurso da presidenta da República Dilma Rousseff na abertura do debate geral da 68ª Assembleia Geral das Nações Unidas**. Brasília, 2013. Disponível em: https://www.gov.br/mre/pt-br/centrais-de-conteudo/publicacoes/discursos-artigos-e-entrevistas/presidente-da-republica/presidente-da-republica-federativa-do-brasil-discursos/dilma-vana-rousseff-2011-2016/discurso-da-presidenta-da-republica-dilma-rousseff-na-abertura-do-debate-geral-da-68-assembleia-geral-das-nacoes-unidas. Acesso em: 28 fev. 2025.

BRASIL. **Estratégia de segurança da informação e comunicações e de segurança cibernética da administração pública federal 2015-2018 Presidência da República. Gabinete de Segurança Institucional.** v. 1.0 / Gabinete de Segurança Institucional, Secretaria-Executiva, Departamento de Segurança da Informação e Comunicações. – Brasília : Presidência da República, 2015c. Disponível em: <https://www.gov.br/gsi/pt-br/arquivos/4_estrategia_de_sic.pdf> . Acesso em: 14 fev. 2025.

BRASIL. Agência Brasileira de Inteligência. **Revista Brasileira de Inteligência,** v. 1, n. 1, 2025. Disponível em: https://www.gov.br/abin/pt-br/centrais-de-conteudo/revista-brasileira-de-inteligencia/RBI1.pdf. Acesso em: 28 fev. 2025.

BRASIL. **Contrainteligência.** Gov.br, Brasília, DF 2020. Disponível em: <https://www.gov.br/abin/pt-br/assuntos/inteligencia-e-contrainteligencia/CI> . Acesso em 11 fev. 2025.

BRASIL. **Agência Brasileira de Inteligência. Membros do Congresso comparecem à ABIN para discutir soberania nacional.** Gov.br, 14 set. 2023a. Disponível em: https://www.gov.br/abin/pt-br/centrais-de-conteudo/noticias/membros-do-congresso-comparecem-a-abin-para-discutir-soberania-nacional. Acesso em: 13 out. 2024.

BRASIL. **Gabinete de Segurança Institucional**. Segurança de infraestruturas críticas. Gov.br, Brasília, DF 2023b. Disponível em: https://www.gov.br/gsi/pt-br/assuntos/seguranca-de-infraestruturas-criticas. Acesso em: 16 ago 2024.

BRAUCH, Hans G, *et al*. **Coping with global environmental change, disasters and security : threats, challenges, vulnerabilities and risks**. Berlin: Springer, 2011, p. 101-106.

BUZAN, Barry. **People, states and fear: An agenda for international security studies in the post-Cold War era.** Harvester Wheatsheaf, 1991.

CANONGIA, Claudia; MANDARINO, Raphael Junior. Segurança cibernética: o desafio da nova Sociedade da Informação. **Parcerias Estratégicas**, Brasília, DF. V. 14, n. 29, p.21-46, jul./dez. 2009. Disponível em: <https://cdi.mecon.gob.ar/bases/doc/parceriasest/29.pdf#page=23>. Acesso em: 18 fev. 2025.

CANTO, MARIANA. Made in Surveillance: A regulação da importação e do uso de tecnologias de vigilância estrangeiras e a relativização dos direitos fundamentais e da soberania estatal. **IV Simpósio internacional Lavits,** p. 11, 2019. Disponível em: https://lavits.org/wp-content/uploads/2019/12/Canto-2019-LAVITS.pdf. Acesso em: 10 set 2024.

CEPIK, M. Inteligência e Políticas Públicas: dinâmicas operacionais e condições de legitimação. **Security and Defense Studies Review,** v. 2, p. 246, 2002. Disponível em: https://professor.ufrgs.br/sites/default/files/marcocepik/files/cepik_-_2002_-_intel_e_pol_pub_-_sec_and_def_review.pdf. Acesso em: 06 fev. 2025.

CEPIK, M. **Espionagem e democracia.** Rio De Janeiro: Fgv, 2003.

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

DESOLDA, Giuseppe et al. Human factors in phishing attacks: a systematic literature review. **ACM Computing Surveys (CSUR)**, v. 54, n. 8, p. 1-35, 2021. Disponível em: https://dl.acm.org/doi/abs/10.1145/3469886. Acesso: em: 12 fev. 2025.

Documentário sobre Edward Snowden ganha prêmio internacional. **G1**, 02 dez. 2014. Disponível em: https://g1.globo.com/pop-arte/noticia/2014/12/documentario-sobre-edward-snowden-ganha-premio-internacional.html. Acesso em: 19 mar. 2025.

Entenda o caso de Edward Snowden, que revelou espionagem dos EUA. G1, 02 jul. 2013. Disponível em: https://g1.globo.com/mundo/noticia/2013/07/entenda-o-caso-de-edward-snowden-que-revelou-espionagem-dos-eua.html .Acesso em: 20 mar. 2025.

FAGUNDES, George et al. A cooperação internacional entre Brasil e Estados Unidos em matéria de Segurança e Defesa cibernética. XVI Congresso Acadêmico de Defesa Nacional (CADN), Rio de Janeiro. **Anais** [...]. Rio de Janeiro: Escola Naval . Março, 2019. Disponível em: https://www.gov.br/defesa/pt-br/arquivos/ajuste-01/ensino_e_pesquisa/defesa_academia/cadn/artigos/xvi_cadn/aa_cooperaaoa_internacionala_entrea_brasila_ea_estadosa_unidosa_ema_materiaa_dea_segurana.pdf . Acesso em: 12 ago. 2024.

FERREIRA, Juliano Rodrigues. RODRIGUES, Cristina C. Fonseca. Desafios tecnológicos emergentes: impactos para a Contrainteligência e a resposta a Ameaças Cibernéticas e Interesses adversos. *In* ABIN (org). **Inteligência na Democracia: Desafios e perspectivas para a Agência Brasileira de Inteligência.** Escola de Inteligência, 2024. p. 257-280 Disponível

em:https://repositorio.enap.gov.br/bitstream/1/8217/1/ABIN_Inteligencia_na%20_Democracia.pdf . Acesso em 20 fev. 2025.

GEORG, et al. Os desafios da Segurança Cibernética no setor público federal do Brasil: estudo sob a ótica de gestores de tecnologia da informação. **Revista Ibérica de Sistemas e Tecnologias de Informação**, p. 602-616, maio/jul, 2022. Disponível em: https://ppee.unb.br/wp-content/uploads/2023/07/Os-desafios-da-Seguranca-Cibernetica-no-setor-publico-federal-do-Brasil-estudo-sob-a-otica-de-gestores-de-tecnologia-da-informacao.pdf. Acesso em: 19 fev. 2025.

GEORGE, R. Z.; BRUCE, J. B. (ed.). **Analyzing Intelligence: origins, obstacles, and innovations.** Georgetown University Press: 2008.

GOLDMAN, J.; MARET, S. **Intelligence and Information Policy for National Security: Key Terms and Concepts.** Maryland: Rowman & Littlefield, 2016.

GONÇALVES, Joanisval Brito. **Atividade de inteligência e legislação correlata.** 6. ed., rev. e atual. Niterói: Impetus, 2018.

MORGENTHAU, Hans J. **Politics among nations: the struggle for power and peace**. 5. ed. New York: Alfred A. Knopf, 1973.

HARDING, Luke. **Os arquivos Snowden: A história secreta do homem mais procurado do mundo.** Tradução de Cássio de Arantes Leite. São Paulo: Companhia das Letras, 2014.

HOWLETT, M.; RAMESH, M. **Studying public policy: Policy cycles and policy subsystems**. Don Mills, Ont.: Oxford University Press, 2003.

IVANISSEVIC, ALICIA. Espionagem: qual o limite? **Ciência Hoje**, Rio de Janeiro, 12 jul. 2013. Disponível em: https://cienciahoje.org.br/artigo/espionagem-qual-o-limite/. Acesso em: 28 set. 2024.

KAMAKAWA, Marcos. Um estudo sobre a organização e o funcionamento do Sistema Brasileiro de Inteligência (Lei nº 9.883/99 e Decreto 4.376/2002): para consonância e aplicabilidade no Sistema de Inteligência da PMPR. ISSN: 2595-3621. **Brazilian Applied Science Review**, Curitiba, v.6, n.2, p.534-544, mar/abr., 2022. DOI: :10.34115/basrv6n2-012. Disponível em: <https://scholar.archive.org/work/4cycl4c2wvcojggmwfk3ng4up4/access/wayback/https://brazilianjournals.com/index.php/BASR/article/download/46246/pdf> . Acesso em: 17 fev. 2025

LIOTTA, P.H; OWEN, Taylor. Why Human Security? **The Whitehead Journal of Diplomacy and International Relations**, Seton Hall University, set./dez. 2006. Disponível em: https://ciaotest.cc.columbia.edu/olj/shjdir/v7n1/v7n1_04.pdf. Acesso em: 21 mar. 2025.

Lista revela 29 integrantes do governo Dilma espionados pelos EUA. **G1**, 04 jul. 2015. Disponível em: https://g1.globo.com/politica/noticia/2015/07/lista-revela-29-integrantes-do-governo-dilma-espionados-pelos-eua.html. Acesso em: 7 jul. 2024.

LOPES, Gills Vilar. Vigilância Cibernética no Brasil: O Caso Snowden sob o PRISMa de um insider. **Revista Eco Pós, Tecnopolíticas e vigilância,** v. 18, n.2, 2015. Disponível em: https://revistaecopos.eco.ufrj.br/eco_pos/article/view/2238/2245 . Acesso em: 26 mar. 2025.

MANDARINO, R. **Um estudo sobre a segurança e a defesa do espaço cibernético brasileiro**. 2009. Monografia (Especialização) — Universidade de Brasília, Departamento de Ciência da Computação, Brasília, 2009. p. 29.

MIRANDA FILHO, Fábio Nogueira. O papel do serviço de inteligência na segurança das infraestruturas críticas. **Revista Brasileira de Inteligência**, n. 7, p. 79-92, 2012. Disponível em: https://www.bibliotecadeseguranca.com.br/wp-content/uploads/2020/08/o-papel-do-servico-de-inteligencia-na-seguranca-das-infraestruturas-criticas.pdf . Acesso em: 6 out 2024

MORGENTHAU, H. J.; THOMPSON, K. W. **Politics Among Nations.** McGraw-Hill Humanities, Social Sciences & World Languages, 1993, p. 3.

MORAES, Maurício. Brasil. **Espionagem abre discussão sobre preparo do Brasil para uma guerra cibernética**. BBC Brasil, 11 out. 2013. Disponível em: https://www.google.com/url?q=https://www.bbc.com/portuguese/noticias/2013/10/131011_defesa_seguranca_cibernetica_brasil_mm&sa=D&source=docs&ust=1743755870335746&usg=AOvVaw0IfMTpyJ2fA8XJ9WX7VSVx . Acesso em: 19 mar. 2025.

MUTIMER, David. Critical Studies: A Schismatic History. *In*: COLLINS, Alan (org.). **Contemporary Security Studies**. 3. ed. London: Oxford University Press, 2013. p. 69. Disponível em: https://www.oxfordpoliticstrove.com/display/10.1093/hepl/9780198862192.001.0001/hepl-9780198862192-chapter-7. Acesso em: 09 mar. 2025

NCSC. National Counterintelligence and Security Center Strategic Plan,| 2018–2022. **National Counterintelligence and Security Center**, 2017. Disponível em: <https://www.odni.gov/files/NCSC/documents/Regulations/2018-2022-NCSC-Strategic-Plan.pdf> Acesso em: 11 fev. 2025.

OLIVEIRA, Hércules Rodrigues de. Propriedade intelectual: uma visão de inteligência. **Revista Brasileira de Inteligência, Abin**, n. 7, jul. 2012. Disponível em: https://rbi.abin.gov.br/RBI/article/view/96/77. Acesso em: 16 fev. 2025.

OLIVEIRA, Lúcio Sérgio Porto. **A história da atividade de inteligência no Brasil.** Brasília, DF: ABIN, 1999.

PAULA, Geovani de, et al. Tecnologia Da Informação E Comunicação E As Atividades De Inteligência. **Revista Ordem Pública.** Vol.5 n°1. 2012. Disponível em: https://pdfs.semanticscholar.org/1a59/126e0c7c6cc5504256e16e4bbced4d7a4f4a.pdfPAULA,%20Geovani%20de,%20et%20al.%20Tecnologia%20Da%20Informa%C3%A7%C3%A3o%20E%20Comunica%C3%A7%C3%A3o%20E%20As%20Atividades%20De%20Intelig%C3%AAncia.%20Revista%20Ordem%20P%C3%BAblica.%20Vol.5%20n%C2%B01.%202012. Acesso em: 03 mar. 2025.

PINHEIRO, Marta Macedo Kerr. Informational state: implications for information and intelligence policies at the beginning of the 21th Century. **Varia Historia**, v. 28, p. 61-77, 2012. Disponível em: https://www.scielo.br/j/vh/a/jkhSSFJLRFBK7TdkwQY87wR/. Acesso em: 05 mar. 2025.

PONTES, Marcos Rosas Degaut. Presidência da República Gabinete de Segurança Institucional Agência Brasileira de Inteligência (ABIN). **Revista Brasileira de Inteligência,** Nº 9, 2015. Pág. 9-26. Disponível em: https://www.gov.br/abin/pt-br/centrais-de-conteudo/revista-brasileira-de-inteligencia/copy_of_RBI9.pdf. Acesso em: 8 fev. 2025.

SPANIOL, BRUNA PAIANI NASSER. **A vigilância na internet: a circulação midiática brasileira do vazamento de dados da NSA por Edward Snowden**. 2015. 105f. Dissertação (Mestrado em Estudos da Mídia) - Centro de Ciências Humanas, Letras e Artes, Universidade Federal do Rio Grande do Norte, Natal, 2015. Disponível

em: https://repositorio.ufrn.br/bitstream/123456789/20970/1/BrunaPaianiNasserSpaniol_DISSERT.pdf. Acesso em: 2 out 2024.

SUN TZU. **A arte da guerra.** 1. ed - São Paulo: Pé da Letra, 2016.

TERRA. **Brasil terá centro de certificação para evitar espionagem**. Jornal de Notícias, 14 Ago. 2013. Disponível em: https://www.terra.com.br/amp/noticias/brasil/brasil-tera-centro-de-certificacao-para-evitar-espionagem,025219fd65870410VgnCLD2000000ec6eb0aRCRD.html . Acesso em: 25 Mar. 2025.

ULLMAN, Richard. Redefining security. In: **Security Studies**. Routledge, 2011. p. 11-17.

WALT, Stephen M. The renaissance of security studies. **International studies quarterly**, v. 35, n. 2, p. 211-239, 1991. Disponível em: https://academic.oup.com/isq/article-abstract/35/2/211/1792023. Acesso em: 12 fev. 2025.

WOLFERS, Arnold apud Pontes, 2015, p. 11. National Security as an Ambiguous Symbol. **Political Science Quarterly**, v. 67, n. 4, dec.1952. Disponível em: https://pdfs.semanticscholar.org/1a59/126e0c7c6cc5504256e16e4bbced4d7a4f4a.pdf. Acesso em: 05 fev. 2025.