UNIVERSIDADE FEDERAL DO RIO GRANDE DO SUL
FACULDADE DE CIÊNCIAS ECONÔMICAS
PROGRAMA DE PÓS-GRADUAÇÃO EM ESTUDOS ESTRATÉGICOS INTERNACIONAIS

VANESSA COPETTI CRAVO

EM BUSCA DE UMA ESTRATÉGIA NACIONAL DE SEGURANÇA CIBERNÉTICA: MARCO LEGAL E AUTORIDADE NACIONAL DE SEGURANÇA CIBERNÉTICA

PORTO ALEGRE
2023

VANESSA COPETTI CRAVO

EM BUSCA DE UMA ESTRATÉGIA NACIONAL DE SEGURANÇA CIBERNÉTICA: MARCO LEGAL E AUTORIDADE NACIONAL DE SEGURANÇA CIBERNÉTICA

Tese de Doutorado apresentada ao Programa de Pós-Graduação em Estudos Estratégicos Internacionais da Faculdade de Ciências Econômicas da Universidade Federal do Rio Grande do Sul como requisito final para a obtenção do título de Doutora em Estudos Estratégicos Internacionais.

Orientador: Prof. Dr. José Miguel Quedi Martins

PORTO ALEGRE

2023

CIP - Catalogação na Publicação

Cravo, Vanessa Copetti
Em busca de uma Estratégia Nacional de Segurança Cibernética: marco legal e autoridade nacional de segurança cibernética / Vanessa Copetti Cravo. -- 2023.
226 f.
Orientador: José Miguel Quedi Martins.

Tese (Doutorado) -- Universidade Federal do Rio Grande do Sul, Faculdade de Ciências Econômicas, Programa de Pós-Graduação em Estudos Estratégicos Internacionais, Porto Alegre, BR-RS, 2023.

1. Segurança cibernética. 2. Estratégia nacional de segurança cibernética. 3. Marco legal.. 4. Autoridade nacional de segurança cibernética. I. Martins, José Miguel Quedi, orient. II. Título.

Elaborada pelo Sistema de Geração Automática de Ficha Catalográfica da UFRGS com os dados fornecidos pelo(a) autor(a).

VANESSA COPETTI CRAVO

EM BUSCA DE UMA ESTRATÉGIA NACIONAL DE SEGURANÇA CIBERNÉTICA: MARCO LEGAL E AUTORIDADE NACIONAL DE SEGURANÇA CIBERNÉTICA

Tese de Doutorado apresentada ao Programa de Pós-Graduação em Estudos Estratégicos Internacionais da Faculdade de Ciências Econômicas da Universidade Federal do Rio Grande do Sul como requisito final para a obtenção do título de Doutora em Estudos Estratégicos Internacionais.

Aprovada em: Porto Alegre, 27 de fevereiro de 2023.

BANCA EXAMINADORA:

_____

Prof. Dr. José Miguel Quedi Martins – Orientador

UFRGS

_____

Prof. Dr. Érico Esteves Duarte

UFRGS

_____

Profª Dra. Danielle Jacon Ayres Pinto

USFC

_____

Prof. Dr. Diego Rafael Canabarro

Universidad de San Andrés

_____

Prof. Dr. Marcelo Antônio Osller Malagutti

Instituto Vegetius

Dedico esse esforço à minha família, especialmente ao meu marido William e às minhas filhas Laura e Bruna.

AGRADECIMENTOS

Em primeiro lugar agradeço a Deus pela graça de ter conseguido concluir o processo de doutoramento, especialmente de elaboração da tese. Em segundo lugar, agradeço ao meu esposo, William Mendes Fantinel, que me forneceu o suporte fundamental para essa empreitada. Na sequência, agradeço às minhas filhas pela compreensão e paciência diante das minhas ausências, a quem dedico esse esforço.

Da mesma forma, agradeço aos meus pais pelo exemplo, por propiciarem a minha formação acadêmica e pelo apoio, especialmente nas últimas semanas que antecederam à entrega. Agradeço também a minha irmã, Daniela Copetti Cravo, e ao meu cunhado, Eduardo Jobim, que fizeram uma revisão geral de parte do trabalho, quando os meus olhos já não mais conseguiam vislumbrar os vícios. Agradeço ao meu orientador, Prof. Dr. José Miguel Quedi Martins, pelo acolhimento no programa, aulas, paciência e norte durante a elaboração da pesquisa. Também agradeço ao Programa e aos professores que o compõe pelas disciplinas que contribuíram para minha formação. Da mesma forma, agradeço aos Professores que compuseram a Banca de Qualificação, contribuindo sobremaneira para a evolução da tese, bem como aos Professores que aceitaram compor a Banca de Doutoramento. Não posso esquecer do auxílio fundamental do Prof. João Gabriel Burmann da Costa durante às últimas semanas do processo de finalização da escrita. Por fim, agradeço à Agência Nacional de Telecomunicações - Anatel, especialmente nas pessoas de Rafael André Baldo de Lima, que forneceu o suporte para que eu pudesse cursar as disciplinas; e Eduardo Kruel Milano do Canto e Gustavo Santana Borges, que além de encorajamento e crença no meu trabalho, asseguraram o amparo final para que eu pudesse concluir a redação da pesquisa.

Às (Aos) colegas do Grupo Técnico de Segurança Cibernética e Gestão de Riscos de Infraestrutura Crítica (GT-Ciber) da Anatel agradeço pela parceria, confiança e todas as trocas no cumprimento da nossa missão, notadamente nas pessoas de Adeilson Evangelista Nascimento e Rafael Andrade Reis de Araujo.

E, finalmente, aos colegas das Comissões Brasileiras de Comunicação (CBCs), estrutura formal da Anatel instituída para organizar a representação brasileiras nos foros internacionais de telecomunicações, agradeço pela oportunidade, imenso aprendizado e reconhecimento do trabalho desenvolvido. No âmbito das CBCs e, considerando as discussões de segurança cibernética, agradeço especialmente a Andrea Mamprim Grippa, Cristiana Camarate Silveira Martins Leão Quinalia, Roberto Mitsuake Hirayama, Ronaldo Neves de Moura Filho e Victor Muniz Estevam Dias. Além disso, embora não mais colegas de Anatel, agradeço a Miriam Wimmer e Jeferson Fued Nacif, pela inserção nos debates e inspiração.

RESUMO

A temática da segurança cibernética é um dos temas principais da agenda internacional dos últimos anos, sendo discutida nas mais diversas e importantes organizações regionais e internacionais. É indiscutível a necessidade de coordenação, cooperação e atuação internacional para o enfrentamento do problema, visto que os incidentes de segurança são transnacionais, ou seja, não conhecem fronteiras. Também não pode ser esquecido que o desafio se insere em um contexto mais amplo de Quarta Revolução Industrial, Transformação Digital e Desenvolvimento. Nacionalmente, a resposta de dezenas de países é estruturada na elaboração de políticas e/ou estratégias nacionais de segurança cibernética, justamente a fim de organizar o modelo de governança e de todos os temas que flutuam ao seu redor, assim como engajar todos os atores e definir objetivos e prioridades. Nesse sentido, busca-se estudar os modelos internacionais que orientam os países no desenvolvimento desses instrumentos e compreender o arcabouço jurídico e de políticas públicas existente no nosso ordenamento. Com base nessas conclusões, defende-se um processo de construção de uma Estratégia Nacional de Segurança Cibernética para o Brasil, tanto em forma quanto em matéria, apoiada em duas condições: o estabelecimento do marco legal adequado e a instituição de uma Autoridade Nacional de Segurança Cibernética, elencando as premissas associadas para cada uma dessas prescrições.

PALAVRAS-CHAVE: Segurança Cibernética. Estratégia Nacional de Segurança Cibernética. Marco Legal. Autoridade Nacional de Segurança Cibernética.

ABSTRACT

Cybersecurity is one of the main themes on the international agenda in recent years, being discussed in the most diverse and important regional and international organizations. The need for coordination, cooperation, and international action to tackle the problem is indisputable, given its transnational nature. It cannot be also forgotten that this challenge is part of a broader context of the Fourth Industrial Revolution, Digital Transformation and Development. Nationally, the response of dozens of countries is structured in the elaboration of national cybersecurity policies and strategies, precisely in order to organize the governance model and all the themes that revolve around it, as well as to engage all stakeholders and define objectives and priorities. In this sense, the aim of this research is to study the international models that guide countries in the development of these instruments and to understand the already existing Brazilian legal and policy framework. Based on these conclusions the research advocates for building a formal and material National Cybersecurity Strategy for Brazil, based on two conditions: the establishment of an adequate cybersecurity legal framework and the institution of a National Cybersecurity Authority, with the associated premises for each one of these prescripts.

KEYWORDS: Cybersecurity. Nacional Cybersecurity Strategies. Legal Framework. National Cybersecurity Authority.

LISTA DE ILUSTRAÇÕES

LISTA DE SIGLAS E ABREVIATURAS

AE	Ação Estratégia
AED	Ações Estratégicas de Defesa
AGNU	Assembleia Geral das Nações Unidas
ANATEL	Agência Nacional de Telecomunicações
ANPD	Autoridade Nacional de Proteção de Dados
APF	Administração Pública Federal
APWG	*Antiphising Working Group*
BID	Base Industrial de Defesa
BRASSCOM	Associação Brasileira das Empresas de Tecnologia da Informação e Comunicação
CDCIBER	Centro de Defesa Cibernética
CDEP	Comitê de Políticas sobre Economia Digital
CENELEC	Comitê Europeu para a Normalização Eletrotécnica
CERT.br	Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil
CETIC.br	Centro Regional de Estudos para o Desenvolvimento da Sociedade da Informação
CGCTIR	Coordenação-Geral do Centro de Tratamento de Incidentes de Rede do Governo
CGI.br	Comitê Gestor da Internet no Brasil
CGNSC	Coordenação-Geral do Núcleo de Segurança e Credenciamento
CGSI	Comitê Gestor de Segurança da Informação
CGSIC	Comitê Gestor de Segurança de Infraestruturas Críticas
CICTE	Secretaria do Comitê Interamericano contra o Terrorismo da OEA
CIRT/CSIRT/CERT	Equipes de Prevenção, Tratamento e Reposta a Incidentes Cibernéticos
CMM	Modelo de Maturidade de Capacidade de Segurança Cibernética
CMSI	Cúpula Mundial sobre a Sociedade da Informação
CNJ	Conselho Nacional de Justiça
CNSS	Comitê de Sistemas de Segurança Nacional dos Estados Unidos
ComDCiber	Comando de Defesa Cibernética
CPI	Comissão Parlamentar de Inquérito

CREDEN	Câmara de Relações Exteriores e Defesa Nacional
CTIR Gov	Centro de Prevenção, Tratamento e Resposta a Incidentes Cibernéticos de Governo
DoS	Ataque de Negação de Serviço
DSI	Departamento de Segurança da Informação do Gabinete de Segurança Institucional da Presidência da República
DSIC	Departamento de Segurança da Informação e Comunicações do Gabinete de Segurança Institucional da Presidência da República
E-Ciber	Estratégia Nacional de Segurança Cibernética
E-Digital	Estratégia Brasileira para a Transformação Digital
EGC	Exercício Guardião Cibernético
EMBRAPII	Empresa Brasileira de Pesquisa e Inovação Industrial
EnaDCIBER	Escola Nacional de Defesa Cibernética
END	Estratégia Nacional de Defesa
ENISA	Agência da União Europeia para a Cibersegurança
ENSC	Estratégia Nacional de Segurança Cibernética
ENSEC-PJ	Estratégia Nacional de Segurança da Informação e Cibernética do Poder Judiciário
ENSI	Estratégia Nacional de Segurança da Informação
ENSIC	Estratégia Nacional de Segurança de Infraestruturas Críticas
ETIR	Equipe de Tratamento e Resposta a Incidentes em Redes Computacionais
ETSI	Instituto Europeu de Normas de Telecomunicações
EUA	Estados Unidos da América
FIRST	*Forum of Incident Response and Security Teams*
FNDCT	Fundo Nacional de Desenvolvimento Científico e Tecnológico
GCA	Agenda Global de Segurança Cibernética
GCI	Índice Global de Segurança Cibernética
GCIv1	Primeira Iteração do Índice Global de Segurança Cibernética
GCIv2	Segunda Iteração do Índice Global de Segurança Cibernética
GCIv3	Terceira Iteração do Índice Global de Segurança Cibernética
GCIe4	Quarta Edição do Índice Global de Segurança Cibernética
GCSCC	Centro Global de Capacidade de Segurança Cibernética da *Oxford Martin School* da Universidade de Oxford

GSI/PR	Gabinete de Segurança Institucional da Presidência da República
GT SEG CIBER	Grupo Técnico de Segurança Cibernética da CREDEN
ICCP	Comitê sobre Políticas de Informação, Computadores e Comunicação da OCDE
IEC	Infraestrutura Crítica
IGF	Fórum de Governança da Internet
IoT	Internet das Coisas
ISO	Organização Internacional de Normalização
LAC-AAWG	*Latin America and Caribbean Anti-abuse Working Group*
LDO	Lei de Diretrizes Orçamentárias
LGPD	Lei Geral de Proteção de Dados Pessoais
LGT	Lei Geral de Telecomunicações
LNCC	Laboratório Nacional de Computação Científica
LOA	Lei Orçamentária Anual
MCI	Marco Civil da Internet
MCTI	Ministério de Ciência, Tecnologia, Inovações
MCTIC	Ministério de Ciência, Tecnologia, Inovações e Comunicações
MD	Ministério da Defesa
NIC.br	Núcleo de Informação e Coordenação do Ponto BR
NIST	Instituto Nacional de Padrões e Tecnologia dos Estados Unidos
OCDE	Organização para a Cooperação e Desenvolvimento Econômico
OCEE	Organização para Cooperação Econômica Europeia
OEA	Organização dos Estados Americanos
OND	Objetivos Nacionais de Defesa
OTAN	Organização do Tratado do Atlântico Norte
PD&I	Pesquisa, Desenvolvimento e Inovação
PLANSIC	Plano Nacional de Segurança de Infraestruturas Críticas
PND	Política Nacional de Defesa
PNSI	Política Nacional de Segurança da Informação
PNSIC	Política Nacional de Segurança de Infraestruturas Críticas
PNUD	Programa das Nações Unidas para o Desenvolvimento
PPA	Plano Plurianual
ReGIC	Rede Federal de Gestão de Incidentes Cibernéticos
RNP	Rede Nacional de Pesquisa

SI	Sociedade da Informação
TCU	Tribunal de Contas da União
TI	Tecnologia da Informação
TIC	Tecnologia de Informação e Comunicação
UIT	União Internacional de Telecomunicações
UIT-D	Setor de Desenvolvimento das Telecomunicações da UIT
UIT-R	Setor de Radiocomunicação da UIT
UIT-T	Setor de Normalização das Telecomunicações da UIT
UNESCO	Organização das Nações Unidas para a Educação, a Ciência e a Cultura
WPDGP	Grupo de Trabalho sobre Privacidade e Governança de Dados na Economia Digital da OCDE
WPISP	Grupo de Trabalho sobre Segurança da Informação e Privacidade do ICCP da OCDE
WPSDE	Grupo de Trabalho sobre Segurança na Economia Digital da OCDE
WPSPDE	Grupo de Trabalho sobre Segurança e Privacidade na Economia Digital da OCDE

SUMÁRIO

1 INTRODUÇÃO

O presente Capítulo tem o intuito de apresentar a temática de segurança cibernética que é objeto da tese, a sua delimitação e demonstrar a sua relevância e inserção como um dos tópicos prioritários das discussões das organizações internacionais e sustentáculo da transformação digital, através da revisão sistemática da literatura. Além disso, o Capítulo I também abordará o desenho de como a pesquisa foi conduzida e demonstrará a existência de diferentes dimensões e conceitos de segurança cibernética, indicando qual a abordagem utilizada para fins do trabalho.

Para tanto, o presente Capítulo está subdividido em marco teórico; desenho de pesquisa; dimensões de segurança cibernética e conceito; e conclusões parciais.

Já o Capítulo II será destinado a detalhar o trabalho relacionado ao fomento do desenvolvimento de Estratégias Nacionais de Segurança Cibernética de três organizações, que são: a Organização para a Cooperação e Desenvolvimento Econômico (OCDE), a União Internacional de Telecomunicações (UIT) e o Centro Global de Capacidade de Segurança Cibernética (GCSCC), da *Oxford Martin School* da Universidade de Oxford. Essas iniciativas serão consideradas como modelos para fins da pesquisa.

Na sequência, o Capítulo III direcionará seu olhar para o Arcabouço Nacional Jurídico e de Políticas Públicas, descrevendo as políticas, estratégias e legislação correlata em matéria de segurança cibernética, também recordando o histórico de desenvolvimento das políticas e marcos associados.

Por fim, o último, Capítulo IV, utilizar-se-á dos acúmulos dos três capítulos anteriores, isto é, da revisão sistemática da literatura deste Capítulo I; dos subsídios ofertados pelos modelos apresentados no Capítulo II; e da descrição do Arcabouço Nacional realizada no Capítulo III, para propor contribuições para as políticas públicas brasileiras nessa seara, especialmente endereçando dois aspectos que desde já se enuncia: Marco Legal e Autoridade Nacional de Segurança Cibernética.

Dessa forma, inicia-se com a apresentação da revisão sistemática da literatura, na subseção que discorrerá sobre o marco teórico.

1.1 MARCO TEÓRICO

A economia e a sociedade sofreram e continuam a sofrer profundas transformações em face da utilização das tecnologias que viabilizam os processos de digitização e de digitalização

e cujos efeitos econômicos e sociais são denominados de transformação digital. Digitização e Digitalização não se confundem, porém são fenômenos complementares, na medida em que a digitização refere-se à conversão de dados e processos analógicos para um formato digital, ou seja, que pode ser processado por um computador. Já a digitalização representa a utilização de tecnologias digitais e dados, assim como a interconexão que delas resulta, em novas atividades ou mudanças nas atividades existentes (ORGANIZAÇÃO PARA A COOPERAÇÃO E DESENVOLVIMENTO ECONÔMICO - OCDE, 2019).

Veja-se que com a Pandemia da Covid-19, tanto os processos de digitização quanto de digitalização foram acelerados, em face da necessidade de manter minimamente as atividades sociais e econômicas em funcionamento durante um período de restrições relacionadas ao necessário distanciamento e isolamento sociais, refletindo em todos os setores da economia e da vida em sociedade. Esses efeitos são justamente o que se descreve como transformação digital.

São precisamente as Tecnologias de Informação e Comunicação (TICs)[1] que permitem esses fenômenos e viabilizam a transformação digital, cujo impacto na sociedade e na economia também passou a progressivamente repercutir nas relações internacionais.

O desenvolvimento e a incorporação de novas tecnologias para fins de defesa não constituem uma novidade, ao contrário. E também não se restringem às TICs. No entanto, os processos, hoje identificados como digitização e digitalização oportunizados pelas TICs, têm repercussões que precisam ser adequadamente equacionadas pelas Forças Armadas[2]. Afinal, a expansão das TICs e a utilização do espaço cibernético forneceram novas capacidades aos militares, mas também novos desafios (BARRY; ZIMET, 2009, p. 1), visto que aquilo que pode ser utilizado para benefício da sociedade, também pode ser usado em seu detrimento (KURBALIJA, 2016, p. 81).

Contudo, essas repercussões, não são vivenciadas somente na área securitária, expandindo-se e impactando de forma sem precedentes a vida das sociedades contemporâneas, sob todos os seus aspectos e de todas as nações. E, portanto, tornaram-se relevantes para a estabilidade do Sistema Internacional e passaram a dominar as pautas das agendas internacionais.

---

[1] Conceituadas como "*tecnologias utilizadas para tratamento, organização e disseminação de informações*", no livro verde da Sociedade da Informação no Brasil (BRASIL, 2000b, p. 176).

[2] Sobre digitalização e guerra ver: Martins (2008) e Duarte (2012).

Um dos primeiros fóruns direcionados a travar essa discussão na comunidade internacional foi a Cúpula Mundial sobre a Sociedade da Informação (CMSI), cuja primeira fase ocorreu em Genebra, na Suíça, em 2003, e a segunda fase, em Túnis, na Tunísia, em 2005.

Como conceito de Sociedade da Informação, adota-se o constante do Livro Verde da Sociedade da Informação no Brasil, o qual destaca sua caracterização como profunda mudança na organização da sociedade e da economia, como fenômeno global e com dimensões político-econômica e social (BRASIL, 2000, p. 5) [3]. Ademais, o Livro já indicava, há mais de duas décadas atrás, a defesa de que seria um novo paradigma técnico-econômico, o que nas palavras de Carlota Perez implica em um modelo de melhor prática para o mais efetivo uso de novas tecnologias dentro e além de novas indústrias, assim transformando outras indústrias e atividades. Para Carlota Perez (2010) seria justamente o paradigma aliado à forte interconectividade e interdependência dos sistemas participantes em suas tecnologias e mercados que caracterizaria uma revolução tecnológica.

Dialogando com os conceitos apresentados Carlota Perez, tenta-se contextualizar o fenômeno sob o manto das revoluções industriais, com o objetivo de chegar no conceito da Quarta Revolução Industrial proposto por Klaus Schwab, Presidente-Executivo do Fórum Econômico Mundial. Em 2016, o autor já alertava que estávamos à beira de revolução tecnológica que seria responsável por modificar fundamentalmente como vivemos, trabalhamos e nos relacionamos uns com os outros, sendo que sua escala, escopo e complexidade importaria em uma transformação sem precedentes na história da humanidade (SCHWAB, 2016, p. 3).

Mais de duas décadas do Livro Verde da Sociedade das Informação no Brasil; mais de seis anos da alcunha do termo "Quarta Revolução Industrial" por Klaus Schwab; e dois anos da Pandemia da Covid-19, parece incontestáveis as premissas apontadas.

Klaus Schwab, em um esforço de simplificação, identifica a Primeira Revolução Industrial com a utilização da energia da água e do vapor para a mecanização da produção. Já a Segunda Revolução Industrial estaria associada à utilização da energia elétrica para criar a produção em massa. Na Terceira, tem-se a utilização de eletrônicos e tecnologia da informação

[3] Como Sociedade da Informação, adota-se também a noção apresentada no livro verde acima citado: "Representa uma profunda mudança na organização da sociedade e da economia, havendo quem a considere um ***novo paradigma técnico-econômico***. É um ***fenômeno global,*** com elevado potencial transformador das atividades sociais e econômicas, uma vez que a estrutura e a dinâmica dessas atividades inevitavelmente serão, em alguma medida, afetadas pela infra-estrutura de informações disponível. É também acentuada sua ***dimensão político-econômica***, decorrente da contribuição da infra-estrutura de informações para que as regiões sejam mais ou menos atraentes em relação aos negócios e empreendimentos. Sua importância assemelha-se à de uma boa estrada de rodagem para o sucesso econômico das localidades. Tem ainda marcante ***dimensão social***, em virtude do seu elevado potencial de promover a integração, ao reduzir as distâncias entre pessoas e aumentar o seu nível de informação" (BRASIL, 2000, p. 5).

para automatizar a produção e, por fim, a Quarta Revolução é caracterizada pela fusão de tecnologias que acabam ofuscando os limites entre as esferas física, digital e biológica (SCHWAB, 2016, p. 3).

Outrossim, o autor também elucida que embora a Quarta esteja construída sobre a Terceira, que já ocorre desde o meio do século passado, ela não se trata apenas de mero incremento em face da sua velocidade, escopo e impacto sistêmico. Inteligência Artificial, Robótica, Internet das Coisas, Veículos Autônomos, Impressão 3D, nanotecnologia, biotecnologia e computação quântica seriam alguns dos principais padrões de reconhecimento dessa Quarta Revolução (SCHWAB, 2016, p. 3).

Schwab e Davis assinalam que a Quarta Revolução Industrial é uma maneira de "*descrever um conjunto de transformações em curso e iminentes dos sistemas que nos rodeiam*". Além do mais, não se trata de uma alteração ínfima, mas de um "*novo capítulo do desenvolvimento humano*", que é respaldado por uma "*crescente disponibilidade e interação de um conjunto de tecnologias extraordinárias*", as quais estão identificadas no parágrafo anterior, além de outras (SCHWAB; DAVIS, 2018, p. 35).

Adere-se à ideia de que já estamos vivenciando não apenas um processo de evolução tecnológica, uma mera coleção de sistemas de tecnologia, mas uma verdadeira revolução tecnológica e, portanto, apoiada em um novo paradigma técnico-econômico, conforme prescreve Carlota Perez (2010, p. 8-9).

Partindo da premissa exposta, enuncia-se a oportunidade de avanço para o país em trajetórias de crescimento com o processo de *catching up* como ensina Carlota Perez e Luc Soete, tendo em vista que o período de transição tecnológica constitui janela de oportunidade temporária para os países. Nessa janela os países podem aprender, enquanto todos buscam o conhecimento, e aproveitar que as barreiras de entradas são as menores (1988, p. 477). No entanto, para que um país possa se aproveitar da transição na busca do seu desenvolvimento, requer a capacidade de reconhecê-la, a competência e a imaginação necessária para desenhar a estratégia adequada, as condições sociais e a vontade política para realizá-la (PEREZ; SOETE, 1988, p. 478).

Nesse ponto, retoma-se um dos pontos centrais da obra de Celso Furtado, o conceito de Centros de Decisão. Deter no seu próprio território o centro principal de decisão da vida econômica do país, significa ter grau de autonomia para comandar a vida econômica do país e poder colocar a economia à serviço de uma política de desenvolvimento nacional (FURTADO, 1962, p. 112).

Considerando que estamos no limiar da Quarta Revolução Industrial (SCHAWB, 2016, p. 3) e a janela de oportunidade para fins de desenvolvimento (PEREZ; SOETE, 1988, p. 477), o conceito de Centro de Decisão auxilia a interpretação de movimentos estatais relacionados ao domínio e liderança das tecnologias associadas a essa revolução, assiste na compreensão de tensões geopolíticas recentes e permite tecer contribuições às políticas públicas brasileiras, que ainda se apresentam muito tímidas no enfrentamento da autonomia do Brasil para fins explorar as oportunidades que a Quarta Revolução Industrial pode alavancar.

Embora o foco do trabalho seja segurança cibernética, essas premissas iniciais colocadas são fundamentais para compreender as dimensões que envolvem o problema e que o colocam como um dos principais temas da agenda internacional e dos mais importantes fóruns e organizações internacionais, enunciando-se desde já que segurança cibernética é o elemento que permite a fruição dessas tecnologias e dos seus benefícios. Não é possível pensar na exploração de todas as potencialidades da Internet das Coisas, Carros Autônomos, Computação Quântica, Inteligência Artificial e Robótica, para citar alguns exemplos, prescindindo de segurança cibernética, cujo conceito será explorado no trabalho.

Segurança cibernética: agenda internacional e prioridade nacional — ressalva-se que a emergência do tema e o florescimento em todas as agendas das organizações internacionais de maior relevância não é novidade e não está relacionada apenas à Quarta Revolução Industrial. Veja-se que a eflorescência está associada com o surgimento das TICs, e, portanto, às tecnologias da Terceira Revolução Industrial, o que é demonstrado pelo trabalho de mais de duas décadas de diversas organizações nessa matéria. No entanto, no contexto atual, sua importância é exponencial, decorrente do aumento da superfície de ataque, com o intuito de conexão de tudo e de todos; da crescente interdependência de todas infraestruturas críticas (IECs); do impacto das tensões geopolíticas na cadeia de fornecedores; do impacto financeiro de crimes cibernéticos; e da própria transformação da sociedade e da economia em face dos fenômenos da digitização e digitalização.

Corroborando essa afirmação, Vichi alerta a precisão do postulado de que "*o nível de vulnerabilidade é diretamente proporcional ao de digitalização*" e o risco é atual é de interrupção, de uma descontinuidade muito abrangente das IECs, fazendo com que a ausência de pensamento e atuação estratégica por parte dos países coloque em risco o próprio Sistema Internacional (VICHI, 2021, p. 7), argumento que reforça a prevalência da questão nos debates internacionais.

Nessa linha, o espaço cibernético é sustentado como um dos pilares das infraestruturas nacionais e internacionais (BARRY; ZIMET, 2009, p. 3), auxiliando a compreensão da agitação

da comunidade internacional. Assim, já no início dos anos 2000, tem-se a CMSI, cujos documentos finais desse processo - Declaração de Princípios de Genebra, Plano de Ação de Genebra, Compromisso de Túnis e Agenda de Túnis para a Sociedade de Informação (COMITÊ GESTOR DA INTERNET NO BRASIL - CGI.br, 2014) comprovam que a segurança associada à utilização das TICS foi identificada como ponto-chave das discussões e das agendas internacionais.

Radu ensina que o tema passou de preocupação nacional para uma prioridade internacional, sendo tratado por todas as organizações regionais e internacionais importantes (RADU, 2013, p. 39). Exemplificando tal assertiva, cita-se diversas resoluções da Assembleia Geral das Nações Unidas (AGNU) sobre o tema[4], as quais abordam comportamento responsável dos Estados, criação de uma cultura de segurança cibernética e direito à privacidade; bem como reconhecem a gravidade do problema, a importância de combate a essa criminalidade e a necessidade imperativa de cooperação internacional para uma luta eficaz. No tocante à necessidade de cooperação internacional, destaca-se que a transnacionalidade inerente às TICs, rompe com paradigmas tradicionais referentes à criminalidade e aos próprios conflitos internacionais, bem como gera questionamentos sobre a necessidade de novos arranjos internacionais para o enfrentamento adequado do problema.

Além disso, diversas outras organizações regionais e internacionais têm trabalhado fortemente na matéria, atuação justificada pela crescente conectividade e interdependência, pelo enorme impacto à economia global, pela ameaça às IECs nacionais e pelos transfronteiriços danos. Estima-se que o custo anual de crimes cibernéticos à economia global seja entre 375 a 575 bilhões de dólares (CENTER FOR STRATEGIC AND INTERNATIONAL STUDIES - CSIS, 2015), também existindo pesquisas mais recentes que calculam de 799 bilhões até 22,5 trilhões de dólares, ao considerar o custo direto somado aos custos sistêmicos (DREYER, 2018, p. 8)

A Pandemia do COVID-19 impôs novo ritmo à transformação digital, exacerbando a necessidade de enfrentamentos das crescentes ameaças e riscos associados, pois, além do acesso

[4] Ver Resoluções da AGNU: 68/167; 69/166; 71/199; 73/179; 75/176; e 77/2011 (Direito à privacidade na Era Digital); 45/95 (Diretrizes para regulação de dados pessoais em arquivos de computador); 73/187 (Combatendo uso das TICs para finalidades criminais); 57/239, 58/199 e 64/221 (Criação de uma cultura de segurança cibernética e proteção de infraestrutura crítica de informação); 55/63 e 56/121 (Combatendo o uso criminal das tecnologias de informação); e 73/266, 75/32 e 77/37 (comportamento responsável dos Estados no espaço cibernético no contexto de Segurança Internacional), além das resoluções sobre "*Avanços no campo da informação e das telecomunicações no contexto da segurança internacional",* editada desde 1998 (Resoluções 53/70, 54/49, 55/28, 56/19, 57/53, 58/32, 59/61, 60/45, 61/54, 62/17, 63/37, 64/25, 65/41, 66/24, 67/27, 68/243, 69/28, 70/237, 71/28, 73/27, 74/29, 75/240, 76/19 e 77/36). Todas as resoluções estão disponíveis em: https://www.un.org/en/sections/documents/general-assembly-resolutions/index .html.

à rede, ou seja, além da conectividade, faz-se necessário promover a segurança das informações e da própria rede, ou seja, da infraestrutura. Essa inevitabilidade decorre especialmente dos desafios impostos pelas novas e emergentes tecnologias, as quais estão atreladas ao conceito da Quarta Revolução Industrial. O Relatório de Riscos Globais do Fórum Econômico Mundial de 2022 aponta que falhas de segurança cibernética são um dos riscos que mais pioraram durante à pandemia (WORLD ECONOMIC FORUM, 2022, p. 48).

Como resposta internacional para fazer face aos riscos, os países trabalham, sob diferentes perspectivas, em diversos fóruns multilaterais e multissetoriais, na tentativa de estabelecer normas de comportamento responsável no ciberespaço e medidas de construção de confiança, assim como para fomentar a construção de capacidades e para promover a coordenação e cooperação, atributos essenciais para o enfrentamento de um problema que não reconhece fronteiras e que se alarga exponencialmente.

Marcelo Malagutti ensina que, nacionalmente, o ciberespaço passou a ser considerado como o quinto domínio de guerra ao lado dos outros quatro domínios: terra, mar, ar e espaço. E assim como nestes últimos quatros elementos, verifica-se a busca da preservação de supremacia no espaço cibernético por parte dos Estados Unidos da América (EUA), que manteria a vantagem conquistada pela liderança associada ao desenvolvimento das TICs, notadamente computadores, Internet e *software* (MALAGUTTI, 2022b, p. 1-4). É uma zona de guerra (CLARKE e KNAKE, 2012) e nota-se também a pretensão dos EUA de influenciar os processos internacionais de elaboração de normas para o ciberespaço e garantir sua posição de liderança nessa seara (GIORDANO; BOSSO, 2021, p. 43).

Naturalmente, essa identificação do espaço cibernético como uma área estratégica ou um quinto domínio não é uma preocupação restrita aos EUA e o desenvolvimento e a utilização de capacidades nessa seara retroalimentam o debate nas organizações internacionais, inclusive sob a perspectiva securitária, tratando-se de um novo campo de luta pela sobrevivência para as nações (AYRES PINTO, PAGLIARI e GRASSI, 2021, p. 11). No entanto, não se desconsidera a existência de posicionamentos divergentes na literatura que disputam a qualificação do espaço cibernético como quinto domínio. Essa divergência baseia-se nas diferenças entre o espaço cibernético e os outros quatro domínios, dentre as quais se destaca a impossibilidade de isolamento em relação aos demais em razão da penetração, cada vez maior, desse espaço em todas as atividades humanas (LIBICKI, 2012; CEPIK; CANABARRO; FERREIRA, 2015, p. 24).

Acrescentando mais uma camada à discussão, Barry e Zimet enfatizam que com frequência o espaço cibernético é empregado em operações em um dos outros domínios, como

suporte. Não obstante, o poder cibernético também pode ser empregado exclusivamente no âmbito do espaço cibernético para sobrepujar um oponente (BARRY; ZIMET, 2009, p. 5).

Em que pese a divergência, registra-se que não tem reflexos para o presente esforço, tendo em vista o foco na construção de capacidades para além da seara de defesa e segurança nacional. Independentemente da constituição como quinto domínio, ou não, é inquestionável a crescente relevância do espaço cibernético para os debates securitários.

Ayres Pinto *et al* reforçam que as dinâmicas associadas ao espaço cibernético impõem desafios ao paradigma da concepção tradicional de Estado, cuja satisfação de interesses está atrelada ao uso da força e coerção, apresentando-se como uma das alternativas de solução o desenvolvimento de um arcabouço institucional que contemple uma estratégia geopolítica para esses novos desafios. É justamente nesse contexto que as autoras identificam o surgimento de importante atividade institucional desde o início do Século XXI, com o intuito de estabelecimento do arcabouço de promoção de defesa cibernética nos Estados-chave do Sistema Internacional, sem ser olvidada a utilização desse espaço para a guerra (2021, p. 11-12).

Estruturação das respostas — somando-se às capacidades militares relacionadas à defesa, os países têm buscado responder no campo civil às ameaças com a adoção de ações que abarquem as várias dimensões do problema, tais como medidas legislativas, medidas técnicas e procedimentais, estruturas organizacionais, construção de capacidades e cooperação internacional (INTERNATIONAL TELECOMMUNICATION UNION - ITU, 2009)[5].

Especificamente quanto às medidas organizacionais, o estabelecimento do arcabouço institucional adequado, com o estabelecimento de um modelo mínimo de governança para segurança cibernética e a definição de prioridades e objetivos, tem sido o foco de muitos países, inclusive do Brasil, e ganhou impulso a partir de 2008 (SHAFQAT; MASOOD, 2016, p. 131). Atualmente cento e vinte e sete países possuem estratégias nacionais de segurança cibernética ou estão no processo de sua elaboração (UIT, 2021b, p. 9) e Brustolin frisa que é importante compreender essas políticas públicas, bem como colher as lições que podem ser utilizadas e adaptadas para contextos diversos (BRUSTOLIN, 2019, p. 94).

[5] Adota-se aqui como referências os pilares da Agenda Global de Segurança Cibernética, iniciativa lançada em 2007 pela União Internacional de Telecomunicações (ITU, 2009). Mais informações disponíveis em: https://www.itu.int/en/action/cybersecurity/Pages/gca.aspx. No entanto, ressalta-se a existência de modelos diversos, como o Modelo de Maturidade de Capacidade do GCSCC, da *Oxford Martin School* da Universidade de Oxford, o qual é centrado em cinco dimensões: política e estratégia; cultura e sociedade; educação, treinamento e habilidades; arcabouço legal e regulatório; e padrões, organizações e tecnologias, com grande convergência nos modelos entres os tópicos tratados (OXFORD, 2016; 2021), os quais serão detalhados no Capítulo II.

Não é possível entendimento diferente de que segurança cibernética se tornou prioridade nacional, motivando o surgimento de uma nova geração de políticas governamentais (OECD, 2012). Nota-se que inclusive é possível perceber diferentes gerações de ENSCs, tendo em vista que um primeiro conjunto de instrumentos foi identificado no início dos anos 2000 e o estudo da OCDE, publicado em 2012, revela uma nova geração de estratégias (OECD, 2012, p. 5).

Esse estudo realiza análise comparativa de dez ENSCs[6] e constata evolução das estratégias, as quais são centrais em uma percepção governamental de que TICs e a Internet são fundamentais para o desenvolvimento econômico e social, constituindo-se IECs; e que as ameaças no ambiente cibernético estão aumentando e evoluindo em um ritmo avançado. Essas premissas refletem no escopo dos novos instrumentos, no intuito de proteger a sociedade como um todo, traduzindo o papel dessas tecnologias na nossa sociedade (OECD, 2012).

Outro estudo comparativo de Shackelford e Kastelic, que engloba o exame de 34 ENSCs (G20 e países com maior penetração de Internet), aponta que 2013 foi ano com maior desenvolvimento desses instrumentos (SCHACKELFORD; KASTELIC, 2016, p. 926).

Esse movimento de elaboração de arcabouços normativos estratégicos é fomentado por diversas organizações internacionais, destacando-se o trabalho da OCDE. Essa, com base nos seus trabalhos anteriores, desde 2015 fomenta especificamente a adoção de ENSCs junto aos seus membros (bem como junto aos seus membros aderentes), em implementação da Recomendação do Conselho sobre Gerenciamento de Riscos de Segurança Digital para Prosperidade Econômica e Social (OECD, 2015, p. 7).

Na mesma direção, a União Internacional de Telecomunicações (UIT), no cumprimento do seu mandato em segurança cibernética, liderou a elaboração do Guia para Desenvolvimento de uma Estratégia Nacional de Segurança Cibernética (ITU *et al*., 2018a), atualmente já na sua segunda edição, o qual busca enfrentar a crescente complexidade dos riscos cibernéticos (ITU *et al*., 2021c, p. 4).

Sabillon *et al* ressaltam que as políticas de segurança cibernética são um instrumento desenvolvido pelos países para expressar o que buscam proteger no ciberespaço, incorporando um estágio de governança que vincula fortemente aos seus cidadãos (SABILLON, 2016, p. 67). Luiijf notabiliza também que as diferenças nas abordagens nacionais decorrem dos diferentes pontos de partida de cada estratégia, seja de prosperidade econômica, seja de segurança nacional ou militar (LUIIJF, 2011, p. 7). Todavia interessante estudo de Shafqat e Massod

[6] A análise abrangeu Alemanha, Austrália, Canadá, Espanha, EUA, Finlândia, França, Japão, Noruega e Países Baixos (OECD, 2012, p. 5).

aponta que a maioria desenvolveu estratégias separadas para defesa nacional e segurança cibernética (SHAFQAT; MASSOD, 2016, p. 130).

Aprofundando a análise, Brantly e Puyvelde enfatizam que embora existam diferenças significativas entre as estratégias, os países enfrentam um número comum de desafios para promover a segurança no ciberespaço. Os autores também revelam que as estratégias nacionais dos três principais poderes (Estados Unidos, China e Rússia) convergem no sentido de realçar a necessidade de coordenação de múltiplos atores e abordagens (BRANTLY; PUYVELDE, 2019, p. 122). No entanto, Tvaronavičienė *et al* alertam sobre relevante lacuna em tema comum de muitos documentos, visto que muitas ENSCs não endereçam especificamente a proteção de IECs, embora o risco seja presente e crescente (TVARONAVIČIENĖ *et al*, 2020, p. 803).

Lindstrom e Luiijf apontam três elementos de uma estratégia bem formulada: viabilizar que ministérios e departamentos governamentais consigam traduzir a visão nacional do governo em políticas coerentes e implementáveis; clarificar como os Estados poderiam atuar nas relações internacionais; e vincular a estratégia com as demais estratégias nacionais e internacionais, a fim de harmonizar as políticas que são compartilhadas com Estados afins (LINDSTROM; LUIIJF, 2012, p. 46-47).

Veja-se que o primeiro elemento supracitado se refere à governança e a pesquisa comparativa de Shackelford e Kastelic denota a emergência de um momento de produção de arcabouços de governança, com países com preferência para modelos focados no papel do Estado, inclusive com alto nível de centralização. No tocante à dimensão de governança, o estudo constatou uma área de grande convergência entre os países analisados, visto que quase 70% vivenciaram a expansão e (re)definição das atribuições de estruturas governamentais já existentes (SCHACKELFORD; KASTELIC, 2016, p. 920-921).

Os autores sustentam que o desenvolvimento das estratégias é positivo, embora não devam ser elaboradas apenas para atendimento de uma formalidade. Também defendem que as futuras ou revisadas ENSC devem definir boas práticas e métricas, enfatizar a cooperação internacional, esclarecer terminologias e abranger a construção de capacidades, em termos de conscientização e de educação (SCHACKELFORD; KASTELIC, 2016, p. 939).

Resposta brasileira — considerando a inexistência de um arcabouço estratégico nacional, o Brasil elaborou a sua primeira Estratégia Nacional de Segurança Cibernética (E-Ciber), aprovada pelo Decreto nº 10.222, de 5 de fevereiro de 2020 (BRASIL, 2020a), sendo o penúltimo país dentre as quinze maiores economias a elaborar a sua estratégia, embora em 2010 parecesse estar em ritmo semelhante a de seus pares (MALAGUTTI, 2022b, p. 3-1, 3-2).

Para entender o contexto da sua aprovação deve-se remontar à publicação de importantes antecessores, tais como as Estratégias Brasileiras para a Transformação Digital (E-Digital), publicadas em 2018 e 2022; bem como a Política Nacional de Segurança da Informação (PNSI), aprovada pelo Decreto nº 9.637, de 26 de dezembro de 2018, os quais serão detalhados no Capítulo III da tese.

Em termos de avaliação da maturidade em segurança cibernética, o Índice Global de Segurança Cibernética da UIT (ITU, 2018b), que busca mensurar o nível de comprometimento dos Estados-membros aos cinco pilares da Agenda Global de Segurança Cibernética (ITU, 2009) demonstra o impacto da existência de uma estratégia no *ranking*, fazendo que o Brasil caísse para a 70º posição em 2018. Essa posição foi resultado da inexistência de uma estratégia nacional brasileira e do aumento do número de países que desenvolveram e/ou aprimoraram estratégias nacionais desde a primeira publicação do índice em 2015, com base em dados coletados em 2013 e 2014 (ITU, 2015).

Atualmente, o Brasil foi elevado a 18º posição no Índice (ITU, 2021b, p. 25), refletindo os esforços do país principalmente no pilar de capacidade institucional e organizacional. Cita-se como avanços que possibilitaram a melhoria de desempenho: a aprovação da PNSI e da E-Ciber, vários outros avanços em termos de capacidades técnicas e também de medidas de cooperação, ressalvando-se desde logo que o Índice não mensura a implementação das capacidades, mas tão somente a sua existência, como será demonstrado no Capítulo II do trabalho.

O GCSCC da Universidade de Oxford, a convite da Organização dos Estados Americanos (OEA), publicou o estudo "Revisão da Capacidade de Cibersegurança: República Federativa do Brasil" (UNIVERSITY OF OXFORD - OXFORD, 2020a; 2020b). Essa revisão foi iniciada em 2018 e sua análise incluiu os avanços consolidados com a publicação da E-Ciber. A avaliação utiliza o Modelo de Maturidade de Capacidade de Segurança Cibernética (CMM) desenvolvido pelo Centro e classifica os fatores de cada dimensão em estágios de maturidade (a saber: início; formativo; estabelecido; estratégico e dinâmico). Um dos fatores que compõe o CMM é Estratégia Nacional de Segurança Cibernética (ENSC), cuja maturidade brasileira foi identificada como Estágio Formativo-Estabelecido, recomendando alguns itens para aprimoramento, como por exemplo, o estabelecimento de métricas e o engajamento do setor privado (OXFORD, 2020, p. 40, 53).

Por fim, cumpre ainda mencionar que o Relatório da OCDE, publicado em outubro de 2020, "*Going Digital in Brazil*" destaca que o Brasil atingiu um ponto de inflexão em 2018-2019 com a edição da E-Digital e da PNSI, bem como com o processo da elaboração da E-

Ciber (OCDE, 2020a, p. 117). O Relatório ainda aponta que a Estratégia é um excelente primeiro passo, mas que precisa ser traduzido em ações, reconhecendo que o Brasil está em um estágio inicial de desenvolvimento nessa seara e recomendando a adoção de uma agenda de implementação da E-Ciber e a avaliação periódica da sua efetividade (OCDE, 2020a, p. 122, 123).

Contribuições de Bresser-Pereira — dentre os inúmeros aportes deste consagrado autor, que se notabilizou pelas suas contribuições ao debate sobre o Desenvolvimento e a Reforma do Estado, há um ponto decisivo e pouco explorado. Trata-se da sua advertência contra o dogmatismo e à tentação de sucumbir a soluções prontas. Esse alerta ajusta-se com perfeição ao estudo das ENSC.

Como acautela Bresser-Pereira:

> É por isso, principalmente, que fracassam as tentativas dos países ricos e das instituições financeira por eles controladas de exportar instituições, reformas, para os países em desenvolvimento. Instituições não se exportam. Podem e devem ser importadas, porque, assim, não apenas elas sofrerão as adaptações necessárias para se adequarem à realidade nacional, mas, principalmente, elas ganharão a legitimidade de se tornarem propriedade de quem a importou (BRESSER-PEREIRA, 2004, p. 7).

Mais do que se aproveitar do recurso do autor para encontrar soluções brasileiras para problemas brasileiros, há que se enfatizar a categoria central da qual se vale Bresser-Pereira para formular as diretrizes da Reforma do Estado. Trata-se da esfera pública não-estatal. Tal esfera compreende-se como dispositivo mediador entre propriedade estatal e a privada.

Aqui cabe lembrar das lições de Bresser-Pereira e Nuria Grau de que a esfera pública não-estatal é espaço de "*democracia participativa ou direta*", constituindo-se como organizações de controle que são orientadas ao interesse público (BRESSER-PEREIRA; GRAU, 1999, p. 16), de defesa dos valores coletivos (BRESSER-PEREIRA; GRAU, 1999, p. 29), com responsabilidade no alcance das necessidades da coletividade (BRESSER-PEREIRA; GRAU, 1999, p. 29) e, portanto, dividindo com o setor estatal o mesmo propósito de satisfação do interesse público.

Nessa mesma direção os autores concluem que a esfera não-estatal é fenômeno multidimensional, econômico e político, e que seu sustentáculo é "*construção da cidadania em sua dimensão material e política*" (BRESSER-PEREIRA; GRAU, 1999, p. 43-44). Nota-se que os autores advertem que a contribuição da esfera não-estatal exige, não só atuação do Estado, mas também da própria sociedade que precisa reconhecer a sua responsabilidade (BRESSER-PEREIRA; GRAU, 1999, p. 44).

A conexão da proposição de Bresser-Pereira com segurança cibernética pode ser de imediato antecipada: segurança cibernética necessariamente extrapola a esfera estatal. No entanto, também ultrapassa a esfera privada. A junção dessas duas categorias, sozinha, também não consegue abarcar todo o fenômeno. Não se trata de uma mera conveniência a inclusão da esfera pública não-estatal nessa seara, mas de um imperativo.

Esse imperativo decorre das características do fenômeno que impõe papéis e responsabilidades a todos os atores. Ademais, a perspectiva do controle social e do interesse público são componentes fundamentais que devem conformar tanto as políticas públicas de segurança cibernética quanto a sua implementação.

Além do espírito crítico-reflexivo (antidogmático) e da esfera pública não-estatal, cumpre realçar o lugar reservado ao Princípio da Eficiência da Administração Pública[7]. O tema conquanto abordado pelo autor no âmbito da Reforma do Aparelho do Estado, ajusta-se às discussões hodiernas acerca da governança da segurança cibernética no país. Nas suas palavras, o Estado eficaz é fundamental para o estabelecimento das condições, tanto institucionais quanto econômicas, que viabilizarão o desenvolvimento e o crescimento (BRESSER-PEREIRA, 2008, p. 391).

E conforme se buscou demonstrar, a promoção da segurança cibernética cria o ambiente propício necessário à transformação digital da sociedade e da economia, permitindo assim que um país colha esses frutos no fomento do seu desenvolvimento. Dessa forma, qualquer avaliação da eficiência da arquitetura institucional adequada que seja limitada tão somente ao argumento do custo ao Erário é demasiadamente simplista e não reconhece o tamanho e a importância do desafio.

No contexto da reforma gerencial defendida e executada, na extensão possível no âmbito da Reforma do Aparelho do Estado, Bresser-Pereira sempre advogou pelo reforço do papel do Estado e pela eficiência do seu aparelho, especialmente, do núcleo de propriedade estatal, no exercício das funções do núcleo estratégico e das funções exclusivas de Estado (BRESSER-PEREIRA, 1996, 1998, 2008; BRASIL, 1995). Tais funções, hoje se pode aduzir, inquestionavelmente estariam envolvidas no debate das competências de uma Autoridade Nacional de Segurança Cibernética. Desse modo, a governança nacional de segurança

[7] ***Princípio da Eficiência*** - com relação à terminologia eficiência, atenta-se para a constatação da utilização na obra de BRESSER-PEREIRA dos termos eficiência, eficácia e efetividade para qualificar a atuação da Administração Pública Federal pretendida com a reforma do seu aparelho. No âmbito dessa Reforma Gerencial foi aprovada a Emenda Constitucional n.º 19, de 4 de junho 1998, a qual incluiu o Princípio da Eficiência no *caput* do art. 37 da Constituição Federal, como um dos princípios que regem a Administração Pública de todos os Poderes e de todos os entes da Federação.

cibernética abarca tanto a definição de políticas públicas quanto a sua implementação e fiscalização.

Nesse espírito, qualquer escolha institucional deve conformar a necessidade, realidade e interesse nacional, tendo premente a dimensão do desafio. Todos esses aportes do consagrado autor revelaram-se de grande valia na pesquisa para a compreensão dos modelos, bem como para as prescrições normativas.

Por todo o exposto, esse marco teórico buscou demostrar: a relevância do tema e o seu enquadramento como um dos principais tópicos das agendas internacionais, inclusive sob o aspecto securitário; e a sua inserção em um contexto mais amplo de Quarta Revolução Industrial, Transformação Digital e Desenvolvimento dos países. Além disso, esse apanhado também expressou a resposta dos países, inclusive na seara civil, notadamente por meio da elaboração de ENSCs, as quais são formuladas com o suporte de modelos internacionais. Nesse ponto, aproveitou-se para trazer o alerta sobre a importação de modelos e outras contribuições de Bresser-Pereira à discussão; e, finalmente, para expressar uma visão geral da situação brasileira. Passa-se, assim, à descrição do desenho de pesquisa.

1.2 DESENHO DE PESQUISA

Inicialmente importa trazer à baila os objetivos da pesquisa. O objetivo geral que guiou a realização do presente esforço foi justamente a contribuição para o aprimoramento das capacidades brasileiras em matéria de segurança cibernética. Já quanto aos objetivos específicos, cita-se a internalização da discussões de alguns foros internacionais que abordam o tema por meio da promoção do desenvolvimento da capacidade de governança institucional de segurança cibernética; a facilitação da compreensão de modelos internacionais pertinentes; e a contribuição para o processo de aprimoramento do nosso Arcabouço Nacional, notadamente a E-Ciber.

Com essa finalidade, o tema da segurança cibernética foi desenvolvido em quatro passos analíticos sucessivos e complementares. No primeiro passo, operou-se uma revisão bibliográfica do tema, partindo-se de uma perspectiva mais ampla de Quarta Revolução Industrial, Transformação digital, Desenvolvimento e Segurança Internacional, a fim de alcançar a temática de segurança cibernética propriamente dita e, mais especificamente, o tópico das ENSCs, como resposta ao fenômeno.

Essa análise permitiu concluir pela centralidade e predominância da temática na agenda internacional decorrentes da aceleração da transformação digital de toda sociedade e de todos

os setores da economia, bem como da necessidade de mitigar os riscos associados. Em última instância, a promoção da segurança cibernética é a condição necessária para que os países e suas respectivas sociedades possam maximizar os benefícios da transformação digital, com o intuito de alavancar o seu desenvolvimento.

Outra conclusão evidenciada no marco teórico, resultante do processo acima descrito é a estruturação pelos países de uma resposta doméstica aos desafios. Esta resposta materializa-se nas ENSCs e na existência de modelos internacionais que apoiam os países no esforço do seu desenvolvimento. Nesse contexto, tais modelos foram objeto da advertência da necessidade de importação adaptada à realidade e ao interesse do país.

Como segundo passo analítico, realizou-se justamente o estudo dos três modelos utilizados pela comunidade internacional para essa finalidade. Designou-se como modelos:

a) as Recomendações da OCDE, quais sejam, a Recomendação de 2015 sobre Gerenciamento de Riscos de Segurança Digital para Prosperidade Econômica e Social e as Recomendações de 2022 sobre Gerenciamento de Riscos de Segurança Digital e Estratégias Nacionais de Segurança Digital;
b) o Guia para o Desenvolvimento de uma Estratégia Nacional de Segurança Cibernética coordenado pela UIT; e
c) o Modelo de Maturidade de Capacidade de Segurança Cibernética do GCSCC da *Oxford Martin School* da Universidade de Oxford. A análise desses modelos confirmou a valia, flexibilidade e forçosa necessidade de adaptação ao contexto e realidade brasileiros.

O que conduziu ao terceiro passo. Ele constituiu-se com o escrutínio da experiência brasileira, considerando o Arcabouço Jurídico e de Políticas Públicas vigente no país. Desse modo, valeu-se especialmente da Estratégia Nacional de Segurança de Cibernética (E-Ciber), aprovada pelo Decreto nº 10.222, de 5 de fevereiro de 2020, bem como de outras políticas públicas, inclusive da seara de defesa, para advogar pela timidez, limitação e insuficiência do arcabouço vigente.

A timidez advém da forma como o tema é tratado diante de todos os riscos que necessariamente precisam ser geridos e a magnitude do desafio que se descortina. A limitação resulta da abrangência restrita à Administração Pública Federal (APF) e, portanto, não engloba os demais Poderes, nem entes da Federação. Muito menos os atores não estatais. Por fim, a insuficiência manifesta-se na incapacidade de expressar resposta eficiente.

No último passo, procurou-se sistematizar esses acúmulos resultantes dos três passos anteriores, que correspondem respectivamente aos três primeiros capítulos. Esses subsídios,

especialmente dos modelos internacionais e do Arcabouço Nacional, permitiram perseguir soluções normativas. Elas foram desdobradas em duas vertentes: a instituição do Marco Legal e o estabelecimento de uma Autoridade Nacional de Segurança Cibernética. Ademais, foram elaborados delineamentos para cada umas dessas duas dimensões, estipulando-se um conteúdo, ou seja, uma prescrição mínima que precisa ser incorporada aos debates e aos respectivos instrumentos.

Desde logo, cumpre-se antecipar que, para efeitos normativos no âmbito desse trabalho, Marco Legal foi compreendido como a edição de uma lei aprovada pelo Congresso Nacional. Atende-se, dessa forma, rigorosamente ao Princípio da Legalidade. Portanto, partiu-se do reconhecimento acerca da inexistência de lei específica na matéria consoante a descrição que foi realizada no Capítulo III - Descrição das Políticas Públicas de Segurança Cibernética no Brasil.

Como conclusão principal do trabalho, tem-se a constatação de que, embora o Brasil tenha um instrumento aprovado por Decreto presidencial, que é intitulado de "Estratégia Nacional de Segurança Cibernética – E-Ciber", o mesmo não se constitui como uma verdadeira ENSC. A despeito dos vícios decorrentes da timidez, limitação e insuficiência apresentados, o instrumento configura formalmente uma ENSC. Aqui importa sublinhar a diferença contida na dicotomia formal *versus* material. Essa é usual nos vários ramos das Ciências Jurídicas e Sociais e serve para apresentar a distinção entre o cumprimento de uma formalidade e rito (formal) e o conteúdo, a substância de determinado ato (material).

Portanto, não há que se falar em inexistência de uma ENSC no Brasil, visto que a E-Ciber foi aprovada e está vigente. No entanto, sustenta-se sua ausência material, conforme exposto no trabalho.

Nessa toada, as duas prescrições normativas referentes ao marco legal e à instituição da Autoridade Nacional de Segurança Cibernética erigem-se como condições inarredáveis para a criação do ambiente necessário ao desenvolvimento de uma ENSC. Salienta-se que o trabalho não tem a pretensão de apresentar uma proposta de ENSC, a qual se trata de uma construção que necessariamente precisa ser realizada por toda nação.

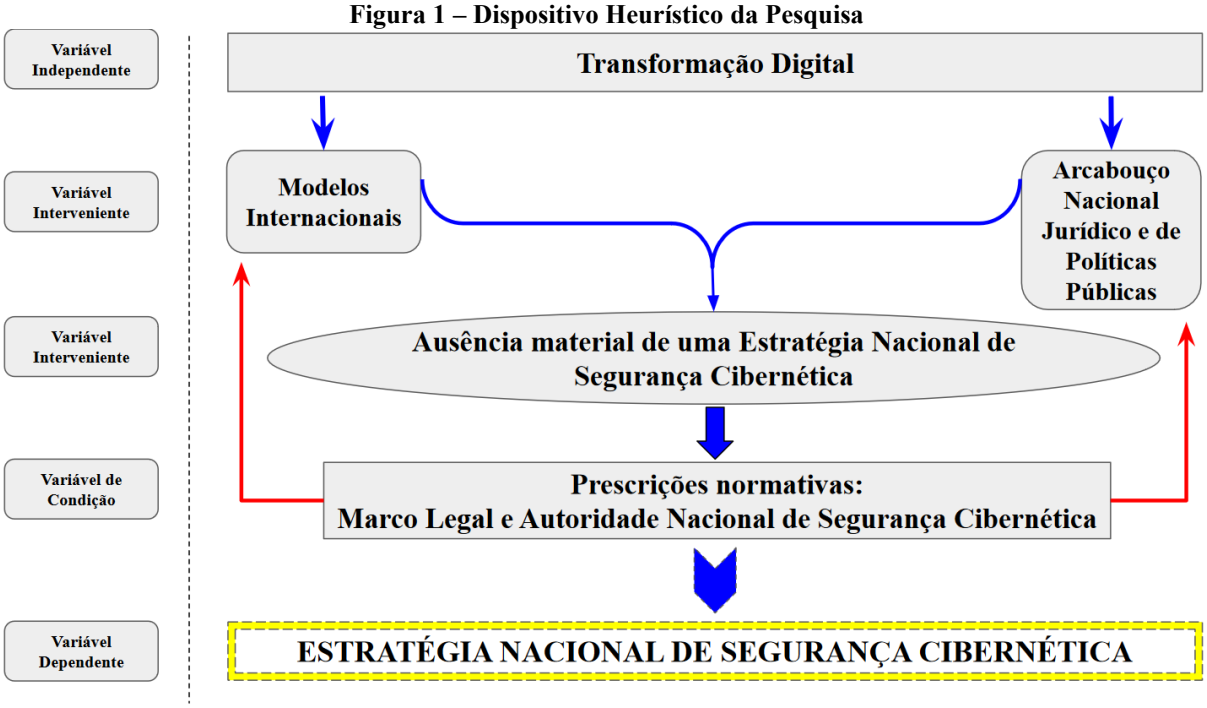
Dessa forma, o problema de pesquisa é: existe uma Estratégia Nacional de Segurança Cibernética no Brasil em sentido material? Em resposta ao problema de pesquisa, formulou-se como hipótese central do trabalho o fato de que embora o país possua uma ENSC formal, ela materialmente não se configura como tal.

Partindo da hipótese de inexistência material de uma ENSC, foram propostas prescrições normativas, as quais condicionam o esforço que deve ser empreendido pelo país na

busca de uma ENSC. Trata-se do estabelecimento do Marco Legal em segurança cibernética e da instituição de uma Autoridade Nacional de Segurança Cibernética. É justamente esse esforço que se buscou traduzir no título do trabalho.

Foi elaborado o quadro abaixo com a finalidade de ilustrar os passos analíticos empenhados, fazendo-se uso do esquema de Van Evera (1997, p. 7-11), com a indicação das variáveis e a hipótese central da pesquisa.

Figura 1 – Dispositivo Heurístico da Pesquisa



Fonte: Autora.

Explicando-se o quadro, tem-se como fenômeno causal a variável independente de Transformação Digital no seu sentido mais abrangente de efeitos econômicos e sociais dos processos de digitização e digitalização. Como fenômenos intervenientes tem-se a resposta da comunidade internacional por meio dos modelos que guiam o desenvolvimento de ENSC e, no contexto brasileiro, a resposta manifestada no Arcabouço Nacional Jurídico e de Política Públicas. A conjunção dessas variáveis permite confirmar a hipótese de inexistência material de uma ENSC no Brasil.

Com base nesse diagnóstico, as prescrições de política pública configuram uma variável de condição, como pressuposto antecedente, que impacta diretamente na variável dependente, qual seja a existência de uma ENSC em termos materiais e formais.

Assim, adotando a tipologia de tese apresentada por Van Evera (1997, p. 91), a tese comportou a avaliação de política pública, notadamente associada à E-Ciber, e, ao mesmo

tempo, prescrição de política pública, uma vez que buscou justamente contribuir para o seu processo de aprimoramento.

Nesse sentido, tem-se uma pesquisa qualitativa, centrada no Estudo de Caso dos três modelos; e da E-Ciber e demais instrumentos que compõem o Arcabouço Nacional relacionado. Essa pesquisa, abarcou uma parte essencialmente descritiva (GERRING, 2012), na medida em que se fazia necessária a descrição, tanto do fenômeno da edição das políticas públicas e marcos em segurança cibernética, quanto dos modelos, e a sua contextualização, a fim de permitir a análise e verificação da hipótese central.

Para tanto, foi utilizada pesquisa bibliográfica e documental. A primeira almejou o embasamento teórico referente à Quarta Revolução Industrial, à Transformação Digital, à Segurança Internacional, à segurança cibernética e aos arcabouços existentes de enfrentamento desse problema, ou seja, estratégias e políticas nacionais. Já a pesquisa documental abrangeu os atos normativos brasileiros, assim como diversos documentos produzidos por organizações, órgãos e entidades nacionais e internacionais que atuam nessa seara.

Nesse ponto, nacionalmente, destacou-se, em termos de pesquisa documental: Estratégia Nacional de Defesa (END), PNSI, E-Digital, E-Ciber; e outros documentos e instruções do Gabinete de Segurança Institucional da Presidência da República (GSI/PR). Já internacionalmente, foram abordadas as Resoluções da Assembleia Geral das Nações Unidas; assim como relatórios, resoluções e materiais da UIT, da OCDE e do GCSCC.

Finalizado o desenho da pesquisa, avança-se para uma explanação sobe a definição de trabalho de segurança cibernética, mostrando as diferentes abordagens e terminologias.

1.3 DIMENSÕES DE SEGURANÇA CIBERNÉTICA E CONCEITO

Após uma apresentação do objeto do trabalho, da revisão bibliográfica que o embasa e da descrição de como a pesquisa foi conduzida, busca-se apresentar e explorar o conceito de segurança cibernética adotado na pesquisa. Esse exercício demonstra as diversas terminologias que procuram descrever o fenômeno e as diferentes perspectivas que são contempladas, a fim de indicar a nomenclatura utilizada e harmonizar o seu uso para fins do presente trabalho.

Certamente um dos maiores desafios do presente esforço é a assertiva definição de trabalho do objeto sobre qual a pesquisa se debruça. Embora a delimitação, o recorte que se pretende dar ao fenômeno seja de extrema relevância, a definição do conceito "segurança cibernética" não é tarefa menos complexa, sendo encontrada na literatura acadêmica, documentos normativos e pesquisa bibliográfica uma série de terminologias que buscam ou

pretendem tratar do mesmo fenômeno. Algumas terminologias são utilizadas como sinônimos, porém nem todas abarcam as mesmas perspectivas, as quais já se adianta, são inúmeras.

Existe um extensivo rol de terminologias que tenta exprimir essa conjuntura e o vocábulo "ciber" é um dos grandes destaques, normalmente acrescentado a diversos outros vocábulos[8]. Essa utilização busca construir certo paralelismo entre a realidade física, então como era conhecida, e essa nova fronteira, novo espaço que cada dia mais concentra nossas atividades sociais, econômicas, culturais, profissionais, educacionais e cívicas. Não há limites para a transformação digital da vida em sociedade e dos setores da economia e a Pandemia da Covid-19 acelerou e tornou urgente um processo que já estava em constituição.

Segurança Cibernética, Segurança Digital, Cibersegurança, Segurança da Informação, Segurança na Internet, Segurança da Internet, Segurança na Rede, Segurança on-line, Riscos Digitais, Crimes Cibernéticos, Crimes Informáticos, Crimes de Computador, Incidentes de Segurança, Incidente Cibernético, Ciberataques, Ataques Cibernéticos, Ciberespaço, Espaço Cibernético, Cibernética, Defesa Cibernética, etc. Talvez uma página inteira sequer fosse suficiente para listar todas as nomenclaturas encontradas.

Como já adiantado, essas terminologias não são necessariamente sinônimas, embora eventualmente possam ser utilizadas para descrever o mesmo fenômeno. Outrossim, o trabalho não tem como objetivo conceituar cada um desses termos. Menciona-se a existência da diversidade terminológica a fim de alertar sobre a sua existência, algo que adiciona ainda mais complexidade para a sua compreensão (AYRES PINTO, GRASSI, 2020, p. 110).

O presente trabalho utilizará a terminologia "segurança cibernética" e sua escolha não é aleatória. Em primeiro lugar, remonta-se a um dos primeiros instrumentos internacionais que se destina a endereçar o fenômeno, com o intuito de assegurar a efetividade da persecução penal. Nesse sentido, o primeiro tratado celebrado para combater o uso ilício dessas tecnologias foi a Convenção de Budapeste, assinada em 23 de novembro de 2001[9], a qual já adotava a terminologia crimes cibernéticos e cuja adesão foi aprovada recentemente no Brasil[10].

Outro marco internacional, a Resolução nº 239 da 57° Sessão da AGNU, realizada no ano de 2002, intitulada "Criação de uma Cultura Global de Segurança Cibernética", menciona,

[8]Embora não seja objeto do trabalho, interessante notar que a obra de Thomas Rid, intitulada "*Rise of the Machines: a cybernetic history*" (2016) oferece um panorama histórico e cultural do surgimento do prefixo ciber, bem como das terminologias cibernética e espaço cibernético, traçando uma linha que remonta à Década de 1940.

[9] Texto oficial da Convenção, lista de países aderentes, vigência e protocolos adicionais podem ser consultados em: http://conventions.coe.int/Treaty/en/Treaties/Html/185.htm . Acesso em: 22 out. 2022.

[10] Decreto Legislativo nº 37, de 2021, promulgado pelo Congresso Nacional dia 16 de dezembro de 2021. Maiores informações, consultar: https://legis.senado.leg.br/norma/35289207/publicacao/35300588. Acesso em: 26 out 2022.

pela primeira vez em uma de suas resoluções, o termo "segurança cibernética" e aborda o aspecto cultural do problema que afronta a segurança da informação (UNGA, 2002b).

Ainda no Plano Internacional, a UIT, agência especializada do Sistema das Nações Unidas para as TICs, lançou em 2007 a Agenda Global de Segurança Cibernética (ITU, 2008; 2009b), com objetivo de oferecer aos Estados-membros uma abordagem flexível para o enfrentamento desses desafios, reiterando a utilização da terminologia "segurança cibernética". Esta, foi definida pelo Grupo de Estudos 17, um dos Grupos de Estudos da entidade, líder na elaboração de padrões de segurança, na Recomendação X.1205 do Setor de Normalização da UIT (ITU, 2009a, p. 2-3, tradução nossa)[11]:

> A segurança cibernética é a coleção de ferramentas, políticas, conceitos de segurança, segurança salvaguardas, diretrizes, abordagens de gerenciamento de risco, ações, treinamento, melhores práticas, garantia e tecnologias que podem ser usadas para proteger o ambiente cibernético e os ativos da organização e do usuário. Os ativos da organização e do usuário incluem dispositivos de computação conectados, pessoal, infraestrutura, aplicativos, serviços, sistemas de telecomunicações e a totalidade das informações transmitidas e/ou armazenadas no ambiente cibernético. A segurança cibernética se esforça para garantir a obtenção e manutenção das propriedades de segurança da organização e dos ativos do usuário em relação a riscos de segurança relevantes no ambiente cibernético. Os objetivos gerais de segurança incluem o seguinte: disponibilidade; integridade, que pode incluir autenticidade e não repúdio; e confidencialidade.

A Agência da União Europeia para a Cibersegurança (ENISA) elaborou um estudo em 2017 apresentando um panorama sobre as terminologias de segurança cibernética e correlatos e define segurança cibernética (terminologia por ela adotada) como:

> **Segurança Cibernética** abrange todos os aspectos de prevenção, previsão; tolerância; detecção; mitigação, remoção, análise e investigação de **incidentes cibernéticos**. Considerando os diferentes tipos de componentes do espaço cibernético, a segurança cibernética deve abranger os seguintes atributos: **Disponibilidade, Confiabilidade, Segurança, Confidencialidade, Integridade, Manutenibilidade** (para sistemas, informações e redes tangíveis) **Robustez, Sobrevivência, Resiliência** (para apoiar a dinamicidade do ciberespaço), **Responsabilidade, Autenticidade e Não Repúdio** (para apoiar a segurança da informação). (ENISA, 2017, tradução nossa, grifos do autor).

[11] "*Cybersecurity is the collection of tools, policies, security concepts, security safeguards, guidelines, risk management approaches, actions, training, best practices, assurance and technologies that can be used to protect the cyber environment and organization and user's assets. Organization and user's assets include connected computing devices, personnel, infrastructure, applications, services, telecommunications systems, and the totality of transmitted and/or stored information in the cyber environment. Cybersecurity strives to ensure the attainment and maintenance of the security properties of the organization and user's assets against relevant security risks in the cyber environment. The general security objectives comprise the following: Availability; Integrity, which may include authenticity and non-repudiation; and Confidentiality*" (ITU, 2009a, p. 2-3).

Interessante notar que a iniciativa da ENISA também aborda as terminologias de segurança da informação e segurança da informação e de rede, as quais são expressamente tratadas como subconjuntos de segurança cibernética, ao contrário, por exemplo, da concepção brasileira, como se verá na evolução do texto. Em um trabalho anterior específico sobre a definição de segurança cibernética e a identificação de sobreposições e lacunas (ENISA, 2015), a mesma organização explora as terminologias de seis organizações, identificando as dimensões endereçadas e os conteúdos compartilhados, bem como as singularidades encontradas. Nesse trabalho foram examinadas as terminologias do Comitê de Sistemas de Segurança Nacional dos Estados Unidos (CNSS); Instituto Europeu de Normas de Telecomunicações (ETSI); Instituto Nacional de Padrões e Tecnologia dos Estados Unidos (NIST); Organização do Tratado do Atlântico Norte (OTAN); Organização Internacional de Normalização (ISO); e UIT (2015, p. 19).

Esse esforço foi realizado pela ENISA em parceria com o Grupo de Coordenação de Segurança Cibernética do Comitê Europeu de Normalização, Comitê Europeu para a Normalização Eletrotécnica (CENELEC) e ETSI. Esse Grupo de Coordenação foi criado em 2011 e é o único grupo conjunto que reúne três organizações europeias oficiais de normalização e com mandato para coordenar padrões de segurança cibernética dentro das suas respectivas organizações (2015, p. 8). Essa iniciativa específica decorre de atendimento a um estudo, realizado em resposta à Estratégia de Segurança Cibernética da União Europeia aprovada em 2013[12], que contemplou recomendação específica sobre a necessidade de revisão das definições do termo "*segurança cibernética*" (ENISA, 2015, p. 6).

O documento esclarece que chegar a um entendimento comum sobre o conceito é um desafio enorme e que poderia não ser possível harmonizar a definição e uso do termo. Assim, apresenta como finalidade do trabalho a descrição das noções divergentes, a fim de orientar uma compreensão adequada do termo para ser usado no contexto do uso pretendido pelos atores e elaboradores de políticas públicas. Além disso, uma finalidade adicional seria justamente listar as organizações que trabalham na normalização de segurança cibernética, ou seja, organizações que desenvolvem padrões de segurança cibernética, fornecendo um panorama das atividades e identificando lacunas e duplicações (ENISA, 2015, p. 8-9).

[12] Texto integral da Estratégia de Segurança Cibernética da União Europeia aprovado em 12 de setembro de 2013 pode ser consultado em: https://www.europarl.europa.eu/doceo/document/TA-7-2013-0376_EN.html. Acesso em: 27 out. 2022. Cumpre ressaltar que em dezembro de 2020 a União Europeia aprovou nova Estratégia de Segurança Cibernética, a qual pode ser consultada em: https://digital-strategy.ec.europa.eu/en/policies/cybersecurity-strategy. Acesso em: 01 fev. 2023.

Nota-se que até mesmo a grafia do termo em inglês não é uniforme, sendo possível identificar até mesmo diferenças na utilização da grafia "*cybersecurity*" e "*cyber security*" (ENISA, 2015, p. 10), problema que não é enfrentado na Língua Portuguesa, embora possamos identificar as terminologias segurança cibernética e cibersegurança, que também adicionam complexidade à discussão e dúvidas sobre os respectivos conceitos.

Das definições abordadas, uma das mais abrangente, a elaborada pela UIT na Recomendação X.1205 já foi citada anteriormente, cabendo trazer a definição apresentada por um dos organismos de normalização, a ISO, que conceitua segurança cibernética como a preservação da confidencialidade, integridade e disponibilidade da informação no ambiente cibernético (ENISA, 2015, p. 15). Aqui se deve pontuar que o conceito de segurança da informação da ISO (ISO/IEC 27000)[13] é definido como a preservação da confidencialidade, integridade e disponibilidade da informação, e, dessa forma, reveste-se de maior abrangência que o atrelado à segurança cibernética. Nesse último reside o elemento de qualificação "ambiente cibernético", esclarecendo-se, assim, que segurança cibernética estaria abarcada dentro do espectro maior de segurança da informação para essa organização.

Das definições de organismos internacionais, cita-se ainda a terminologia utilizada pela OCDE, a qual adota segurança digital para ressaltar a perspectiva social e econômica do fenômeno. Nota-se que o documento que acompanhada a Recomendação de 2015 da OCDE sobre Gerenciamento de Riscos de Segurança Digital para Prosperidade Econômica e Social na sua introdução expressa que os assuntos de segurança digital são frequentemente capturados na terminologia abrangente "segurança cibernética", a qual cobre diversas dimensões desde tecnologia até aspectos econômicos e sociais; jurídicos; de aplicação da lei; de direitos humanos; de segurança nacional; inteligência; estabilidade internacional; e guerra, dentre outros (OCDE, 2015, p. 19-20).

Ademais o documento justamente esclarece que esse uso disseminado da terminologia "segurança cibernética" mascara a amplitude e complexa natureza desse assunto, destacando que segurança digital pode ser abordada por ao menos quatro diferentes perspectivas: tecnológica; crimes cibernéticos; segurança nacional e internacional; e prosperidade social e econômica. O mandato da OCDE residiria em abordar segurança digital da perspectiva social e econômica, a qual contempla a criação de riqueza; inovação; crescimento; competitividade e emprego em todos os setores da economia, assim como aspectos relacionados às liberdades

[13] A Norma ISO/IEC 27000 está publicamente disponível em: https://standards.iso.org/ittf/PubliclyAvailable Standards/index.html. Acesso em: 30 out. 2022.

individuais, saúde, educação, cultura, participação democrática, ciência, lazer e outras dimensões do bem-estar nas quais o ambiente digital está guiando o processo (2015, p. 19-20).

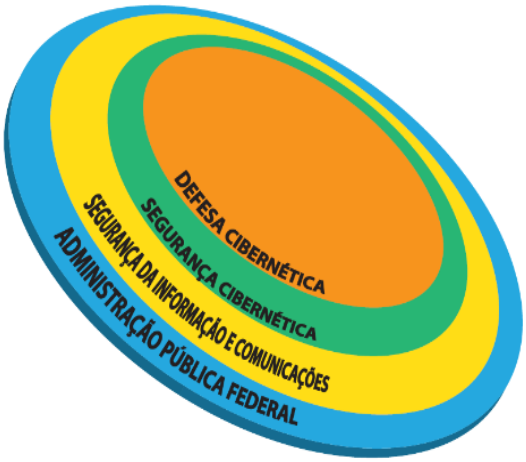
Após ser apresentado o panorama de como é conceituada segurança cibernética em diversas organizações internacionais, inclusive indicando as diferenças de terminologia existentes, volta-se ao plano nacional. Segurança Cibernética para o GSI/PR e, portanto, para toda a APF, é definida no Glossário de Segurança da Informação do Departamento de Segurança de Informação do GSI/PR (BRASIL, 2019d) como:

> [...] ações voltadas para a segurança de operações, de forma a garantir que os sistemas de informação sejam capazes de resistir a eventos no espaço cibernético capazes de comprometer a disponibilidade, a integridade, a confidencialidade e autenticidade dos dados armazenados, processados ou transmitidos e dos serviços que esses sistemas ofereçam ou tornem acessíveis.

Sem muito adiantar a seção 3.4 do Capítulo III que tratará da PNSI, apenas se registra que, à semelhança do conceito da ISO, no qual segurança cibernética é um subconjunto de segurança da informação, de forma análoga, esses conceitos são tratados nas políticas públicas brasileiras. Nesse racional, a PNSI expressamente menciona que segurança da informação abrange: segurança cibernética; defesa cibernética; segurança física e proteção de dados organizacionais; e ações destinadas a assegurar disponibilidade, integridade, confidencialidade e autenticidade da informação (BRASIL, 2018f). Ademais, também pode ser apontado que o Glossário de Segurança da Informação do DSI do GSI/PR define segurança da informação como "[...] ações que objetivam viabilizar e assegurar a disponibilidade, a integridade, a confidencialidade e a autenticidade das informações" (BRASIL, 2019d).

A antiga Estratégia de Segurança da Informação e Comunicações e de Segurança Cibernética da Administração Pública Federal 2015-2018 (BRASIL, 2015a) traz ilustração que exemplifica essa visão de segurança da informação e de segurança cibernética:

Figura 2 - Visão em Camadas: Segurança da Informação, Segurança Cibernética e Defesa Cibernética



Fonte: Brasil (2015a, p. 34).

Diante dessas diferentes terminologias e definições, as quais demonstram as diferentes abordagens e dimensões do nosso objeto, reforça-se que o presente trabalho adotou a terminologia segurança cibernética, harmonizando-se com a terminologia escolhida pelas nossas políticas públicas[14]. Também refletindo a opção de diversas organizações internacionais, como UIT, ENISA e, até mesmo, AGNU, as quais corroboram a utilização desses termos nos seus instrumentos.

Na mesma esteira e, considerando que o objeto do trabalho tem delimitação focada na ENSC brasileira e de prescrição de política pública relacionada, adota-se o conceito do Glossário de Segurança da Informação do DSI do GSI/PR, que incorpora a visão de segurança cibernética como um dos subconjuntos de segurança da informação, consoante figura acima apresentada, e que está alinhada à definição constante das Normas da ISO. Essa definição difere de outras definições ainda mais abrangentes como da UIT e da ENISA, as quais não se limitam a garantir a tríade da segurança da informação (confidencialidade, integridade e disponibilidade) no ambiente cibernético, mas também abrangem ativos físicos relacionados.

Nesse ponto cabe atentar para as consequências desse ponto de inflexão entre as terminologias, de abrangência de ativos físicos, visto que a opção pela perspectiva mais estrita de segurança cibernética demanda a elaboração de instrumentos mais amplos. Por exemplo, além de uma ENSC, será necessário o desenvolvimento de políticas que contemplem os outros aspectos não abarcados pelo conceito adotado, motivo pelo qual o Brasil possui uma PNSI, uma Estratégia Nacional de Segurança da Informação (ENSI) e uma ENSC.

[14] Cumpre destacar a presença do vocábulo cibersegurança em alguns momentos do texto para a fiel citação de nome de obras, entidade e proposição de autores.

Ademais, outro ponto de atenção é a necessária compreensão dessas diferenças nos debates e negociações internacionais, visto que segurança da informação, como já referido, detém um alcance maior e inclusive pode abarcar, como no caso brasileiro, o tratamento de informações classificadas.

Por todo o exposto, a opção terminológica e conceitual do Glossário de Segurança da Informação do DSI do GSI/PR alinha-se às políticas públicas brasileiras, facilita a compreensão e promove a harmonização quando da descrição e análise dessas políticas, bem como quando da prescrição de política pública. Entretanto, não se olvida da importância de contextualizá-la dentro das políticas mais amplas relacionadas à segurança da informação, motivo pelo qual a PNSI é apresentada no Capítulo III do trabalho, passando-se agora à apresentação das conclusões parciais do presente capítulo.

1.4 CONCLUSÕES PARCIAIS

Este capítulo contemplou a Introdução do presente trabalho que abarcou marco teórico; desenho de pesquisa; e dimensões de segurança cibernética e conceito.

A primeira conclusão que se apontou é que a segurança cibernética se assenta em um quádruplo aspecto: Transformação Digital, Quarta Revolução Industrial, Desenvolvimento e Segurança Internacional. A conexão entre esses elementos, espera-se, que tenha sido suficientemente demonstrada na operacionalização das obras citadas no Marco Teórico, as quais serviram de inspiração, enquanto construto heurístico para análise e formulação de prescrições normativas em segurança cibernética: Marco Legal e Autoridade Nacional de Segurança Cibernética.

Salientou-se também o caráter sistêmico do tema por intermédio da sua dominância nas pautas das organizações internacionais. Dentre organismos e fóruns que abordam a temática citou-se: Assembleia Geral das Nações Unidas, Organização dos Estados Americanos; Organização para a Cooperação e Desenvolvimento Econômico (OCDE); e União Internacional de Telecomunicações (UIT).

Para além da inserção do tópico na contextualização mais ampla, o Marco Teórico também incorporou a resposta doméstica dos países aos desafios relacionados à promoção de segurança cibernética, traduzida nas Estratégias Nacionais de Segurança Cibernética (ENSCs).

Finalizando-se a sistematização da literatura, aportou-se as contribuições de Bresser-Pereira ao trabalho, as quais foram transpostas na tese para advogar pela necessidade de importação e, consequente adaptação de modelos estudados; pela relevância da esfera não-

estatal considerando o papel de todos os atores; e pelo reforço do núcleo de propriedade estatal do Aparelho do Estado, argumento que ilumina o raciocínio de proposição da instituição de uma Autoridade Nacional de Segurança Cibernética.

Centrou-se na análise do contexto brasileiro, buscando o aprimoramento das nossas políticas públicas, confrontando-o com os elementos trazidos pelas iniciativas da OCDE, da UIT e do Centro Global de Capacidade de Segurança Cibernética da *Oxford Martin School* da Universidade de Oxford (GCSCC). Essas iniciativas focam nas ENSCs, as quais foram denominadas de 'modelos', para fins da presente tese.

A correlação desses acúmulos permitiu concluir que a formulação da ENSC diz respeito a um esforço a ser empreendido por toda nação. E não, como usualmente se pensa, um esforço de indivíduos ou organizações. É justamente essa percepção que se buscou traduzir no título do trabalho.

De fato, a instituição de um Marco legal e de uma Autoridade Nacional de Segurança Cibernética emerge como condição desse esforço e envolve vários desafios, os quais foram endereçados nos delineamentos apresentados para cada umas dessas duas proposições. Nesse sentido, estipulou-se detalhadamente no Capítulo IV um conteúdo, ou seja, uma prescrição mínima que precisa ser incorporada aos debates e aos respectivos instrumentos.

Dessa forma, procurou-se ajustar o marco teórico ao problema de pesquisa e à hipótese. Identificou-se como problema de pesquisa o questionamento sobre a existência material da ENSC brasileira. Lembrando-se, como referido no decurso desse capítulo, a utilização da distinção entre forma e materialidade.

Retoma-se a utilização da dicotomia formal *versus* material, usual pelos vários ramos das Ciências Jurídicas e Sociais, para apresentar a diferença entre o cumprimento de uma formalidade e rito (formal) e o conteúdo, a substância de determinado ato (material).

A hipótese central do trabalho é a de que embora o país formalmente possua uma ENSC, visto que a Estratégia Nacional de Segurança Cibernética (E-Ciber) foi aprovada e está vigente, materialmente não se configura como tal. Nessa linha, anteciparam-se as duas prescrições normativas que, sem se confundirem com a ENSC, são condições inarredáveis para sua elaboração: estabelecimento do Marco Legal e instituição de uma Autoridade Nacional de Segurança Cibernética, previamente mencionados. Portanto, a tipologia adotada pela tese é, principalmente, a prescrição de política pública, conforme Van Evera (1997, p. 91).

Também se procurou tratar da abrangência dos limites difusos do conceito de segurança cibernética. Conquanto se tenha procurado delimitar a pesquisa, atrelando-o ao estudo das ENSCs, o tema é mais vasto e complexo.

Para esses fins, estipulou-se que a terminologia “segurança cibernética” e diversos termos relacionados encerram diferentes dimensões, perspectivas e abordagens, adotando-se a terminologia “segurança cibernética”. Como definição de trabalho, elegeu-se o conceito constante do Glossário de Segurança da Informação do Gabinete de Segurança Institucional da Presidência da República. Essa escolha reside no fato do trabalho prover prescrições normativas às políticas públicas brasileiras e, portanto, a harmonização terminológica com o Arcabouço Nacional é natural e necessária.

Após essas premissas iniciais fixadas nesse Capítulo, abre-se o Capítulo II, com o detalhamento da pesquisa documental, despontando-se a apresentação dos três modelos da OCDE, UIT e GCSCC.

2 MODELOS DE POLÍTICAS E ESTRATÉGIAS NACIONAIS DE SEGURANÇA CIBERNÉTICA

A crescente relevância e emergência da temática na agenda internacional fez com que diversas organizações internacionais desenvolvessem iniciativas nessa seara direcionadas a diferentes dimensões de segurança cibernética. Uma dessas dimensões foi justamente a governança do tema no âmbito doméstico, abrangendo tanto a parte instrumental quanto a parte institucional, a fim de que os países pudessem estruturar estrategicamente as suas ações de fomento à segurança cibernética.

Dentre as diversas iniciativas que surgiram com esse foco específico, o presente trabalho foca em dois esforços desenvolvidos por organizações intergovernamentais, quais sejam da OCDE e da UIT, bem como um modelo proposto pela academia, particularmente o modelo criado pelo GCSCC, da *Oxford Martin School* da Universidade de Oxford.

Dessa forma, passa-se a discorrer sobre cada uma dessas iniciativas, com destaque especial ao recorte metodológico do trabalho, também apresentando brevemente a organização, mandato e estrutura das entidades, conforme a pertinência, iniciando-se com a OCDE.

2.1 ORGANIZAÇÃO PARA A COOPERAÇÃO E DESENVOLVIMENTO ECONÔMICO

A primeira iniciativa que será apresentada é da OCDE, que é justamente a organização intergovernamental precursora no desenvolvimento de diretrizes e recomendações relacionadas à segurança da informação, como será a seguir demonstrado.

O nascimento da OCDE remonta ao período após o fim da Segunda Guerra Mundial, sendo sucessora da Organização para Cooperação Econômica Europeia (OCEE), a qual foi criada para administrar o Plano Marshall para a reconstrução da Europa. Em 1960 a OCEE foi transformada na OCDE com a assinatura de Convenção em Paris pelos seus membros mais Canadá e Estados Unidos, com vigência a partir de 30 de setembro de 1961, data que marca o nascimento oficial da entidade (OECD, 2020c, p. 3).

Atualmente, a OCDE conta com trinta e oito países-membros[1], sendo que o Brasil, assim como Argentina, Bulgária, Croácia, Peru e Romênia, iniciou as tratativas com a OCDE para acessão, seguindo decisão do Conselho da OCDE em 25 de janeiro de 2022. Em junho de 2022

[1] Informações atualizadas sobre os Estados-membros e parceiros podem ser consultadas no sítio oficial da entidade, disponível em: https://www.oecd.org/about/. Acesso em: 12 ago. 2022.

foi aprovado o roteiro de adesão do Brasil[2], constituindo-se uma das prioridades do então Governo de Jair Bolsonaro (OCDE, 2020b, p. 6).

Relembra-se que o Brasil já fazia parte do Programa de Engajamento Aumentado desde 2007, ao lado de África do Sul, China, Índia e Indonésia (OCDE, 2020c, p. 21), sendo que a soma dos membros e desses parceiros, totaliza quarenta e três países e responde por oitenta por cento do comércio e investimento mundial (OCDE, 2020c, p. 21). Ademais, o Brasil já havia apresentado em maio de 2017 o pedido formal de acessão à organização e trabalhado domesticamente, desde então, para aderir às recomendações e alinhar as políticas aos instrumentos e às boas práticas da organização (THORSTENSEN e NOGUEIRA, 2020, p. 45).

Nesse sentido, até o final de 2020, o Brasil já havia aderido a noventa e quatro instrumentos legais da OCDE; participava com status de associado ou membro de vinte e cinco dos seus órgãos; e engajava-se com *status* de participante (participação apenas nas sessões não confidenciais) em vinte e cinco comitês, grupos e reuniões conjuntas (OCDE, 2020b, p. 61-64).

Aqui cabe a observação de que embora as recomendações adotadas pelo Conselho não sejam vinculantes aos aderentes, representam um compromisso político e geram a expectativa de que os aderentes adotarão seu melhor esforço para implementá-las. Essa expectativa pode se tornar bastante significativa diante de um processo de adesão à organização, como o processo em curso de adesão brasileira à OCDE. Ainda cumpre uma segunda nota, a qual se refere à inexistência de clareza sobre a continuidade da priorização do processo de adesão do Brasil à OCDE no novo Governo do Presidente Luiz Inácio Lula da Silva, algo que será clarificado somente após a conclusão dessa pesquisa.

Nos termos do art. 1º da Convenção da OCDE, os objetivos da entidade são promover políticas para: a) atingir o mais alto e sustentável crescimento econômico, de emprego e de padrão de vida nos países-membros, enquanto mantendo a estabilidade financeira e, assim, contribuindo para o desenvolvimento da economia mundial; b) contribuir para sólida expansão econômica nos países-membros e não membros no processo de desenvolvimento econômico; e c) contribuir para a expansão comércio mundial de maneira multilateral e não discriminatória, de acordo com as obrigações internacionais (OCDE, 2020c, p. 3).

Na busca desses objetivos, os membros da OCDE deverão, de forma individual e conjunta, com espeque no art. 2° da Convenção: promover o uso eficiente dos recursos econômicos; promover o desenvolvimento de recursos nos campos científico e tecnológico,

[2] Informações atuais sobre o processo de adesão podem ser consultadas na página da OCDE dedicada ao Brasil, disponível em: https://www.oecd.org/latin-america/countries/brazil/. Acesso em: 12 ago. 2022. Da mesma forma, também podem ser consultadas na página do governo brasileiro dedicada a esse processo, disponível em: https://www.gov.br/casacivil/pt-br/assuntos/ocde. Acesso em: 12 ago. 2022.

fomentando pesquisa e promovendo capacitação; perseguir políticas desenhadas para atingir o crescimento econômico e a estabilidade financeira interna e externa e evitar desenvolvimentos que possam colocar em risco as suas economias ou as de outros países; perseguir esforços para reduzir ou abolir obstáculos à troca de bens e serviços e atuais pagamentos, bem como manter e estender a liberalização do movimento de capitais; e contribuir para o desenvolvimento econômico dos países-membros e não membros em processo de desenvolvimento econômico pelos meios apropriados, e, em particular, pelo fluxo de capital para países, considerando a importância para essas economias de receber assistência técnica e de assegurar a expansão de mercados de exportação[3].

Em termos organizacionais, a estrutura da OCDE é composta de um conselho, integrado pelos representantes de cada um dos Estados-membros e da Comissão Europeia, uma secretaria e comitês. O Secretário-Geral da OCDE preside o Conselho e lidera o secretariado na condução dos esforços da organização (OCDE, 2020c, p. 5). O trabalho da OCDE é desenvolvido em mais de trezentos comitês, grupos de trabalho e grupo de experts, ao quais trabalham em todas as áreas relacionadas à elaboração de políticas[4].

Como antecipado, a OCDE é pioneira no desenvolvimento de estudos e recomendações relacionadas à segurança da informação, cabendo lembrar que em 1992 o Conselho aprovou as Diretrizes da OCDE para a Segurança dos Sistemas de Informação (OCDE, 1992), as quais foram desenvolvidas em grupo de trabalho criado no âmbito do Comitê sobre Políticas de Informação, Computadores e Comunicação (*Committee on Information, Communications and Computer Policy - ICCP*), que compunha a Diretoria para Ciência, Tecnologia e Indústria.

Considerando que as TICs transformaram as economias e as sociedades, sendo fundamentais para o desenvolvimento social, cultural e econômico, o ICCP foi criado para tratar das questões políticas que são chave para a Economia da Internet, relacionadas à conectividade, à criatividade e à confiança. Essa última refere-se justamente a como dar proteção e fortalecer a autonomia dos consumidores e usuários.

O Comitê possuía 4 (quatro) grupos de trabalho: Grupo de Trabalho sobre Políticas de Serviços e Infraestrutura de Comunicações; Grupo de Trabalho sobre Economia da Informação; Grupo de Trabalho sobre Segurança da Informação e Privacidade; e Grupo de Trabalho sobre Indicadores da Sociedade da Informação (OCDE, 2010; CRAVO, 2012, p. 112).

---

[3] O texto integral da Convenção da OCDE pode ser consultado em: https://www.oecd.org/general/conventionontheorganisationforeconomicco-operationanddevelopment.htm. Acesso em: 12 ago. 2022.

[4] Sobre a organização dos trabalhos da OCDE, ver: https://www.oecd.org/about/structure/. Acesso em 13 ago. 2022.

A análise e o desenvolvimento de políticas; elaboração de recomendações e diretrizes para elaboração de políticas; troca de experiências entre os Estados-membros; e iniciativas de indicadores eram algumas das atividades principais do ICCP (OCDE, 2010), destacando-se na presente tese, o Grupo de Trabalho sobre Segurança da Informação e Privacidade (*Working Party on Information Security and Privacy - WPISP*). O WPISP constituía-se como um fórum intergovernamental, desenvolvendo, por consenso, opções de políticas com o objetivo de sustentar a confiança em uma sociedade global conectada e contando com participação de vários atores (OCDE, 2005).

Cita-se como resultado dos esforços do grupo, a elaboração das Diretrizes da OCDE de 2002 para a Segurança das Redes e Sistemas de Informação: em Direção à Cultura de Segurança, as quais substituíram as diretrizes de 1992 (OCDE, 2002).

Com relação às diretrizes aprovadas em 2002, é interessante notar que o processo de revisão foi contextualizado pela dramática mudança do ambiente de tecnologia da informação plasmado nas diretrizes de 1992. Tal mudança trouxe novos desafios e demandou outro olhar de todos os atores para a segurança, especialmente diante da crescente interconectividade. Ademais, esse esforço de revisão foi acelerado pelos eventos de 11 de setembro de 2001, consoante destacado no próprio documento na parte dedicada ao procedimento de elaboração (OCDE, 2002, p. 17).

Cabe mencionar que os princípios elencados por essas diretrizes aprovadas em 2002 constam do Anexo à Resolução da AGNU nº 239, aprovada na 57º (quinquagésima sétima) sessão, realizada em 2002, intitulada *Criação de uma Cultura Global de Segurança Cibernética* (UNGA, 2002b). Essa resolução é um marco de trabalho importante nessa seara para o órgão máximo das Nações Unidas, sendo a primeira vez que essa terminologia é utilizada no âmbito das resoluções do órgão e que a dimensão cultural do problema é enfrentada[5].

Embora a resolução não mencione expressamente o vínculo com o trabalho da OCDE, os princípios elencados são exatamente os mesmos nove princípios constantes das diretrizes aprovadas pela OCDE em 2002, os quais denotam a atualização dos princípios constantes das Diretrizes de 1992, demonstrando a relevância do trabalho desenvolvido pela OCDE.

O ICCP teve seu mandato expirado em 2013 e o WPISP tornou-se o Grupo de Trabalho sobre Segurança e Privacidade na Economia Digital (*Working Party on Security and Privacy in the Digital Economy - WPSPDE*), dentro do Comitê de Políticas sobre Economia Digital (*Committee on Digital Economy Policy - CDEP*). Esse Grupo foi responsável pelo processo de

[5] Para histórico de enfrentamento de questões relacionadas à segurança cibernética no âmbito de resoluções da Assembleia Geral das Nações Unidas, ver CRAVO, 2012, p. 59-71.

revisão das diretrizes de 2002, que resultou na Recomendação de 2015 da OCDE sobre Gerenciamento de Riscos de Segurança Digital para Prosperidade Econômica e Social (OCDE, 2015, p. 3).

Por fim, em termos organizacionais, ainda falta mencionar a estrutura institucional e mandato do WPSPDE, que sofreu nova alteração em 2019, em face da crescente complexidade dos desafios relacionados à proteção de dados e privacidade. Embora possuam forte intersecção, esses temas não se confundem com questões de segurança e provocaram uma importante separação desses assuntos. Assim, o WPSPDE passou a endereçar tão somente segurança digital, agora denominado de Grupo de Trabalho sobre Segurança na Economia Digital (*Working Party on Security in the Digital Economy – WPSDE*). E para os outros temas, restou criado novo grupo de trabalho específico de governança de dados e privacidade - Grupo de Trabalho sobre Governança de Dados e Privacidade na Economia Digital (*Working Party on Data Governance and Privacy on the Digital Economy - WPDGP*)[6].

Em termos de participação brasileira nessas atividades de segurança digital, o Brasil participou como membro observador *ad hoc* de reuniões do WPISP, ocorridas em 2009 e 2010, apresentando em 2010 estudo comparativo sobre estratégias nacionais de segurança cibernética, o que motivou a criação de um grupo de trabalho com a presença de países voluntários, incluindo o Brasil, cuja presidência foi de Portugal (BRASIL, 2010, p. 21). Além disso, o país é participante do CDEP e do WPSDE (OCDE, 2022, p. 71).

A Recomendação de 2015 da OCDE sobre Gerenciamento de Riscos de Segurança Digital para Prosperidade Econômica e Social é dividida em duas partes, sendo que a primeira abarca os princípios que denotam o pioneirismo da OCDE no assunto e, a segunda, destinada a tratar das Estratégias Nacionais. Essas devem ser consistentes com os primeiros, criando condições para que todos os atores possam administrar os riscos de segurança digital para atividades econômicas e sociais e promover confiança no ambiente digital (OCDE, 2015, p. 13).

De mais a mais, no próprio preâmbulo da documentação é destacada a importância do ambiente digital para o funcionamento das nossas economias e sociedades (OCDE, 2015, p. 6), afirmação que desde a edição da Recomendação se torna cada mais vez assertiva, com a transformação digital e a busca pela redução da brecha digital com o objetivo de conectar a todos.

---

[6] Mandato do ICPP, CDEP, WPSDE e WPDGP, bem como lista de participantes e da presidência dos trabalhos, pode ser consulta no site da OCDE destinado às suas atividades, disponível em: https://oecdgroups.oecd.org/Bodies/ListByDirectorateView.aspx. Acesso em: 13 ago. 2022.

Outrossim, a Recomendação também ressalta que os benefícios desse ambiente, especialmente da Internet, espalham-se a todos os setores da economia e todos aspectos do progresso social; e que esses benefícios decorrem da natureza global, aberta, interconectada e dinâmica das TICs, especialmente da Internet. Reconhece também que o uso, gestão e desenvolvimento do ambiente digital está sujeito a incertezas que são dinâmicas em sua natureza e que a gestão de riscos de segurança digital é uma abordagem flexível e ágil para endereçar essas incertezas e para permitir o alcance integral dos benefícios econômicos e sociais; promover serviços essenciais e operar infraestruturas críticas; preservar direitos humanos e valores fundamentais; e proteger indivíduos de ameaças de segurança digital (OCDE, 2015, p. 6-7).

O preâmbulo ainda enfatiza que a gestão de riscos de segurança digital confere fundação robusta para a implementação do Princípio de Salvaguardas de Segurança constante das Diretrizes de Privacidade da OCDE. Do mesmo modo, chama à atenção que governos, organizações públicas e privadas, assim como os indivíduos possuem responsabilidade compartilhada, baseada nos seus papéis e no contexto, para gerir os riscos de segurança digital e para proteger o ambiente digital, sendo que a cooperação é essencial em todos os níveis: doméstico, regional e internacional (OCDE, 2015, p. 7).

Na Seção I, a Recomendação traz os Princípios Gerais, os quais formam a fundação sobre a qual o ciclo operacional de gestão de riscos de segurança digital deve ser estabelecido. São eles:

a) conscientização, habilidades e empoderamento, que pregam que todos atores devem entender os riscos de segurança digital e saber como gerenciá-los, o que implica em empoderá-los com a educação e habilidades necessárias;
b) responsabilidade, todos atores devem responsabilizar-se pela gestão do riscos de segurança digital, com base no seu papel e na sua habilidade de agir;
c) direitos humanos e valores fundamentais, que demanda a gestão de riscos de forma transparente e consistente com esses direitos e valores; e
d) cooperação, que deve orientar a conduta de todos atores, inclusive para cooperação transfronteiriça (OCDE, 2015, p. 9-10).

E também apresenta os Princípios Operacionais de gestão de riscos que devem guiar a ação de líderes e tomadores de decisão, os quais devem garantir que:

a) o risco de segurança digital seja tratado com base em processo contínuo de avaliação de risco;

b) medidas de segurança sejam apropriadas e proporcionais aos riscos;

c) a inovação seja considerada; e

d) que um plano de preparação e continuidade seja adotado (OCDE, 2015, p. 10-11).

A Seção II da Recomendação destaca que as Estratégias Nacionais devem ser apoiadas pelo mais alto nível do governo e articular uma abordagem clara e de todo o governo (*whole-of-government*) que seja flexível, tecnologicamente neutra e coerente com outras estratégias que promovam a prosperidade econômica e social. Também devem indicar claramente o objetivo de beneficiar-se do ambiente digital para prosperidade social e econômica com a redução do nível de risco, sem restrição desnecessária do fluxo de tecnologia, dados e comunicações (OCDE, 2015, p. 11-12).

Adicionalmente, devem expressar o objetivo de garantir a provisão de serviços essenciais e operação das IECs; de proteger os indivíduos de ameaças, ao mesmo tempo que considerando a necessidade de salvaguardar a segurança nacional e internacional; e de preservar valores fundamentais e direitos humanos (OCDE, 2015, p. 12).

No tocante à abrangência, as Estratégias devem ser direcionadas a todos os atores e adequadas às pequenas e médias empresas e indivíduos, articulando a responsabilidade de acordo com os seus respectivos papéis, habilidade de agir e contexto em que operam. Já quanto ao processo de elaboração, as Estratégias devem ser resultado de uma abordagem intragovernamental coordenada e de um processo aberto e transparente envolvendo todos os atores, com revisão regular e aprimoramento baseado na experiência e boas práticas, usando, quando disponíveis, métricas internacionalmente comparáveis (OCDE, 2015, p. 12).

A Recomendação ainda detalha medidas que as Estratégias Nacionais devem incluir para fazer com que os governos liderem por exemplo; fortaleçam a cooperação internacional e assistência mútua; engajem-se com outros atores; e criem condições para que todos os atores colaborem com a gestão dos riscos de segurança digital (OCDE, 2015, p. 12-15).

No tocante à liderança pelo exemplo, o documento cita a adoção de arcabouço compreensivo para as atividades do próprio governo; o estabelecimento de mecanismos de coordenação entre todos atores governamentais relevantes; o estabelecimento de equipes de prevenção, tratamento e resposta a incidentes (CIRTs/CSIRTs/CERTs)[7]; a utilização de sua posição no mercado para promover a segurança digital na sociedade e economia através das compras governamentais e recrutamento de profissionais qualificados em gestão de riscos; e o

[7] Embora as siglas CIRT, CSIRT e CERT apontem para diferentes tipos de times de resposta a incidentes, para fins do trabalho utiliza-se a listagem para identificar os centros de resposta a incidentes, independentemente das suas especificidades.

encorajamento da utilização de padrões e boas práticas internacionais, promovendo o seu desenvolvimento (OCDE, 2015, p. 12-13).

A adoção de técnicas de segurança inovadoras para gestão de riscos de segurança digital; a coordenação e promoção de pesquisa e desenvolvimento público sobre gestão de riscos de segurança digital; o apoio ao desenvolvimento de mão de obra qualificada que possa gerenciar os riscos de segurança digital; a adoção de arcabouço jurídico abrangente para combate aos crimes cibernéticos; e a alocação de recursos para a implementação complementam o rol das medidas citadas (OCDE, 2015, p. 12-13).

Com relação ao fortalecimento da cooperação internacional e de assistência mútua, a Recomendação salienta três ações. A primeira refere-se à participação em fóruns relevantes regionais e internacionais; ao estabelecimento de relações bilaterais e multilaterais para troca de experiências e melhores práticas; e à promoção de uma abordagem nacional de gestão de riscos de segurança digital que não eleve o risco para outros países. A segunda refere-se a prover assistência e suporte a outros países, de forma apropriada e voluntária, e estabelecer pontos de contato para endereçar tempestivamente pedidos transfronteiriços relacionados a assuntos de gestão de riscos de segurança. Finalmente a terceira, trata de esforço para aprimorar a resposta a ameaças domésticas e transfronteiriças, incluindo cooperação entre CSIRTs, exercícios coordenados e outras ferramentas de colaboração (OCDE, 2015, p. 13-14).

Quanto ao engajamento com outros atores, as Estratégias devem explorar como os governos e outros atores podem se ajudar mutuamente para melhor gestão dos riscos de segurança digital das suas atividades; identificar e endereçar os potenciais impactos negativos que políticas governamentais podem ter sobre as atividades de outros atores ou sobre a prosperidade social e econômica nacional; estabelecer práticas e processos de gestão de riscos de segurança digital e levar ao conhecimento do público; encorajar a responsável divulgação, reporte e/ou correção de vulnerabilidades por todos os atores; e elevar o nível de conscientização, habilidades e empoderamento em toda a sociedade para a gestão de riscos de segurança digital através de iniciativas tecnologicamente neutras apropriadas às necessidades especiais das diferentes categorias de atores (OCDE, 2015, p. 14).

O último ponto refere-se à criação de condições para que todos os atores colaborem para na gestão de riscos de segurança digital. Para tanto, as Estratégias devem fomentar a participação ativa de atores relevantes em iniciativas e parcerias mutualmente confiáveis (envolvendo diversos atores, abordagens e níveis). Essas ações visam o compartilhamento de conhecimento, habilidades, experiências e práticas de sucesso na gestão de riscos de segurança digital, abarcando os níveis operacionais e de formulação de políticas (OCDE, 2015, p. 14).

Além do mais, as Estratégias também devem promover a troca de informações sobre a gestão de riscos de segurança digital; e planejar e antecipar oportunidade e desafios futuros. Outrossim, a Estratégia deve promover a coordenação entre todos os atores para aprimorar a remediação e identificação de ameaças e vulnerabilidades, assim como a mitigação dos riscos; encorajar todos os atores a trabalhar conjuntamente para ajudar a proteger indivíduos e pequenas e médias empresas, bem como aumentar sua habilidade de fazer a gestão desses riscos para suas atividades; incentivar a gestão de riscos de segurança cibernética e aumentar transparência e eficiência do mercado; encorajar inovação assim como o desenvolvimento de ferramentas para a proteção de indivíduos e de organizações; e encorajar o desenvolvimento de métricas comparáveis internacionalmente. Essas métricas devem traduzir metodologias, padrões e boas práticas de mensuração de riscos e serão utilizadas para aperfeiçoar a efetividade, eficiência e transparência da gestão dos riscos de segurança digital (OCDE, 2015, p. 14-15).

A Recomendação ainda possui um documento complementar que apresenta o contexto, a evolução dos princípios ao longo dos anos, definições, aplicabilidade dos princípios e possíveis áreas de trabalho futuro nessa seara.

É de interesse para o trabalho, pontuar algumas das questões trazidas nesse documento complementar que acompanha a Recomendação. Em primeiro lugar, para entender a abrangência dos princípios e das Estratégias equacionadas na Recomendação, deve-se atentar para o conceito de ator, o qual nos termos da Recomendação é considerado como governo, organizações públicas e privadas e indivíduos que dependem do ambiente digital para toda ou parte das suas atividades sociais e econômicas, podendo inclusive acumular diferente papéis (OCDE, 2015, p. 8). Aqui a terminologia governo engloba todos os seus órgãos e em todos os níveis (por exemplo: central, federal, internacional, regional, nacional, provincial, local, etc), em um claro intuito de abranger todos os órgãos de governo nas diferentes formas que um Estado pode se organizar (OCDE, 2019a, p. 29).

A acumulação de papéis para os governos, pode ser denotada como responsável pela adoção das políticas públicas necessárias relacionadas ao ambiente digital, assim como um usuário do ambiente digital, o qual depende fortemente dele para a prestação de serviços públicos, assim como para outras funções governamentais (OCDE, 2019a, p. 29).

Ao tratar do Princípio da Responsabilidade, o documento destaca que o princípio não contempla a responsabilidade civil ou penal, ou seja, não está relacionado às consequências jurídicas. Relaciona-se à noção fundamental de que todos os atores compartilham, em diferentes níveis ou degraus, a responsabilidade pela gestão dos riscos de segurança. Além do mais, não

é viável depender de outro ator para todos os aspectos da gestão desses riscos, também alertado que o ambiente digital não difere de outros ambientes e que algum risco deve ser aceitável para o alcance de objetivos sociais e econômicos (OCDE, 2015, p. 44).

Dessa forma, todos atores precisam fazer a gestão dos riscos para reduzi-los a níveis aceitáveis, fazendo uso dos princípios operacionais citados na Recomendação. No entanto, o documento complementar reforça que os atores não são iguais em termos de responsabilidade, sendo que a suas habilidades de identificar, avaliar e gerenciar esses riscos variam substantivamente. Nesse sentido, não se pode esperar que alguns atores, como indivíduos e pequenas empresas, por exemplo, possam identificar, avaliar e gerenciar os riscos da mesma forma que atores que possuem recursos significativos, cabendo aos atores que desenvolvem, operam e gerenciam componentes do ambiente digital criar as condições para que seus consumidores possam tomar decisões responsáveis de gestão de risco (OCDE, 2015, p. 45).

Especificamente quanto aos governos, o documento aponta que devem desenvolver estratégias nacionais e adotar medidas e iniciativas de políticas públicas para fomentar a gestão de riscos por todos os atores. Adicionalmente, o documento aponta a realidade dos países da OCDE, cuja maioria já teria adotado as fundações. Essas são materializadas na legislação relativa à persecução penal dos crimes cibernéticos e à proteção da privacidade; na capacidade de resposta; nas iniciativas educacionais; nas parcerias público-privadas, etc. Ademais, já destacava em 2015 o movimento de alguns países de formulação de suas políticas em termos mais estratégicos e aumento da consistências das suas abordagens, com novos ou melhorados mecanismos de cooperação, como agências dedicadas (OCDE, 2015, p. 46).

Para finalizar esse ponto, o documento ressalva que as políticas públicas para a gestão de riscos de segurança digital são inerentemente horizontais e exigem cooperação não só dentro do governo, mas também de todos atores dos níveis domésticos, regionais e internacionais, conforme refletido na Seção II da Recomendação que endereça as Estratégias Nacionais, sendo um esforço estratégico de políticas públicas de longo prazo (OCDE, 2015, p. 48).

Cabe ressaltar que o Brasil aderiu à Recomendação de 2015 em 2018[8] (OCDE, 2020b, p. 63) e participou do processo de revisão da Recomendação iniciado em 2020 no âmbito do WPSDE. Esse processo gerou um Arcabouço de Política de Segurança Digital, o qual compreende todas as recomendações na temática da OCDE e confere uma narrativa comum aos instrumentos legais (OCDE, 2022e).

[8] Lista de adesões com as suas respectivas datas pode ser consultada em: https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0415#adherents. Acesso em: 24 dez. 2022.

O processo de revisão da Recomendação de 2015 gerou o desmembramento das partes que tratam dos princípios que abordam o gerenciamento de riscos das orientações destinadas às estratégias nacionais, as quais passam a constituir recomendações em apartado. Dessa forma, foram aprovadas em 2022 a Recomendação do Conselho sobre Gerenciamento dos Riscos de Segurança Digital (OCDE, 2022a) e a Recomendação do Conselho sobre Estratégias Nacionais de Segurança Digital (OCDE, 2022b).

Importa esclarecer que os instrumentos não sofreram alterações de monta, permanecendo os princípios e as premissas contidas na Recomendação de 2015 e detalhadas anteriormente. Outrossim, deve-se atentar para a inclusão do Princípio Operacional de Estratégia e Governança na Recomendação do Conselho sobre Gerenciamento dos Riscos de Segurança Digital de 2022. Esse princípio defende que os líderes e tomadores de decisão precisam garantir que o risco de segurança digital está integrado na estratégia mais abrangente de gestão de riscos e administrado como risco estratégico, o qual demanda implementação operacional (OCDE, 2022a).

Um outro elemento interessante acrescido foi a expressa menção da resiliência no princípio operacional de preparação e continuidade. No restante, as alterações foram meros ajustes redacionais, mantendo-se o conteúdo da Recomendação de 2015.

Já a Recomendação sobre Estratégias Nacionais de Segurança Digital manteve todas as premissas endereçadas na Recomendação de 2015, salvo a previsão sobre adoção e implementação de um arcabouço compreensivo para auxiliar a mitigação dos crimes cibernéticos. A temática dos crimes cibernéticos aparece expressamente no texto da Recomendação de 2022 no sentido de justificar que as estratégias nacionais precisam contemplar outros temas que estão fora do escopo da Recomendação, pois não endereçam aspectos sociais e econômicos de segurança digital (OCDE, 2022b).

Cabe trazer à baila que as premissas da Recomendação de 2015 foram reorganizadas na nova recomendação, a qual se estrutura no arcabouço institucional; conteúdo da estratégia; e implementação da estratégia. No entanto, a nova recomendação, diferentemente da Recomendação do Conselho sobre Gerenciamento dos Risco de Segurança Digital, carrega inovações que refletem o lapso temporal entre as versões de 2015 e 2022, ao enfrentar algumas questões como: resposta responsável do setor privado (*hack back*); fomento à indústria de segurança cibernética; antecipação dos desafios relacionados à transformação digital

disruptiva[9]; e encorajamento aos órgãos mais vulneráveis do setor público a fortalecer sua gestão de riscos de segurança digital (OCDE, 2022b).

Não menos relevante é a previsão assertiva no âmbito da Recomendação no arcabouço institucional, no sentido de que deve haver clara atribuição de responsabilidade a um ou mais, novo(s) ou já existente(s), órgão(s) do governo para o desenvolvimento das políticas públicas e para a sua implementação. Ao mesmo tempo, é necessário assegurar a coordenação desse(s) órgão(s) com outras agências e ministérios relevantes em diversas áreas, como persecução penal; regulação setorial; privacidade e proteção de dados; proteção dos consumidores; inovação; educação; governo digital; e relações exteriores (OCDE, 2022b).

Juntamente com essas recomendações aprovadas em apartado, foram aprovadas em 2022 outras duas recomendações na matéria: Recomendação do Conselho sobre Segurança Digital de Produtos e Serviços (OCDE, 2022c) e Recomendação do Conselho sobre o Tratamento de Vulnerabilidades de Segurança Digital (OCDE, 2022d).

Dessa forma, o Arcabouço de Segurança Digital, lançado na Reunião Ministerial do Comitê de Política da Economia Digital da OCDE, realizada em dezembro de 2022, abarca as quatro novas recomendações, além da Recomendação sobre Segurança Digital das Atividades Críticas (OCDE, 2019b) e Diretrizes sobre Política de Criptografia (OCDE, 1997). Com exceção das últimas diretrizes, o Brasil já aderiu a todas as outras recomendações, inclusive as recentemente lançadas em dezembro de 2022[10].

Após a breve explanação sobre a entidade, histórico no desenvolvimento das recomendações relacionadas à segurança digital, participação do Brasil nesses trabalhos e conteúdo da recomendação de 2015 e recomendações de 2022, passa-se a conhecer os trabalhos da União Internacional de Telecomunicações (UIT) nessa questão.

---

[9] Como tecnologia disruptiva, adotam-se as ideias do trabalho precursor de BOWER e CHRISTENSEN que sustentam que essas tecnologias introduzem um pacote de atributos muito diferentes em relação aos que os consumidores já estavam acostumados. Essas tecnologias tendem a ser utilizadas e valorizadas em novas aplicações e possibilitam o surgimento de novos mercados. Diferem das outras tecnologias, visto que nestas, as inovações caminham para fornecer algo mais ou melhor aos consumidores, mantendo a taxa de aprimoramento (BOWER; CHRISTENSEN, 1995, p. 45). Dessa forma, quando se utiliza tecnologias disruptivas no presente trabalho, fala-se de tecnologias como 5G, Computação Quântica, Internet das Coisas, Inteligência Artificial, *Big Data*, etc).

[10] A consulta dos países aderentes e das datas de adesão a cada uma das recomendações pode ser realizada nas respectivas páginas dos instrumentos legais. A página de consulta aos instrumentos legais da OCDE pode ser acessada em: https://legalinstruments.oecd.org/en/. Acesso em: 27 dez. 2022.

2.2 UNIÃO INTERNACIONAL DE TELECOMUNICAÇÕES

Outra organização internacional que se destaca nos esforços relacionados à resposta institucional e organizacional dos países para promover segurança cibernética é a UIT, a agência especializada das Nações Unidas para assuntos ligados às TICs, que foi fundada em 1865, à época, União Internacional do Telégrafo[11].

Antes de adentrar no mandato e nas ações da entidade em segurança cibernética, especialmente na assistência aos países na elaboração de ENSCs, cabe apresentar brevemente a organização. Trata-se de organização intergovernamental, atualmente integrada por 193 Estados-membros (países) e mais de 900 Membros de Setores e Associados, abarcando assim setor privado, academia, entidades regionais e internacionais, dentre outros[12].

O Brasil é País-membro da UIT e é possível rastrear a aprovação de diversos Atos Finais de Conferências dos Plenipotenciários pelo Congresso Nacional e a sua respectiva promulgação pelo Presidente da República. Nesse sentido, os Atos Finais da Conferência Adicional dos Plenipotenciários de 1992 (Genebra) e da Conferência de Plenipotenciários de 1994 (Quioto) foram aprovados pelo Decreto Legislativo n.° 67, de 1998, sendo a Constituição e a Convenção da UIT promulgadas pelo Decreto n.° 2.962, de 23 de fevereiro de 1999. Já os Atos Finais das Conferências de 1998 (Minneapolis) e 2002 (Marraqueche) foram aprovados pelos Decretos Legislativos n.° 34, de 2002, e nº 987, de 2009 (CRAVO, 2011, p. 75), respectivamente, e os referentes às Conferências de 2006 (Antalya) e 2010 (Guadalajara) foram promulgados pelo Decreto nº 10.227, de 5 de fevereiro de 2020 (BRASIL, 2020b). Não houve modificações à Constituição e à Convenção nas Conferências de Plenipotenciários posteriores: 2014 em Busan, 2018 em Dubai (ITU, 2019b); e 2022 em Bucareste (ITU, 2022b).

Os instrumentos básicos da organização são a sua Constituição e Convenção, os quais definem seu mandato, objetivo, estrutura e funcionamento, dentre outras normas. Seu preâmbulo destaca o papel das telecomunicações para o desenvolvimento social e econômico dos países e para a preservação da paz (ITU, 2019b).

Frisa-se das suas finalidades, a manutenção e ampliação da cooperação internacional; a promoção, oferta de assistência técnica e mobilização de recursos no campo das telecomunicações aos países em desenvolvimento; o fomento do desenvolvimento de meios técnicos buscando melhorar a eficiência e universalização dos serviços; a extensão dos

[11] O nome atual foi adotado em 1934 e a UIT tornou-se agência do Sistema nas Nações Unidas em 1947. Nesse ponto ver CRAVO, 2011, p. 74.

[12] Informações sobre países-membros e demais membros e associados podem ser consultadas em: https://www.itu.int/en/about/Pages/default.aspx.

benefícios das novas tecnologias a todos indivíduos; o impulsionamento da utilização de serviços de telecomunicações com o objetivo de facilitar relações pacíficas; a harmonização das ações dos Estados-membros e estímulo à cooperação frutífera e construtiva e parceria entre os Estados-membros e Membros do Setor na realização desses fins; e o impulsionamento, no âmbito internacional, da adoção de uma abordagem mais ampla para as questões das telecomunicações na economia e na sociedade global da informação, em cooperação com outras organizações intergovernamentais internacionais e regionais, bem como com organizações não governamentais relacionadas às telecomunicações (ITU, 2019b).

Para tanto, suas atribuições abrangem: alocação de bandas de espectro de radiofrequências, atribuição de frequências e registro de posição orbitral de satélites geoestacionários; coordenação de esforços para eliminação de interferência prejudicial e para melhoria da utilização do espectro de radiofrequências; facilitação da padronização mundial das telecomunicações; promoção da cooperação e solidariedade internacional na assistência técnica aos países em desenvolvimento; coordenação de esforços para harmonização de instalações de telecomunicações; e fomento à colaboração entre Estados-membros e Membros do Setor, buscando preços acessíveis (ITU, 2019b).

Ainda, o mandato inclui: promoção de medidas de preservação da vida pela cooperação dos serviços de telecomunicações; realização de estudos, elaboração de regulamentações, adoção de resoluções, formulação de recomendações e opiniões, e coleta e publicação de informações relacionadas às telecomunicações; promoção de linhas preferencias de crédito para desenvolvimento de projetos de expansão dos serviços para áreas desassistidas, em cooperação com organismos de financiamento internacionais e de desenvolvimento; e incentivo à participação das entidades interessadas nas atividades da União e cooperação com outras organizações para o alcance dos objetivos da organização (ITU, 2019b).

Em termos de estrutura organizacional, prevista no artigo 7º da Constituição, a UIT é composta pela Conferência de Plenipotenciários, órgão máximo da União; o Conselho, que age em nome da Conferência entre os interstícios; Conferências Mundiais das Telecomunicações Internacionais; o Setor de Radiocomunicação (UIT-R), incluindo as suas Conferências de Radiocomunicação, Assembleias de Radiocomunicação e Conselho de Regulamento de Rádio; o Setor de Normalização das Telecomunicações (UIT-T), incluindo as Assembleias Mundiais de Normalização de Telecomunicação; o Setor de Desenvolvimento das Telecomunicações (UIT-D), incluindo as Conferências Mundiais de Desenvolvimento das Telecomunicações; e a Secretaria-Geral (ITU, 2019b).

De forma muito breve[13], pode-se dizer que a UIT-R foca em radiocomunicações; a ITU-T, em normalização, ou seja o estabelecimento de padrões; e a UIT-D concentra-se em questões relacionadas ao desenvolvimento, inclusive como agência de execução de projetos no âmbito do Sistema de Desenvolvimento das Nações Unidas ou outros fundos, nos termos dos artigos 12, 17 e 21 da Constituição (ITU, 2019b).

Para fins de compreensão do mandato da organização nos temas de segurança cibernética, ainda se faz necessário citar a CMSI. Nesse ponto, a primeira ênfase se refere ao fato de que a realização da Cúpula foi gestada na UIT. Foi a Conferência de Plenipotenciários da UIT de 1998, realizada em Mineápolis, nos Estados Unidos, que aprovou a Resolução nº 73, a qual instruiu o Secretário-Geral da União a incluir a questão da realização dessa Cúpula na pauta da Agenda do Comitê Administrativo de Coordenação das Nações Unidas. No preâmbulo da Resolução fora apontado que a globalização das telecomunicações precisaria considerar a evolução harmoniosa de políticas, regulamentação, redes e serviços em todos os Estados-membros; e destacado o surgimento do conceito de Sociedade da Informação, no qual as telecomunicações desempenham um papel-chave (ITU, 1999).

Após a atividade de preparação da UIT para a Cúpula, a AGNU, na sua Resolução nº 183 aprovada na 56º Sessão, em 21 de dezembro de 2001, chancelou a proposta da UIT, de organização da Cúpula em duas fases, na Suíça e na Tunísia, nos anos de 2003 e 2005, respectivamente, convidando a Agência a liderar a Secretaria da Cúpula e o seu processo de preparação (UNGA, 2002).

Seguindo essas decisões, a primeira fase da CMSI ocorreu em Genebra, no final de 2003, e a segunda, em Túnis, em 2005. A primeira fase contou com a participação de mais de onze mil delegados e quase cinquenta representantes de mais alto nível — Chefes de Estado ou de Governo e Vice-Presidentes (ITU, 2007, p. 9), demostrando a enorme relevância das discussões ali já travadas em 2003.

Já a segunda fase da CMSI contou com a presença de quarenta e cinco representantes de mais alto nível e mais de dezenove mil delegados. Esse último número pode ser decomposto em cinco mil e oitocentos delegados representando mais de cento e setenta e quatro Estados-membros; mil e quinhentos representantes de noventa e duas organizações internacionais; seis mil e duzentos delegados de organizações não governamentais e da sociedade civil; e quatro mil oitocentos e dezesseis do setor privado, além de mais de mil e duzentos jornalistas credenciados, comprovando a mobilização multissetorial (ITU, 2007, p. 9, 12).

[13] Para detalhamento sobre o organismo, sugere-se a consulta de CRAVO, *op. Cit*., p. 72-91.

Como resultados desse processo, têm-se a Declaração de Princípios de Genebra e o Plano de Ação de Genebra, na primeira fase, e o Compromisso de Túnis e a Agenda de Túnis para a Sociedade da Informação, na segunda (CGI.br, 2014). A Declaração inicia com a descrição da visão comum sobre a Sociedade da Informação (SI), cuja construção é apontada como um desafio global para o novo milênio, aproveitando-se aqui para destacar o seu preâmbulo:

> Nós, os representantes dos povos do mundo, reunidos em Genebra de 10 a 12 de dezembro de 2003, para a primeira fase da Cúpula Mundial sobre a Sociedade da Informação, declaramos nosso desejo e compromisso comuns de construir uma Sociedade da Informação voltada para as pessoas, inclusiva e orientada para o desenvolvimento, em que todos possam criar, acessar, utilizar e compartilhar informação e conhecimento, permitindo indivíduos, comunidades e povos empregar todo o seu potencial na promoção do desenvolvimento sustentável e da melhor qualidade de vida, com base nos propósitos e princípios da Carta das Nações Unidas, respeitando plenamente e defendendo a Declaração Universal dos Direitos Humanos (CGI.br, 2014, p. 16).

Para instrumentalizar a visão de SI estabelecida, a Declaração elenca um conjunto de princípios fundamentais para construir uma SI inclusiva: papel dos governos e de todos os interessados na promoção das TICs para o desenvolvimento; infraestrutura da informação e comunicação como fundamento básico da SI; acesso à informação e ao conhecimento; capacitação; construção de confiança e segurança na utilização das TICs; ambiente propício; aplicações de TIC beneficiando todos os aspectos da vida cotidiana; diversidade cultural e identidade, bem com diversidade linguística e conteúdo local; mídia; dimensões éticas da SI; e cooperação internacional e regional (CGI.br, 2014, p. 23-35). Esses princípios foram desdobrados no Plano de Ação de Genebra, que traduziu a visão de SI e os seus princípios em respectivas linhas de ação concreta (C1 a C11), prevendo objetivos e metas (CGI.br, 2014, p. 29-60).

Especificamente com relação à segurança cibernética, a Declaração aponta que o fortalecimento da estrutura de confiança é um pré-requisito para o desenvolvimento da SI, devendo ser promovida, desenvolvida e implementada uma cultura de segurança cibernética em cooperação com todos atores e apoiada em maior cooperação internacional. Ademais, essa cultura deve aprimorar aspectos de segurança e garantir a proteção de dados pessoais e da privacidade, simultaneamente ao trabalho de ampliação do acesso e comércio digital, também apoiando os esforços das Nações Unidas para evitar o potencial uso das TICs para fins não pacíficos, criminosos e terroristas, com respeito aos direitos humanos. Por fim, salienta o problema do *spam* e a necessidade de adequado tratamento nacional e internacional, assim como segurança cibernética (GCI.br, 2014, p. 27).

Já o Plano de Ação de Genebra, ao tratar da Linha de Ação C5 – Construção de Confiança e Segurança no Uso das TICs, acordou o que segue:

> a) Promover a cooperação entre os governos nas Nações Unidas, e de todos os setores e partes interessadas nos demais fóruns apropriados, para aprimorar a confiança do usuário e proteger os dados e a integridade da rede; considerar as ameaças existentes e potenciais às TIC; e tratar de outras questões de segurança da informação e de segurança na rede.
> b) Os governos, em cooperação com o setor privado, devem prevenir, detectar e responder a crimes cibernéticos e ao uso indevido das TIC: desenvolvendo diretrizes que levem em conta os esforços existentes nessas áreas; considerando a legislação que permite a investigação e a repressão eficaz do uso indevido; promovendo esforços efetivos de assistência mútua; reforçando o apoio institucional no nível internacional para a prevenção, detecção e recuperação de tais incidentes; e encorajando a educação e a conscientização.
> c) Os governos e outras partes interessadas devem promover ativamente a educação do usuário e a conscientização sobre privacidade on-line e os meios de proteção da privacidade.
> d) Tomar as medidas adequadas contra o spam nos âmbitos nacional e internacional.
> e) Incentivar a avaliação interna da legislação nacional, com vista à superação de quaisquer obstáculos à utilização eficaz de documentos e transações eletrônicas incluindo meios eletrônicos de autenticação.
> f) Reforçar a estrutura de confiança e segurança com iniciativas complementares e de apoio mútuo nos campos da segurança nos usos das TIC, com iniciativas e diretrizes no que diz respeito ao direito à privacidade, à proteção de dados e dos consumidores.
> g) Compartilhar boas práticas no campo de segurança da informação e de segurança de redes e incentivar a sua utilização por todas as partes interessadas.
> h) Convidar os países interessados a criar pontos focais de tratamento e resposta a incidentes em tempo real, e desenvolver uma rede de cooperação entre esses pontos focais para compartilhar informações e tecnologias de resposta a incidentes.
> i) Incentivar o desenvolvimento de aplicações seguras e confiáveis para facilitar transações on-line.
> j) Incentivar os países interessados a contribuir ativamente com as atividades em andamento nas Nações Unidas para a construção de confiança e segurança na utilização das TIC. (CGI.br, 2014, p. 48-49).

Em relação aos resultados da segunda fase, o Compromisso de Túnis reitera os corolários da primeira fase e a Agenda de Túnis para a Sociedade da Informação aborda os mecanismos de financiamento; a Governança da Internet com a criação de um fórum multissetorial de diálogo sobre políticas, o Fórum de Governança da Internet (IGF); e implementação e acompanhamento dos resultados e compromissos do processo da CMSI (CGI.br, 2014, p. 68-115).

Ao tratar da implementação, a Agenda de Túnis realça a necessidade de um esforço contínuo de todos os atores e reitera o papel de liderança da UIT, da Organização das Nações Unidas para a Educação, a Ciência e a Cultura (UNESCO) e do Programa das Nações Unidas para o Desenvolvimento (PNUD) na facilitação da implementação do Plano de Ação de Genebra e na organização de reuniões como moderadores/facilitadores indicados (não exaustivos) para cada uma das Linhas de Ação, constantes do Anexo à Agenda. A UIT é

identificada como possível moderadora/facilitadora de várias das Linhas de Ação, sendo a única apontada para a Linha de Ação C5, que conforme exposto anteriormente, trata da construção de confiança e segurança no uso das TICs (CGI.br, 2014, p. 103, 112, 113, 116).

Dessa forma, o mandato da UIT em segurança cibernética é conformado não apenas pelos seus instrumentos básicos, mas também pela Linha de Ação C5 do Plano de Ação de Genebra, a qual foi atribuída à UIT para facilitação/moderação.

Em resposta ao seu mandato e à crescente preocupação com o tema na agenda internacional[14], em 2007 a UIT lançou a Agenda Global de Segurança Cibernética (GCA). A GCA coloca-se como um arcabouço dentro do qual a resposta internacional para os crescentes desafios de segurança cibernética pode ser coordenada e endereçada, baseando-se na cooperação internacional e no esforço de engajamento dos atores relevantes na busca da construção de confiança e segurança na SI (ITU, 2009b, p. 12). Ressalva-se que não se constitui como um instrumento vinculante (KUERBIS e BADIEI, 2017, p. 17).

Para tanto, o arcabouço estrutura-se em cinco pilares: medidas legais (arcabouço jurídico adequado e harmonizado para viabilizar a persecução penal dos crimes cibernéticos e outras medidas legais relacionadas); medidas técnicas e procedimentais (medidas-chave para endereçar vulnerabilidades, incluindo padrões, protocolos e esquema de acreditação, bem como capacidade de resposta a incidentes); estruturas organizacionais (arcabouço e estratégias para a prevenção, resposta e gerenciamento de crise de ataques cibernéticos, incluindo a proteção de infraestrutura crítica de informação); capacitação (estratégias para mecanismos de capacitação e conscientização); e cooperação internacional (ITU, 2009b, p. 3).

É interessante notar que é justamente a GCA que fornece os fundamentos gerais e arcabouço abrangente para o Índice Global de Segurança Cibernética (GCI), que é uma das atividades mais notórias da UIT em segurança cibernética. O seu objetivo é mensurar o nível de comprometimento dos países à GCA, usando a estrutura básica da Agenda, ou seja, o desenvolvimento de capacidades nos cinco pilares supracitados (ITU, 2021b). Dessa forma, o questionário coleta as informações dos Estados-membros no tocante às suas ações e iniciativas em medidas legais; medidas técnicas; medidas organizacionais; desenvolvimento de capacidades; e medidas de cooperação.

[14] Relembra-se que o final de abril de 2007 foi marcado pelo início de grave ataque cibernético à Estônia, que através de um ataque distribuído de negação de serviço, causou a interrupção de vários serviços de IECs do país de vários setores (governo, setor financeiro, telecomunicações, etc). Para maiores informações sobre o ataque, ver: Ottis (2008). Veja-se que os reflexos dos ataques à Estônia expandem-se pelos organismos internacionais, fazendo, por exemplo, com que a OTAN repensasse sua política de defesa cibernética (NATASIU, 2016, p. 619).

Metodologicamente, o processo do questionário consiste na indicação pelos Estados-membros da UIT, e Estado da Palestina, de ponto focal, o qual será responsável por receber o questionário; coletar as informações domésticas; repassar os dados à UIT; e validar a avaliação realizada pela UIT, bem como prover subsídios adicionais para comprovar a resposta às questões. O processo do GCI foi iniciado em 2013, e a coleta de dados da primeira iteração do Índice Global de Segurança Cibernética (GCIv1) foi realizada em 2013 e 2014, com a publicação dos resultados em 2015.

No GCIv1, cento e cinco países indicaram um ponto focal e noventa e nove países submeteram as informações. A segunda iteração do Índice Global de Segurança Cibernética GCIv2 coletou as informações em 2016 e, no ano seguinte, 2017, publicou os resultados, contando com centro e trinta e seis nominações e repostas (ITU, 2021a, p. 4). Na sequência, a terceira iteração do Índice Global de Segurança Cibernética (GCIv3) coletou os dados em 2018, publicando os resultados em 2019, e obteve resposta de cento e vinte países, após a nominação de cento e cinquenta e cinco pontos focais. Finalmente, a quarta edição[15] do GCI (GCIe4) envolveu a indicação de cento e sessenta e nove pontos focais e resposta de cento e cinquenta países, com a coleta das informações em 2020 e divulgação dos resultados em junho de 2021 (ITU, 2021a, p. 4).

O índice não reflete o nível de segurança cibernética de um país, nem a efetividade das medidas por ele adotadas, espelhando tão somente o desenvolvimento de capacidades do arcabouço da GCA, ou seja, capacidades relacionadas às medidas legais; medidas técnicas; medidas organizacionais; medidas associadas à capacitação e à conscientização; e medidas de cooperação (ITU, 2021a, p. 5, 9).

Pesquisa documental foi conduzida pela UIT para os países que não responderam ao questionário e submetida aos respectivos países para avaliação e contribuição, caso fosse de interesse. Em caso de ausência de manifestação, os resultados da pesquisa foram considerados para fins de cálculo da pontuação dos países. O GCI é um índice composto baseado na pontuação atribuída para cada uma das questões que integram o questionário, o qual foi sendo aprimorado aos longos das suas edições. Para cada questão é atribuída a pontuação integral, parcial (metade) ou 0 (zero), conforme evidência submetida para cada uma das questões (ao menos um documento de comprovação é necessário para obtenção da pontuação total e

[15] O documento de perguntas frequentes do GCIe4 esclarece que a partir dessa rodada, cada processo será denominado de edição ao invés de iteração. Nesse sentido, ver: ITU (2021a.).

documentos adicionais não alteram a pontuação), que são combinadas em uma média ponderada (ITU, 2021a, p. 5 e 8-9).

As definições das pontuações para cada questão são baseadas nas médias das recomendações de um grupo de experts (*Weightage Experts Group*), os quais representam diversos setores e regiões e foram indicados pelos Estados-membros, além do convite aos experts da edição anterior, totalizando oitenta e oito indivíduos no GCIe4 (ITU, 2021a, p. 5-6). Em termos de apresentação dos resultados, países com a mesma pontuação receberam a mesma posição no índice, sendo mostrados em ordem alfabética. (ITU, 2021a, p. 6).

As mudanças de posições no índice são influenciadas pelas alterações no questionário; modificações na atribuição de pontuação para cada uma das questões do questionário (relembrando-se que o questionário e pontuação não permaneceram imutáveis desde a primeira edição); participação dos países no processo de resposta e validação (com aumento progressivo de países); e, finalmente, o desenvolvimento de capacidades nas cinco áreas que representam os pilares da GCA, sempre com a ressalva de que o índice não mensura implementação, nem a efetividade das medidas (ITU, 2021a, p. 7, 9).

Após essa breve explanação sobre o GCI, passa-se à apresentação dos resultados brasileiros no índice. No GCIv1 o Brasil figurou na quinta (5º) posição no índice, ao lado de outros seis países, com pontuação de 0.706 (ITU, 2015, p. 1), cabendo o destaque que quase metade dos resultados individuais não foram coletados e submetidos pelos próprios países, mas resultado de pesquisa documental da Consultoria *ABI Research*. Dentre os países que não submeteram os dados no GCIv1, notabiliza-se países com notórias capacidades em segurança cibernética, como EUA, China, Rússia, Canadá, Austrália, Japão, Israel e diversos países europeus (ITU, 2015, p. 1-6).

O GCIv2 sofreu atualizações metodológicas importantes, impedindo a sua comparação direta com os resultados do GCIv1 (ITU, 2017, p. 9). Na segunda edição, o Brasil foi classificação na trigésima oitava (38º) posição, com pontuação de 0.593 (ITU, 2017, p. 60), sendo categorizado no grupo de países em amadurecimento (ITU, 2017, p. 15). Ademais, o GCIv2 foi caracterizado pelo forte aumento na resposta ao questionário pelos países, totalizando 136 respostas (ITU, 2021a, p. 4). Para ilustrar as alterações ao longo do processo, o GCIv2 passou-se a utilizar conceito binário para validação das respostas, abandonando o sistema de três níveis utilizados no GCIv1 e contar com vinte e cinco indicadores desdobrados em cento e cinquenta e sete questões (ITU, 2017, p. 5, 9).

Já a terceira edição, GCIv3, novamente traz mudanças metodológicas relevantes, como, por exemplo: redução substantiva no número de questões (passou de cento e cinquenta e sete

para cinquenta questões, mantendo os vinte e cinco indicadores); reavaliação da pontuação atribuída para questões em atendimento às recomendações do *Weightage Experts Group* (ITU, 2019a, *v*); estrutura de resposta predefinidas, incluindo campos de texto livre e perguntas abertas em cada seção do questionário; inclusão de questões de múltipla escolha; e respostas parciais para conferir pontuação adequada a processos em andamento (ITU, 2019a, p. 10-11).

O GCIv3 foi respondido por cento e vinte países (ITU, 2021a, p. 4). Nesse, o Brasil foi classificado na septuagésima (70º) posição no índice global e sexta (6º) na Região das Américas, com pontuação de 0.577 (ITU, 2019a, p. 57), enquadrando-se no grupo médio de nível de cometimento. Esse conjunto refletia os países que estavam desenvolvendo esforços complexos e engajavam-se em programas e iniciativas de segurança cibernéticas (ITU, 2019a, p. 13-14).

Chegando ao GCIe4, última rodada do índice disponível até a presente data, o questionário contemplou oitenta e duas questões agrupadas em vinte indicadores refletindo os cinco pilares da GCA, com resposta submetida por cento e cinquenta países (ITU, 2021b, *vi*). Nesta edição, o Brasil classificou-se na décima oitava (18º) posição no ranking global e terceira (3º) na Região das Américas, totalizando 96,6 pontos (ITU, 2021b, p. 25, 28). Não houve apresentação dos resultados em grupos como ocorreu nas duas edições anteriores (GCIv2 e GCIv3).

Nota-se que nas Américas, a posição brasileira sucede aos Estados Unidos e ao Canadá, os quais sequer submeteram resposta ao questionário, ou seja, a sua pontuação é baseada em pesquisa documental realizada pela UIT embora verificada pelo país e/ou sem oposição à participação no índice (ITU, 2021b, p. *viii*, 25, 27).

Na mesma esteira das edições anteriores, não se pode afirmar que o índice se encontra estável, em termos estruturais e metodológicos, constando-se uma forte reorganização de indicadores, agora contando no GCIe4 com vinte e com novo aumento do número de questões, que passaram de cinquenta para oitenta e duas. Ademais, também houve modificação nas pontuações atribuídas, seguindo contribuições do *Weightage Experts Group* e mudança na escala de pontos, que passou de zero a um, para zero a cem, com vinte pontos para cada pilar (ITU, 2021b, p. 136).

Dessa maneira, o próprio relatório de resultados alerta que a interpretação precisa ser ponderada com cuidado, aliada ao fato de que muitos países, especialmente os com maior performance no índice, estão cada vez mais próximos em termos de pontuação final. Também não se olvida que o crescente engajamento de países no processo possivelmente provoque alterações no índice que sejam positivas à sua classificação (ITU, 2021b, *viii*), fatos que trazem

a necessidade de se ter clareza sobre qual o objetivo do instrumento, o que ele expressa e qual a utilidade para o país.

Nesse sentindo, reitera-se que o índice mensura o nível de desenvolvimento de capacidade de segurança cibernética de um país em cinco áreas, as quais correspondem aos pilares de um arcabouço criado pela UIT em atendimento ao seu mandato, especialmente a Linha de Ação C5 do Plano de Ação de Genebra da CMSI. Esse arcabouço, o qual não endereça questões de defesa e segurança nacional e internacional, é a GCA e foi estruturado em cinco pilares que refletem cinco dimensões de atuação de qualquer país para adequado enfrentamento desse enorme e crescente desafio. É uma abordagem bastante simples e flexível que permite que até mesmos os países menos desenvolvidos consigam compreendê-la e aproveitá-la com o objetivo de desenvolvimento de capacidades.

Os resultados do GCI não indicam a efetividade das capacidades desenvolvidas, nem a sua implementação, apontando tão somente a presença dessa capacidade, a partir de metodologia binária e exigindo apenas uma comprovação para fins de pontuação, sem pontuação adicional para casos com mais de uma evidência. Exemplo: pontuação para um país que realize *n* ações de capacitação será a mesma pontuação de um país que realize uma ação apenas, visto que, conforme relatado, a pontuação será conferida com a comprovação de apenas uma atividade, sem pontuação adicional para demais comprovações.

Com essas ressalvas, também se deve considerar a valia do índice. A UTI é a agência líder na produção de indicadores das TICs e a existência de um índice específico de segurança cibernética gera sensibilização sobre o tema na comunidade doméstica e internacional, permitindo monitorar o desenvolvimentos de capacidades, bem como as lacunas identificadas, a fim de informar ações e iniciativas a serem adotadas pelos próprios países, bem como pelas organizações internacionais com mandatos relacionados.

Domesticamente, os países participantes reportaram a utilização do GCI para a facilitação das discussões através de fóruns formalmente estabelecidos que permitem autoavaliação e maior coordenação; coleta de percepções gerais sobre as iniciativas e recursos nacionais usados para gerir a segurança cibernética em nível nacional; comparação face a boas práticas, parceiros e vizinhos; e conscientização dos atores sobre a coordenação das necessidades domesticamente (ITU, 2021b, *vi*).

Veja-se que com base no questionário, é possível mapear as capacidades nacionais agrupadas nos indicadores sob o guarda-chuva dos pilares, um esforço que exige a coordenação nacional para resposta em face das diferentes entidades e órgãos envolvidos, bem como diferentes atores de diferentes setores. Com base nesse mapeamento, é possível identificar as

lacunas, ou seja, áreas em que é necessário desenvolver capacidades, sempre com a ressalva de que qualquer capacidade não deve ser desenvolvida para fins de pontuação no GCI, ou outro índice qualquer, mas pela razão de ser necessária ao país para o enfrentamento dos desafios relacionados à segurança cibernética, com a devida consideração das particularidades e prioridades nacionais.

Como o questionário foi elaborado e aprimorado ao longo das suas edições com a participação multissetorial e de *experts*, além de ser baseado em um arcabouço flexível, não parece ser o caso de uma imposição de modelo. No entanto, cada país ao fazer essa identificação de lacunas precisa avaliá-las dentro do contexto nacional, a fim de verificar a pertinência do desenvolvimento de determinada capacidade, assim como a sua prioridade.

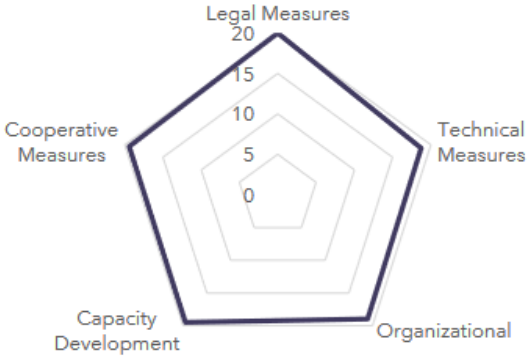
Para contextualizar essa discussão, cabe apresentar os vinte indicadores do GCIe4 que se desdobram em oitenta e duas questões. O pilar da dimensão de medidas legais é composto pelos indicadores direito penal substantivo ou material para crimes cibernéticos e regulação de segurança cibernética. Já o pilar de medidas técnicas abrange os indicadores de CIRT/CSIRT/CERT nacional; CIRT/CSIRT/CERT setorial; arcabouço nacional para implementação de padrões de segurança cibernética; e proteção da criança no ambiente digital. Na sequência, o pilar de medidas organizacionais decompõe-se em ENSC; agência responsável; e métricas de segurança cibernética (ITU, 2021b, p. 138-148).

O quarto pilar endereça as medidas de desenvolvimento de capacidades, integrado pelos indicadores de campanha de conscientização do público em geral sobre segurança cibernética; treinamento de segurança cibernética para profissionais; desenvolvimento ou apoio a programas educacionais ou currículos acadêmicos em segurança cibernética; programas de pesquisa e desenvolvimento em segurança cibernética; indústria nacional de segurança cibernética; e mecanismos governamentais de incentivos. Finalmente, no quinto pilar de medidas de cooperação, tem-se acordos bilaterais; participação em mecanismos internacionais relacionados às atividades de segurança cibernética; acordos multilaterais de segurança cibernética; parcerias com o setor privado; e parcerias interagências (ITU, 2021b, p. 149-156).

O GCIe4 também inovou a apresentar um perfil dos países contendo a pontuação final, pontuação em cada pilar, área(s) de destaque e área(s) de potencial crescimento, também indicando o nível de desenvolvimento do país. Traz-se aqui o perfil do Brasil no GCIe4:

Figura 3 - Perfil do Brasil na Quarta Edição do Índice Global de Segurança Cibernética (GCIe4)

Brazil (Federative Republic of)



Development Level:
Developing Country

Area(s) of Relative Strength
Legal Measures
Area(s) of Potential Growth
Technical, Organizational Measures

Overall Score	Legal Measures	Technical Measures	Organizational Measures	Capacity Development	Cooperative Measures
96.60	20.00	18.73	18.98	19.48	19.41

Fonte: ITU, 2021b, p. 57.

Sem olvidar da ressalva sobre a comparabilidade da classificação das edições anteriores (alteração nos indicadores, número de questões, pontuação e peso das questões, escala de pontuação, etc.), surge o questionamento sobre a melhora substantiva do país no GCIe4. Obviamente, não se trata de um desenvolvimento isolado, em apenas um dos pilares, porém desde a coleta realizada em 2018 o Brasil desenvolveu capacidades principalmente relacionadas às medidas organizacionais, com a aprovação da PNSI, E-Ciber e indicativo do GSI/PR como entidade responsável pela coordenação da segurança cibernética em âmbito nacional. Esses desenvolvimentos, em face do recorte temporal do processo GCIv3 já citado anteriormente, foram considerados somente no GCIe4.

Ademais, outras capacidades também foram posteriores à coleta do GCIv3 e apresentadas no GCIe4 como a existência de simulação nacional de segurança cibernética (Exercício Guardião Cibernético[16]); regulação setorial específica para o setor de telecomunicações[17] e outras normatizações de requisitos de segurança cibernética[18]; processo

[16] Para maiores informações sobre o Exercício Guardião Cibernético ver LIMA E SILVA (2020).

[17] Regulamento de Segurança Cibernética Aplicada ao Setor de Telecomunicações, aprovado em 21 de dezembro de 2020. Disponível em: https://informacoes.anatel.gov.br/legislacao/index.php/component/content/article?id=1497. Acesso em: 11 ago. 2022.

[18] Instrução Normativa nº 4, de 26 de março de 2020, que dispõe sobre requisitos mínimos de Segurança Cibernética que devem ser adotados no estabelecimento das redes 5G, aprovada pelo GSI/PR. Texto na íntegra pode ser consultado em: https://www.in.gov.br/web/dou/-/instrucao-normativa-n-4-de-26-de-marco-de-2020-250059468. Acesso em: 11 ago. 2022.

de adesão à Convenção de Budapeste; e diversos acordos bilaterais de cooperação em segurança cibernética[19].

Esses desenvolvimentos tiveram impacto significativo na pontuação, fazendo com que o Brasil pulasse para a décima oitava (18º) classificação, reiterando-se novamente a advertência das alterações no questionário e na sua metodologia (fato que dificulta a sua comparabilidade), bem como o fato do índice não mensurar a implementação dessas capacidades, nem a sua efetividade, já explicitadas ao longo do texto.

Deixa-se de apresentar aqui a integralidade do questionário, com as suas oitenta e duas questões, tendo em vista que abordam dimensões e tópicos que extrapolam a delimitação dessa pesquisa (por exemplo ao tratar da legislação de crimes cibernéticos). No entanto, detalhou-se o pilar organizacional, em face da sua pertinência temática. Essa seção do questionário contém os seguintes questionamentos[20]:

Questionário GCI: Medidas Organizacionais

1. Estratégia Nacional de Segurança Cibernética

1.1 O seu país tem uma estratégia ou política nacional de segurança cibernética?

- Abarca a proteção de infraestruturas críticas da informação nacionais, incluindo o setor de telecomunicações?
- Tem referência à resiliência cibernética nacional?
- A estratégia é revisada e atualizada de forma contínua?
- A estratégia está aberta a alguma forma de consulta com experts nacionais em segurança cibernética?

1.2 Existe algum plano de ação ou roteiro para a implementação da governança de segurança cibernética?

1.3 Existe uma estratégia nacional para proteção das crianças no ambiente digital?

2. Agência Responsável

2.1. Existe uma agência responsável pela coordenação nacional de segurança cibernética?

2.1.1 Essa agência supervisiona a Proteção Nacional de Infraestruturas Críticas da informação?

2.2.2 Existe uma agência supervisionando nacionalmente o desenvolvimento de capacidades de segurança cibernética?

2.2.3 Existe uma agência supervisionando nacionalmente as iniciativas de proteção das crianças no ambiente digital?

3. Métricas de Segurança Cibernética

3.1. Existem auditorias de segurança cibernética realizadas em nível nacional?

3.2 Existem métricas para avaliar os riscos associados ao ambiente cibernético em nível nacional?

3.3. Existem medidas para avaliar o nível de desenvolvimento de segurança cibernética em nível nacional?

---

[19] Por exemplo, acordos bilaterais com Índia, Israel, Suriname e etc, cujas informações podem ser consultadas, respectivamente em: https://agenciabrasil.ebc.com.br/politica/noticia/2020-01/brasil-e-india-assinam-acordos-em-tecnologia-energia-e-seguranca; https://concordia.itamaraty.gov.br/detalhamento-acordo/12273?TituloAcordo=Israel&tipoPesquisa=1&TipoAcordo=BL,TL,ML; e https://concordia.itamaraty.gov.br/detalhamento-acordo/12440?TituloAcordo=suriname&tipoPesquisa=1&TipoAcordo=BL,TL,ML.

[20] Tradução livre do questionário constante do relatório dos resultados do GCIe4 (ITU, 2021b, p. 145-148).

> **Forneça algumas das melhores práticas/conquistas/desenvolvimentos em andamento do seu país relacionado às medidas organizacionais como parte das suas atividades em segurança cibernética.** (Grifo original).

O Relatório que apresenta os resultados do GCIe4 contextualiza os pilares como temas-chave, apontando que as medidas organizacionais avaliam os mecanismos de governança e coordenação do país em matéria de segurança cibernética. Na mesma linha, essas medidas abrangem a garantia de que a segurança cibernética é amparada no mais alto nível do Poder Executivo e também englobam a identificação dos papéis e responsabilidades das várias entidades nacionais envolvidas, as quais devem prestar contas sobre sua atuação. Nessa toada, ressalta que a insuficiência de medidas organizacionais adequadas pode colaborar para a ausência de clareza nas responsabilidades e na prestação de contas, prejudicando uma coordenação intragovernamental e intersetorial efetiva (ITU, 2021b, p. 8).

Outro ponto de atenção refere-se à importância de ENSC atualizadas, instrumento que é o elemento-chave de medidas organizacionais em âmbito nacional. Relembra-se que a coleta do questionário apontou que cento e vinte e sete países possuíam uma estratégia ou estavam em processo de elaboração. Mais que isso, sessenta países demonstraram progresso na definição de metas claras através do desenvolvimento e revisão de novas estratégias ou através da atualização do respectivo plano de ação (ITU 2021b, p. 9).

Com o amadurecimento do GCI, coloca-se luz na prática dos países que se engajam em processos regulares de atualização das suas estratégias, com o intuito de que estejam adaptadas à realidade. Em que pese desenvolver uma ENSC seja um importante primeiro passo, faz-se necessária a sua revisão contínua. Em termos de linha do tempo, o Relatório observa que muitos países adotam ciclos quadrienais ou quinquenais de revisão. Entretanto, alguns optam por prazos maiores, como uma década ou mais (ITU, 2021b, p. 9).

Para finalizar a apresentação do GCI, faz-se necessário indicar a aprovação de recente alteração relevante na apresentação dos resultados e que impactará a próxima edição do índice (GCIe5), que deverá iniciar a coleta de dados no início de 2023. A Conferência Mundial de Desenvolvimento das Telecomunicações, aprovou proposta para modificar a forma como os resultados do GCI serão apresentados, os quais irão abandonar a classificação individual para passar a classificar tão somente em grupos, nos termos da Resolução nº 45 (Rev. Kigali, 2022) – Mecanismos para aumento da cooperação em segurança cibernética, incluindo combate ao *spam*[21]. Tal providência segue o modelo adotado por outros indicadores da UIT e objetiva

[21] *Resolution 45 (Rev. Kigali, 2022) - Mechanisms for enhancing cooperation on cybersecurity, including countering and combating spam*. "*The World Telecommunication Development Conference (Kigali, 2022) […]*

refletir com mais acurácia o desenvolvimento das capacidades de segurança cibernética. Ou seja, na próxima edição não haverá mais a classificação global e regional dos países, mas tão somente a sua classificação em um dos grupos que refletirão o estágio do desenvolvimento das capacidades nos cinco pilares da GCA, em metodologia não definida na Resolução, nem em outro documento até a presente data.

Nota-se que a apresentação do GCA, do GCI e dos resultados das edições dos GCI serve para corroborar a importância da estruturação pelos países de um modelo institucional e de governança que permita a coordenação de esforços em várias dimensões para promover a segurança cibernética e para enfrentar os crescentes e emergentes desafios. Nessa esteira, traz-se uma outra iniciativa da UIT que dialoga e retroalimenta o GCI, especialmente o pilar de medidas organizacionais, destacando-se o esforço para a elaboração de um documento referencial para assistência aos países na elaboração das suas estratégias iniciais.

Assim, foi desenvolvido um guia para o desenvolvimento de ENSCs e é justamente esse Guia que será considerado como o segundo modelo para fins do presente trabalho.

O *Guia para o Desenvolvimento de uma Estratégia Nacional de Segurança Cibernética - Engajamento estratégico em segurança cibernética,* teve sua primeira edição publicada em 2018 (ITU *et al.*, 2018a), e a segunda edição em 2021 (ITU *et at.*, 2021c). O Guia é fruto de uma parceria multissetorial de várias organizações, contando com doze parceiros na primeira edição (ITU *et al.*, 2018a) e vinte na sua segunda (ITU *et al.*, 2021c).

O Guia contempla tanto o processo quanto o conteúdo de uma estratégia, apresentando-se como um arcabouço flexível, amigável e útil para o estabelecimento da visão socioeconômica de um país e da sua postura de segurança cibernética, assim como para auxiliar os elaboradores de políticas no desenvolvimento de suas estratégias, considerando as particularidades dos países (ITU *et al.*, 2021c, p. 8).

O objetivo de cotejar o documento no trabalho, assim como o modelo da OCDE, não se limita à apresentação desses documentos em si, mas de trazer as considerações que apoiarão a discussão das prescrições normativas da presente tese.

Para fins da pesquisa, utiliza-se a segunda edição do Guia, com a nota metodológica de que seu conteúdo é compatível com a primeira edição, a qual foi ampliada e revisada, também capturando as tendências emergentes e a evolução do panorama dos riscos, os quais devem ser

---

instructs the Director of the Telecommunication Development Bureau […] 5 to change how the results of the GCI are presented so that countries are represented in tiers rather than by individual ranking in order to more accurately reflect the development of cybersecurity in Member States" – ITU (2022a).

considerados no planejamento estratégico nacional. Não houve alteração na estrutura, nem no nível de detalhamento do conteúdo (ITU *et al.*, 2021c, p. 4).

Em termos de estrutura, o documento divide-se em sete partes: visão geral do documento; introdução, ciclo de vida de uma ENSC; princípios; boa prática nacional de segurança cibernética; materiais de referência; e acrônimos (ITU at al., 2021c, p. 3).

Na introdução, o Guia destaca a inexistência de uma definição estabelecida e acordada do que constitui uma ENSC, encorajando os atores a pensar em uma ENSC como expressão da visão, objetivos de alto nível, princípios e prioridades que guiam os países no endereçamento de segurança cibernética; uma visão geral dos atores responsáveis pela segurança cibernética do país, com respectivos papéis e responsabilidades; e uma descrição de passos, programas e iniciativas que o país deve adotar para proteger suas IECs e, nesse processo, aumentar sua segurança e resiliência (ITU *et al.*, 2021c, p. 13).

As prioridades dos países variam, no entanto, o estabelecimento da visão, dos objetivos e das prioridades permite aos governos visualizar segurança cibernética de maneira holística, permitindo uma atuação estratégica. Além disso, a ENSC também oportuniza o alinhamento das prioridades em segurança cibernética com outros objetivos da agenda digital e seu processo de desenvolvimento deve traduzir a visão governamental em políticas coerentes e implementáveis que permitirão o alcance dos objetivos, o que inclui não só as ações e medidas que devem ser implementadas, mas também a alocação de recursos e identificação de métricas (ITU *et al.,* 2021c, p. 13).

A Seção destinada ao ciclo de vida de uma ENSC detalha suas fases e destaca que a autoridade que lidera o processo deve ser neutra durante toda a sequência de desenvolvimento, motivo pelo qual recomenda que a entidade responsável pelo desenvolvimento seja diferente da entidade responsável pela implementação da ENSC ou que se adote outro mecanismo para endereçar o viés inerente e evitar a competição intragovernamental por recursos (ITU *et al.,* 2021c, p. 16-18).

Ao tratar da fase de produção da ENSC, após a fase de análise e inventário, passa-se à fase de redação da Estratégia, a qual deve fornecer uma direção em segurança cibernética para o país; expressar visão e escopo claros; e estabelecer os objetivos com o respectivo prazo e priorizá-los conforme seus impactos. Ademais, deve identificar possíveis ações; incentivar esforços de implementação; e guiar a alocação de recursos, podendo contemplar alguns dos resultados da fase de análise e inventário (ITU *et al.,* 2021c, p. 22).

Não obstante, a Estratégia ainda precisa estabelecer um mecanismo claro de governança que defina papéis e responsabilidades dos atores, incluindo a identificação de responsáveis pela

gestão e avaliação do instrumento, bem como entidade responsável pela implementação. Como exemplo de entidade responsável, o Guia cita um conselho nacional de segurança cibernética ou uma autoridade central. Por fim, a Estratégia precisa definir e/ou confirmar o mandado de diferentes entidades envolvidas na arquitetura de segurança cibernética do país, esclarecendo como essas entidades irão interagir umas com as outras e com a entidade responsável pela implementação (ITU *et al.,* 2021c, p. 22).

A aprovação do documento seguirá o processo particular de aprovação de cada país, o qual pode envolver algum processo legislativo ou somente aprovação do Poder Executivo, por exemplo, através de decreto no contexto jurídico brasileiro. De qualquer maneira, é essencial que não só a aprovação seja do mais alto nível do governo, mas que esse compromisso permaneça durante a fase de implementação, a qual pode ser apoiada com um Plano de Ação que identificará as ações para concretizar os objetivos da ENSC (ITU *et al.,* 2021c, p. 23-24).

Ainda em termos de implementação, a autoridade responsável pela implementação deve identificar entidades governamentais para cada uma das ações, as quais serão responsáveis e deverão prestar contas pela respectiva implementação, assim como coordenar os esforços com os atores relevantes como parte desse processo. Não pode ser esquecida a avaliação sobre a existência de mandato para que as entidades possam implementar as ações e a existência dos adequados recursos, cabendo à autoridade responsável assistir às demais entidades na garantia dos meios necessários. Finalmente, o último componente da fase de implementação e elemento crítico do Plano de Ação é a definição de métricas e indicadores de performance, a fim de avaliar a efetividade e eficiência das iniciativas (ITU *et al.,* 2021c, p. 24-25).

Em termos principiológicos, nota-se um diálogo convergente com o modelo da OCDE. O Guia elenca nove princípios que auxiliarão no desenvolvimento de uma ENSC holística e voltada para o futuro. São eles:

a) a ENSC deve apresentar uma visão clara de todo o governo e de toda a sociedade;
b) a ENSC deve resultar de um entendimento e análise abrangentes sobre o ambiente digital como um todo e contextualizado às prioridades e às circunstância de cada país;
c) a ENSC deve ser desenvolvida com a ativa participação de todos os atores relevantes e deve endereçar as suas necessidades e as suas responsabilidades;
d) a ENSC deve promover a prosperidade social e econômica e maximizar a contribuição das TICs para o desenvolvimento sustentável e inclusão social;
e) a ENSC deve respeitar e ser consistente com os direitos humanos fundamentais;
f) a ENSC deve possibilitar o gerenciamento eficiente dos riscos de segurança cibernética e conduzir à resiliência as atividades econômicas e sociais;

g) a ENSC deve utilizar os mais adequados instrumentos de políticas disponíveis para realizar cada um dos seus objetivos, considerando as circunstâncias específicas de cada país;
h) a ENSC deve ser estabelecida no mais alto nível de governo, sendo assim responsável por atribuir os papéis e responsabilidades relevantes e por alocar os recursos humanos e financeiros suficientes; e
i) a ENSC deve ajudar a criar um ambiente digital em que cidadãos e organizações possam confiar (ITU *et al.,* 2021c, p. 28-31).

A Seção orientada à apresentação de melhores práticas identifica uma série de elementos que otimiza a ENSC, a fim de que se torne efetiva e abrangente, ao passo que, permita sua adequação ao contexto nacional. São sete áreas para foco: governança; gerenciamento dos riscos no contexto de segurança cibernética nacional; preparação e resiliência; IEC e serviços essências; construção de capacidades e conscientização; legislação e regulação; e cooperação internacional (ITU *et al.,* 2021c, p. 34-53).

Em termos Governança, o Guia cita alguns elementos de boas práticas que devem ser considerados para inclusão no texto da ENSC. A ENSC deve indicar claramente os papéis e responsabilidades de atores responsáveis pela implementação e introduzir medidas que permitam a responsabilização de autoridades e funcionários que possuem o dever de implementar, monitorar e avaliar os resultados da ENSC. Nessa esteira, a ENSC deve identificar e empoderar a autoridade competente responsável pela implementação; estabelecer mecanismo para identificar e realizar a atribuição para as entidades governamentais afetadas pela Estratégia ou responsáveis pela sua implementação; comprometer-se com a inclusão de objetivos específicos, mensuráveis, baseados em resultados e com marcos temporais no plano de implementação da ENSC; e reconhecer a necessidade de destinar recursos, dentre os quais cita vontade política, tempo, orçamento e recursos humanos, para alcançar os objetivos desejados (ITU *et al.,* 2021c, p. 34).

Dessa forma, essas premissas para a ENSC em Governança são traduzidas em seis elementos. O primeiro deles diz respeito a garantir o mais alto nível de apoio para a ENSC, aumentando a probabilidade de alocação adequada de recursos e coordenação de esforços, bem como sinalizando para o ecossistema nacional mais amplo que a ENSC está entrelaçada com a economia digital e outros aspectos sociais e políticos, constituindo-se uma prioridade nacional.

Cumpre destacar nesse ponto o alerta do Guia de que a ENSC pode necessitar ser codificada no arcabouço jurídico doméstico para garantir a relevância nacional e priorização (ITU *et al.,* 2021c, p. 34-35).

O segundo elemento aborda o estabelecimento de uma autoridade competente de segurança cibernética. Aqui a ENSC deve identificar uma autoridade nacional competente designada para a sua execução, devendo ser um líder (indivíduo ou entidade) em posição fortemente ancorada no mais alto nível de governo. Essa posição é justificada pela necessidade de guiar, coordenar as ações e monitorar a sua implementação, também sendo responsável por reportar sobre o progresso dos resultados da ENSC.

Além disso, essa autoridade deve fazer a gestão, sendo responsável por definir e clarificar papéis, responsabilidades, processos e tarefas necessárias para garantir a efetiva implementação da ENSC. Dentre o rol de atribuições, também se inclui a identificação de atores que irão supervisionar a implementação e o estabelecimento de metas para todos os órgãos, entidades e indivíduos responsáveis por aspectos específicos da ENSC e subsequente plano de ação (ITU *et al.,* 2021c, p. 35).

Novamente, o próprio Guia adverte que, em alguns casos, a posição dessa autoridade nacional de segurança cibernética precisa ter amparo legal ou de políticas para permitir a execução da sua missão. Outrossim evidencia que essa autoridade precisa ter a habilidade de envolver e guiar os atores relevantes. Essa atribuição, à semelhança dos pontos anteriores, pode exigir legislação adicional que inclua essa competência e determine que as entidades governamentais devem responder à autoridade nacional sobre seu progresso no alcance das metas de implementação (ITU *et al.,* 2021c, p. 35).

O terceiro elemento aborda a garantia de cooperação intragovernamental, devendo a ENSC estabelecer mecanismo de identificar e incluir entidades governamentais abarcadas pela ENSC e/ou responsáveis pela implementação. Nesse ponto específico, o Guia enfatiza que uma autoridade nacional bem estabelecida e de alto nível também contribui para o aprimoramento da coordenação e colaboração intragovernamental.

A efetiva comunicação e coordenação garante que todos ministérios e agências governamentais estão cientes das respectivas atribuições, missões e tarefas de cada uma das entidades e órgãos envolvidos. Como exemplo de mecanismo de coordenação, o Guia cita reuniões periódicas com atores relevantes para revisão dos planos de ação e, como mecanismo de cooperação, cita a criação de força-tarefa intragovernamental (ITU *et al.,* 2021c, p. 35).

Após abordar o elemento de cooperação intragovernamental, o quarto elemento foca na cooperação intersetorial, devendo a ENSC reconhecer a interdependência existente entre governos, setor privado e outros atores não estatais para o alcance de um ecossistema mais seguro e resiliente. Para tanto, a ENSC deve articular como o governo engajar-se-á com os diferentes atores e definir seus papéis e responsabilidades, também se alinhando com outras

prioridades nacionais. Como exemplo desse elemento, o Guia cita a previsão na ENSC de uma rede de pontos de contato nacionais de indústrias críticas, essenciais para a operação e recuperação das IECs (ITU *et al.,* 2021c, p. 36).

O quinto elemento endereça a alocação de orçamento e recursos dedicados, cabendo à ENSC essa especificação para fins de sua implementação, manutenção e revisão. O Guia enfatiza que a suficiente, adequada e consistente alocação de orçamento é a base para uma postura nacional efetiva em segurança cibernética. Os recursos devem especificar orçamento dedicado, pessoas e materiais, em um processo que precisa ser periodicamente reavaliado em conjunto com o progresso de implementação da ENSC. Ainda nesse tema, pode ser avaliado o estabelecimento de um orçamento central de segurança cibernética, a ser gerenciado por um mecanismo de governança central. Independentemente do modelo escolhido, centralizado ou não, é necessária a adequada gestão do orçamento para permitir a implementação exitosa da ENSC (ITU *et al.,* 2021c, p. 36).

O sexto elemento de governança trata do desenvolvimento de plano de implementação, o qual deve acompanhar a ENSC ou ser por ela referenciado, detalhando como os objetivos estratégicos serão atingidos. Planos de implementação efetivos apontam as entidades responsáveis para cada uma das ações, os recursos necessários ao longo do tempo, os processos e os resultados esperados (ITU *et al.,* 2021c, p. 36).

A segunda área de foco de boas práticas para ENSC refere-se à gestão dos riscos no contexto de segurança cibernética nacional. Nesta área, os elementos de melhores práticas envolvem a condução de avaliação de ameaças e o respectivo alinhamento das políticas; a identificação de uma abordagem de gestão de riscos e metodologia comum para o seu gerenciamento; desenvolvimento de perfis de riscos setoriais; e estabelecimento de políticas de segurança cibernética (ITU *et al.,* 2021c, p. 37-38).

A terceira área de foco é a preparação e resiliência, que abarca estabelecimento das capacidades de resposta a incidentes cibernéticos; estabelecimento de planos de contingência para o gerenciamento de crises de segurança cibernética e recuperação de desastres; promoção do compartilhamento de informações; realização de exercícios de segurança cibernética; e estabelecimento de avaliação de impacto ou severidade dos incidentes cibernéticos (ITU *et al.,* 2021c, p. 40-41).

A quarta área de foco enfrenta a temática de IEC e serviços essenciais, cujos elementos em destaque são o estabelecimento de uma abordagem de gestão de riscos para identificação e proteção dessas infraestruturas e serviços; adoção de um modelo de governança com responsabilidades claras; definição de parâmetros mínimos de segurança; utilização de ampla

gama de alavancas de mercado; e estabelecimento de parcerias público-privadas (ITU *et al.,* 2021c, p. 41-44).

A quinta área de foco abrange a construção de capacidades e conscientização, a qual compreende planejamento estratégico; desenvolvimento de currículo de segurança cibernética (multidisciplinar, abrangendo tópicos técnicos e não técnicos e englobando os ensinos fundamental, médio e superior); estimular a qualificação em segurança cibernética; implementar um programa coordenado de conscientização; fomentar iniciativas de inovação e pesquisa e desenvolvimento em segurança cibernética; e adaptar programas para grupos e setores vulneráveis (ITU *et al.,* 2021c, p. 44-47).

Já a sexta área foca em legislação e regulação indicando o estabelecimento de um arcabouço jurídico doméstico sobre segurança cibernética; arcabouço jurídico doméstico sobre crimes cibernéticos e evidência eletrônica; reconhecimento e salvaguarda dos direitos e liberdades fundamentais; criação de mecanismos de conformidade; promoção de capacitação para os órgãos envolvidos na persecução penal; estabelecimento de processos interorganizacionais; e apoio à cooperação internacional para o combate de ameaças e crimes cibernéticos (ITU *et al.,* 2021c, p. 47-50).

Retomando-se o ponto de um arcabouço jurídico de segurança cibernética, cabe o destaque de que a ENSC deve encorajar o desenvolvimento de arcabouços de segurança cibernética e de proteção de dados pessoais. Adicionalmente, e considerando o instrumento utilizado e o sistema jurídico de cada país, a ENSC deve estabelecer, atualizar e reformar o arcabouço legal de segurança cibernética ou promover o seu desenvolvimento e revisão. Como áreas que devem ser objeto desse esforço, o Guia menciona, por exemplo: o estabelecimento de agências nacional e setoriais para tratar de aspectos de segurança cibernética (como por exemplo, agências nacionais de segurança cibernética e CIRTs/CSIRTs/CERTs nacionais e setoriais, etc); identificação de IECs; certificação de organizações, processos, produtos e políticas de segurança cibernética; regras estaduais e nacionais de segurança aplicáveis à segurança do ambiente cibernético; etc (ITU *et al.,* 2021c, p. 47-50).

A última área enfatiza a cooperação internacional assinalando como elementos o reconhecimento de segurança cibernética como um componente de política externa e o alinhamento dos esforços nacionais e internacionais; o engajamento nas discussões internacionais e o comprometimento com a implementação; a promoção de cooperação formal e informal nessa seara; e a promoção de capacitação para cooperação internacional (ITU *et al.,* 2021c, p. 50-53).

Dessa forma, finaliza-se a apresentação da UIT, de suas iniciativas temáticas que se relacionam com o objeto do presente trabalho, especialmente a GCA e o GCI e, mais especificamente, as diretrizes constantes do *Guia para o Desenvolvimento de uma Estratégia Nacional de Segurança Cibernética,* explanando-se na sequência um modelo acadêmico que está sendo utilizado largamente com apoio de organizações intergovernamentais para avaliação e subsídio para a construção de capacidades em segurança cibernética.

2.3 MODELO DE MATURIDADE DE CAPACIDADE DE SEGURANÇA CIBERNÉTICA (CMM) DO CENTRO GLOBAL DE CAPACIDADE DE SEGURANÇA CIBERNÉTICA (GCSCC*), DA OXFORD MARTIN SCHOOL* DA UNIVERSIDADE DE OXFORD

Após a descrição das diretrizes de duas organizações intergovernamentais, continua-se ainda no caminho da demonstração de modelos existentes, apresentando-se um modelo acadêmico, qual seja o Modelo de Maturidade de Capacidade de Segurança Cibernética (CMM) do Centro Global de Capacidade de Segurança Cibernética (GCSCC) da Universidade de Oxford, já destacando que a avaliação das capacidades brasileiras em segurança cibernética foram baseada no CMM e subsidiaram o esforço brasileiro de elaboração da nossa ENSC, a E-Ciber.

O GCSCC é um programa da *Oxford Martin School*, renomado centro de pesquisa da Universidade de Oxford, que se situa no Departamento de Ciência da Computação da Universidade e é líder na pesquisa para eficiência e efetividade na construção de capacidades de segurança cibernética, promovendo aumento de ritmo, escala, qualidade e impacto das iniciativas nessa temática ao redor no mundo. Seu objetivo é garantir que o conhecimento e a pesquisa do Centro possam auxiliar aos países a aprimorarem suas capacidades, contribuindo assim para um ambiente cibernético que promova os direitos humanos, prosperidade e bem-estar para todos (OXFORD, 2021, p. 62).

A edição de 2021 do CMM ressalta que o modelo assiste aos países na compreensão do que funciona; o que não funciona; e o motivo pelo qual não funciona, nas áreas que refletem as capacidades em segurança cibernética. Essa avaliação pode guiar a atuação governamental e privada na adoção de políticas e investimentos que podem ter impacto significativo no aumento da segurança no ciberespaço. Ademais, o Sumário Executivo do documento aponta que o Centro Global de Capacidade de Segurança Cibernética já realizou mais de cento e vinte revisões das capacidades de segurança cibernética para atores-chave internacionalmente, em

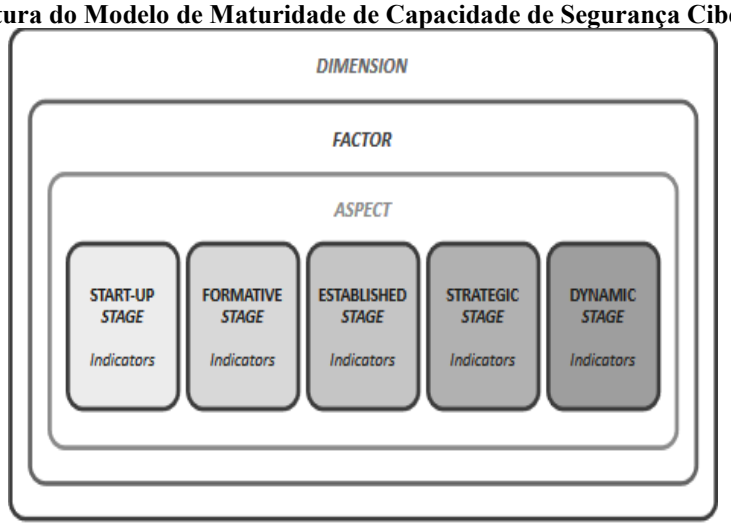
mais de oitenta e cinco países (OXFORD, 2021, p. 2), fato que demonstra a aceitação e difusão do modelo.

O modelo é composto de cinco dimensões: Estratégia e Política de Segurança Cibernética; Cultura de Segurança Cibernética e Sociedade; Construção de Conhecimento e Capacidades em Segurança Cibernética; Arcabouço Legal e Regulatório; e Padrões e Tecnologia, que exprimem capacidade nacional necessária para ser efetiva a entrega de segurança cibernética por qualquer país (OXFORD, 2021, p. 5).

É importante mencionar que o arcabouço do CMM não se limita a endereçar as dimensões em que a capacidade nacional em segurança cibernética deve ser avaliada, mas decompõe-se em fatores dentro de cada uma das dimensões, os quais representam elementos essenciais da capacidade nacional que serão posteriormente mensurados para a avaliação dos estágios de maturidade. Esses fatores ainda podem ser decompostos em aspectos, quando possuem múltiplos elementos e o estágio reflete o grau de progresso de um país em determinado fator ou aspecto de segurança cibernética. Finalmente, os indicadores constituem a parte mais elementar da estrutura do modelo, descrevendo as ações, passos e elementos fundacionais que apontam para um específico estágio de maturidade, configurando-se na sua maioria em forma binária, ou seja, ou o país atende ou não aos critérios daquele indicador (OXFORD, 2021, p. 7).

A figura abaixo representa a decomposição da estrutura do CMM:

Figura 4 - Estrutura do Modelo de Maturidade de Capacidade de Segurança Cibernética (CMM)



Fonte: OXFORD, 2021, p. 7.

Os estágios de maturidade são classificados da seguinte forma: início; formativo; estabelecido; estratégico; e dinâmico, que refletem as ideias centrais de início do

desenvolvimento das capacidades; capacidades estabelecidas; liderar mundialmente; e condições de antecipar e preparar-se para as necessidades futuras (OXFORD, 2021, p. 6).

O Estágio Inicial indica inexistência de maturidade e de evidências de capacidades de segurança cibernética, podendo incluir debates, porém sem ações concretas. No segundo degrau de maturidade, o Estágio Formativo traduz-se na formulação de alguns aspectos, com evidências, mas ainda de forma desorganizada, pontual ou recente. Já no Estágio Estabelecido, nota-se a implantação dos indicadores dos respectivos aspectos do fator e as evidências demonstram seu funcionamento, no entanto, inexiste avaliação sobre efetividade da alocação de recursos, embora o aspecto esteja definido e seja funcional (OXFORD, 2020b, p. 31; 2021, p. 8).

Continuando, o Estágio Estratégico, demostra um olhar estratégico sobre aspectos, como a identificação de áreas prioritárias, a qual se baseia nas particularidades da organização ou Estado. Por fim, o Estágio Dinâmico revela uma abordagem estratégica e capacidade de adaptação, com a existência de mecanismos para alteração da estratégia vigente, permitindo a mudança para enfrentar novas conjunturas. São características desse estágio: processos rápidos de tomada de decisão; realocação de recursos; e permanente monitoramento do contexto. Ademais, também existe evidência de liderança global em assuntos de segurança cibernética (OXFORD, 2020b, p. 31; 2021, p. 8).

Passa-se à análise dos fatores que compõem cada uma das dimensões, com base na recente edição de 2021 do modelo (OXFORD, 2021, p. 9-59), sendo que a Dimensão de Estratégia e Política de Segurança Cibernética é composta de quatro fatores: ENSC; Gerenciamento de Crise e Resposta de Incidentes; Proteção de Infraestrutura Crítica; e Segurança Cibernética na Defesa e Segurança Nacional (OXFORD, 2021, p. 9-11).

Já a Dimensão Cultura de Segurança Cibernética e Sociedade é integrada por cinco fatores: Mentalidade de Segurança Cibernética; Confiança nos Serviços Digitais; Entendimento do Usuário sobre a Proteção de Informações Pessoais On-line; Mecanismos de Denúncia; e Mídia e Redes Sociais (OXFORD, 2021, p. 19-21).

A Dimensão de Construção de Conhecimento e Capacidades em Segurança Cibernética abarca quatro fatores: Conscientização em Segurança Cibernética; Educação em Segurança Cibernética; Treinamento Profissional em Segurança Cibernética; e Pesquisa e Inovação em Segurança Cibernética (OXFORD, 2021, p. 29-31); enquanto que a Dimensão de Arcabouço Legal e Regulatório também elege quatro fatores: Disposições Legais e Regulamentares; Arcabouços Legislativos Relacionados; Capacidade Legal e Regulatória; e Arcabouços Formais e Informais de Cooperação para Combate dos Crimes Cibernéticos (OXFORD, 2021,

p. 38-40).

Finalizando, a Dimensão de Padrões e Tecnologia é formada por seis fatores: Aderência a Padrões; Controles de Segurança; Qualidade de *Software*; Resiliência da Infraestrutura de Internet e de Comunicações; Mercado de Segurança Cibernética; e Divulgação Responsável de Vulnerabilidades (OXFORD, 2021, p. 48-50).

Cabe especificar para fins do trabalho, considerando a delimitação do objeto, os aspectos do Fator ENSC, bem como os indicadores que compõe cada um dos desses aspectos. O Fator ENSC decompõe-se em quatro aspectos: Desenvolvimento da Estratégia; Conteúdo; Revisão e Implementação; e Engajamento Internacional. Cada aspecto apresenta os indicadores que refletem os estágio de maturidade, sendo elaborado o quadro abaixo para facilitar a compreensão[22]:

Quadro 1 - Indicadores que refletem os estágios de maturidade em cada um dos quatro aspectos do Fator Estratégia Nacional de Segurança Cibernética (ENSC) da Dimensão de Estratégia e Política de Segurança Cibernética do Modelo de Maturidade de Capacidade de Segurança Cibernética (CMM)

Aspectos	Estágios				
	Início	**Formativo**	**Estabelecido**	**Estratégico**	**Dinâmico**
Desenvolvimento da Estratégia	- Inexistência de ENSC. Pode ter sido iniciado o processo de desenvolvimento; e - Pode ter sido solicitado o aconselhamento de parceiros internacionais.	- Iniciado processo para desenvolvimento da ENSC; - Minuta da ENSC foi elaborada; e - Processos de consulta dos atores-chave foi acordado, incluindo setor privado, sociedade civil e parceiros internacionais.	- Publicação de ENSC; - Foi conduzida avaliação específica dos riscos nacionais de segurança cibernética do país; - ENSC apresenta necessidade e papéis dos atores relevantes; - Programa de implementação já operacional cobrindo o escopo da ENSC; e - Mecanismos em operação para permitir que responsáveis monitorem o alcance dos resultados, tratem dos problemas de implementação	- Implantados os processos de revisão e renovação estratégicos da ENSC; - Riscos emergentes de segurança cibernética são regularmente avaliados e considerados na atualização da ENSC e do plano de implementação; - Impacto da ENSC na redução do risco e dano é compreendido e usado para informar as decisões orçamentárias e de priorização.	- ENSC e Plano de Implementação são proativamente revisados para considerar desenvolvimentos estratégicos de outros campos no país (ex: social, técnico, econômico, etc); - País tem autoridade reconhecida na comunidade internacional e apoia o desenvolvimento de ENSC e estratégias globais; e - Segurança Cibernética é considerada dentro de outras estratégias relevantes de nível nacional e

[22] Quadro elaborado a partir de tabela constante do modelo (OXFORD, 2021, p. 12-13).

Aspectos	Estágios				
	Início	**Formativo**	**Estabelecido**	**Estratégico**	**Dinâmico**
			e mantenham o alinhamento estratégico.		programas de implementação.
Conteúdo	- Possível existência de políticas nacionais mencionando segurança cibernética, mas não são abrangentes e há pouca evidência que refletem prioridades ou circunstâncias nacionais específicas.	- Reflete prioridades e circunstâncias específicas do país; - Vínculo entre a ENSC (ou sua minuta) e as prioridades nacionais (p. ex., segurança nacional, estratégia digital, etc), mas geralmente é *ad hoc* e sem detalhamento; e - ENSC (ou sua minuta) define alguns resultados-chave que permitem a avaliação do sucesso.	- Baseado em avaliação abrangente de riscos incluindo vínculos expressos entre políticas e estratégias nacionais mais amplas; - Inclui ações para conscientização dos indivíduos e empresas; mitigação de crimes cibernéticos; estabelecimento de capacidade de resposta a incidentes; promoção de parcerias público-privadas; e proteção IEC e a economia; - Foi considerada como a ENSC pode incorporar ou apoiar outros objetivos de políticas digitais mais ampla, como a proteção das crianças; promoção dos direitos humanos; promoção da igualdade, diversidade e inclusão; e tratamento da desinformação.	- Considera o impacto das tecnologias emergentes, bem como seu uso na IECs, sociedade e economia, nos riscos de segurança cibernética; - Resultados definidos na ENSC são específicos e mensuráveis. Foram definidas métricas que permitem aos atores avaliar a efetividade da estratégia na redução do dano; e - A manutenção dos resultados benéficos além do ciclo de vida da ENSC foi considerada, incluindo como financiar novas capacidades.	- Considera o impacto de desenvolvimento mais amplos (político, econômico, ambiental, etc) nos riscos de segurança cibernética; e - Promove e encoraja cooperação bilateral e multilateral entre países para assegurar um espaço cibernético confiável, seguro e resiliente.
Revisão e Implementação	- Inexistência de um programa de implementação abrangente.	- Desenvolvimento de um programa coordenado de implementação, com participação dos	- Plano de implementação detalhado incluindo atores, entidades responsáveis e recursos	- Métricas orientadas ao resultado são utilizadas para monitorar o impacto que o programa tem na redução do	- Mecanismos instalados para realizar mudança abrangente no programa em caso de mudança

Aspectos	Estágios				
	Início	Formativo	Estabelecido	Estratégico	Dinâmico
		atores relevantes, incluindo setor privado e sociedade civil; - Atribuição das ações do programa para responsáveis, porém sem confirmação dos recursos adequados; e - Mecanismos limitados de revisão dos processos.	orçamentários. Plano de implementação envolve atores relevantes dentro do governo e de outros setores; - Órgão de coordenação foi designado e tem autoridade para garantir que os responsáveis prestem contas sobre a execução; - Recursos necessários para as ações foram identificados e instalados. Deficiências orçamentárias são identificadas e escaladas à autoridade competente; e - Processos de revisão do programa e métricas foram implantados, com o adequado orçamento, permitindo a mensuração do progresso, bem como que os riscos e problemas sejam escalados para a autoridade competente.	risco (e de outros objetivos estratégicos); - Evidência que as métricas são utilizadas para refinar os planos de ação; - Métricas (de progresso e orientadas ao resultado) foram elaboradas a partir de amplas fontes governamentais, não governamentais e internacionais; e - Supervisão independente do programa.	significativa de conjuntura (política, econômica, etc); e - Contribuição do programa para desenvolvimento e aplicação global de métricas orientadas ao resultado.
Engajamento Internacional	- Limitada conscientização sobre principais debates internacionais de políticas de segurança cibernética; e - País pode se beneficiar de redes regionais e internacionais	- País está ciente da existência de discussões internacionais sobre políticas de segurança cibernética e assuntos relacionados; - Ocasionalmente	- Realizada avaliação sobre como esses debates sobre políticas e assuntos relacionados em segurança cibernética afetam os interesses e a posição do país	- País está ativamente construindo comunidades internacionais de interesse sobre objetivos específicos de políticas de segurança cibernética; e	- País é líder na construção de consenso, construindo inclusão e moldando o debate sobre assuntos de políticas de segurança cibernética chave;

Aspectos	Estágios				
	Início	**Formativo**	**Estabelecido**	**Estratégico**	**Dinâmico**
	de colaboração operacional, porém sem ativo engajamento.	o país pode participar de discussões regionais e internacionais em assuntos relacionados, porém sem representar um papel ativo; - O país pode participar passivamente em órgãos relevantes de colaboração operacional e de políticas (por exemplo: Fórum de Governança da Internet; CERTs Regionais; Grupo de Experts de Alto Nível das Nações Unidas, etc).	internacional-mente, definindo-se engajamento específico com envolvimento de muito atores nesse processo; - País participa ativamente dos órgãos e fóruns internacionais relevantes, diretamente ou através de órgãos representativos relevantes. Sua voz é considerada e tem impacto; - País ativamente contribui para órgãos relevantes de colaboração operacional e de políticas.	- País faz contribuição importante para órgão operacionais regionais e internacional, bem como está ativamente envolvido na capacitação de países terceiros.	- Foca no futuro diante dos assuntos emergentes e inicia novos debates internacionais nesses tópicos; e - País está ativamente envolvido na criação de novos mecanismos regionais e internacionais de colaboração.

Fonte: adaptado de Oxford (2021, p. 12-13, tradução nossa).

Cumpre aqui esclarecer que não cabe explorar todos os fatores da Dimensão de Estratégia e Política de Segurança Cibernética, nem de todas as dimensões que compõem o CMM. Como visto, o modelo abarca a revisão das capacidades em várias áreas, muitas das quais não dizem respeito ao Arcabouço Jurídico e à Governança Institucional (por exemplo, Fatores Qualidade de *Software* e Divulgação Responsável de Vulnerabilidades) e cujo aprofundamento não auxiliaria na verificação da hipótese principal da pesquisa. Dessa forma, foca-se no detalhamento do Fator ENSC, endereçado no quadro acima.

Embora já tenha sido mencionado anteriormente, reitera-se que o GCSCC, a convite da OEA, especialmente da Secretaria do Comitê Interamericano contra o Terrorismo (CICTE), analisou o nível de maturidade da capacidade de segurança cibernética do Brasil, com o objetivo de que o governo brasileiro compreendesse sua capacidade de segurança cibernética e, a partir disso, tivesse condições de priorizar estrategicamente seus esforços (OXFORD, 2020b. p. 10). O estudo denomina-se "*Revisão da Capacidade de Cibersegurança: República Federativa do Brasil*" e reflete um processo que se iniciou em 2018 e já inclui os avanços consolidados com

a publicação da E-Ciber. Recorda-se que especificamente quanto ao Fator ENSC, a capacidade brasileira foi avaliada como Estágio Formativo-Estabelecido (OXFORD, 2020b, p. 40).

Antes de adentrar na análise detalhada desse fator realizada pelo GCSCC, apresenta-se gráfico com a visão geral da capacidade brasileira em todas as dimensões do CMM. Ressalva-se, apenas, que algumas modificações podem ser constatadas em comparação à descrição do modelo anteriormente feita. Essas decorrem de ajustes sofridos na revisão do modelo publicada em 2021, ou seja, posterior à entrega da avaliação, que foi publicada em 2020.

Gráfico 1 - Visão geral da capacidade de segurança cibernética do Brasil

Fonte: OXFORD, 2020b, p. 12.

Com relação ao gráfico acima, esclarece-se que cada quinta parte do gráfico representa uma das cinco dimensões do modelo, apresentando cada um dos fatores que compunham o CMM à época da análise. Quanto mais próximo do centro, mais inicial o estágio de maturidade,

evoluindo em direção ao perímetro (OXFORD, 2020b, p. 12). Ainda que pelo gráfico não seja possível afirmar o estágio de maturidade das capacidades, permite a visualização de certa harmonização dos estágios de maturidade. Percebe-se que as capacidades não atingem o estágio dinâmico e extrai-se quais fatores e respectivas dimensões o país possui maior capacidade.

Apesar da análise não oferecer uma avaliação consolidada das capacidades, a leitura atenta permite concluir que nenhum dos fatores foi avaliado como Estágio Inicial (primeiro nível) de maturidade. A menor maturidade indicada no gráfico (próxima ao seu centro) indica o segundo nível de maturidade, Estágio Formativo, enquanto que nosso maior estágio de maturidade foi identificado no Fator de Resposta a Incidentes, classificado como Estágio Estabelecido-Estratégico, o que permite identificar no gráfico que o círculo tracejado mais próximo do perímetro corresponde ao Estágio Estratégico.

Com esse aporte da análise do estudo, exprime o gráfico que, embora não tenhamos nenhuma capacidade em nível inicial de maturidade, também não alcançamos os dois níveis mais altos de maturidade, Estágios Estratégico e Dinâmico. Ademais, é possível concluir que a maioria das capacidades brasileiras estão no Estágio Formativo e Formativo-Estabelecido, ou seja, sequer atingem no modelo o Estágio Estabelecido, que corresponderia ao terceiro nível de maturidade (OXFORD, 2020b).

Ao examinar o relatório, Malagutti sustenta que "*apesar a linguagem cuidadosamente adotada pelos autores*" o país encontra-se em "*estágio muito primário em suas capacidades cibernéticas*" (MALAGUTTI, 2022b, 2-23). O autor ainda faz uma comparação interessante das capacidades brasileiras com a revisão do modelo do Reino Unido realizada em 2015, demonstrando que mesmo com defasagem de cinco anos entre as avaliações, as capacidades do Reino Unidos eram muito superiores e, em termos de investimento, o Brasil investiu anualmente cerca de um centésimo do investimento britânico, considerando um ajuste em relação ao PIB brasileiro (2022b, 2-30).

Cabe explicitar que a metodologia do processo de avaliação das capacidades envolve coleta de dados por uma equipe de pesquisadores que realiza consultas *in loco* com atores no país e pesquisa documental, resultando em um relatório baseado em evidências que referencia a maturidade da capacidade de segurança do país; detalha conjunto pragmático de ações de contribuição para o avanço nas lacunas de capacidade identificadas; e identifica prioridades para investimento e construção de capacidades futuras, considerando as necessidades do país (OXFORD, 2021, p. 4). Não obstante, o CMM também pode ser utilizado pelo setor privado, a fim de construção de dossiês de investimento e de melhoria esperada de desempenho (OXFORD, 2021, p. 8).

No tocante à coleta de evidências, trata-se de processo multissetorial envolvendo ampla gama de fontes e organizações, salientando-se que as discussões são importantes para solucionar opiniões divergente e que o formato dessas discussões (presencial ou remota) depende do país sobre qual a revisão está focada (OXFORD, 2021, p. 4).

Quanto à revisão brasileira, envolveu mesas-redondas de consulta realizadas em 19 e 20 de março de 2018, com a participação de representantes de órgãos de persecução penal e da Justiça Criminal; da comunidade de defesa; das áreas de tecnologia da informação (TI) e de entidades do setor público; detentores de IECs; elaboradores de políticas públicas; CSIRTs/CERTs; de TI do setor privado; prestadoras de serviço de telecomunicações; setor bancário; e parceiros internacionais (OXFORD, 2020b, p. 11).

Um ano após, o GCSCC esteve novamente em Brasília para a validação dos resultados de 2018 através da utilização de metodologia semelhante, a qual contou com a participação nas entrevistas do setor acadêmico; detentores de IECs; prestadoras de serviços de telecomunicações e outras entidades do setor privado; ministérios; Poder Judiciário; mídia; comunidade de defesa; setor financeiro; CSIRTs/CERTs; sociedade civil e órgãos responsáveis pela aplicação das leis. Nessas duas visitas, o CMM serviu de base para a consulta realizada, contemplando em 2018, mesas-redondas, e entrevistas de grupo de discussão em 2019 (OXFORD, 2020b, p. 11).

Ainda sobre metodologia, o relatório reconhece que o nível de envolvimentos dos atores no processo foi mais restrito que o desejado, limitando assim a comprovação do alcance dos Indicadores em alguns pontos, embora a representação e composição dos grupos tenha sido julgada, no geral, ampla e equilibrada. Outrossim, o documento também reconheceu utilidade na atividade de validação de 2019, a qual se constituiu como primeira tentativa do GCSCC de ratificar os resultados do trabalho e verificar mudança na maturidade das capacidades, o que não se verificou *in casu*. Dessa forma, não foram detectadas grandes alterações (OXFORD, 2020b, p. 106).

Especificamente quanto ao Fator ENSC, a capacidade brasileira seria Estágio Formativo-Estabelecido (OXFORD, 2020b, p. 40), destacando a revisão a importância de uma ENSC:

> [...] é essencial para a incorporação de uma agenda de segurança cibernética a todo o governo, uma vez que ajuda a priorizar a segurança cibernética como importante área de política, determina responsabilidades e mandatos dos principais atores governamentais e não governamentais de segurança cibernética e direciona a alocação de recursos para as questões e prioridades de segurança cibernética novas e existentes (OXFORD, 2020b, p. 40).

Ao fazer a análise do Fator ENSC, a avaliação revela que os esforços de construção de uma ENSC começaram em 2010 com o Plano Brasil 2022, sendo o Livro Verde sobre Segurança Cibernética no Brasil (BRASIL, 2010) a primeira tentativa e, posteriormente, a elaboração de uma estratégia focada na APF (BRASIL, 2015a), a segunda. No entanto, no início da avaliação em 2018, o país ainda não possuía documento nacional no tema, chancelado pelo Poder Legislativo, e responsável que endereçasse a coordenação dos atores principais (OXFORD, 2020b, p. 40).

Ademais, o documento contextualiza que no início do processo de revisão, em março de 2018, foi compartilhado com o Centro o início de um processo de elaboração de uma ENSC, a partir de um grupo interministerial de mais de quinze ministérios e assistência do GSI/PR. No processo de oitiva dos atores relevantes, o texto foi circulado com noventa e oito organizações, sendo realizadas mais de duzentas reuniões e eventos até àquela análise, no intuito de amadurecer a minuta antes do encaminhamento ao Congresso Nacional. Entretanto cabe manifestar que de não foi obtida comprovação com setor privado da sua efetiva participação nesse processo (OXFORD, 2020b, p. 41).

As críticas mapeadas no processo frisaram a ausência de participação de atores relevantes no processo (organizações da sociedade civil, comunidade da Internet e setor privado detentor de IEC supostamente negligenciado pela APF). Em termos de modelos, os participantes consultados no processo de avaliação denotaram que o modelo descentralizado seria da sua preferência, com setores regulados sendo objeto de supervisão pelas suas respectivas agências reguladoras e com a criação de uma nova agência nacional. Essa seria responsável por coordenar todos esses esforços e a inspiração desse modelo viria da União Europeia, especificamente da Agência da União Europeia para a Cibersegurança (ENISA), conjugada com as particularidades do país: Estado Federativo; papel da APF; e dimensão continental.

Finalizando a avaliação, a estrutura genérica de ações foi considerada, de certa forma, positiva pelas entidades consultadas, conferindo o mandado necessário às autoridades e refletindo a dificuldade do processo legislativo, inclusive em termos da articulação política necessária e complexa atualização (OXFORD, 2020b, p. 41-42).

Já na etapa de validação realizada pela equipe em março de 2019, constatou-se o resultado daquele processo descrito anteriormente, porém diferentemente do seu objetivo. Conforme será relatado em diversos momentos da tese, o anteprojeto de lei, tornou-se o que hoje conhecemos com a PNSI, aprovada por Decreto Presidencial, o qual serviu como base para

elaboração da E-Ciber e estabeleceu o mandamento de processo inclusivo (OXFORD, 2020b, p. 42).

Nesse ponto, cumpre mencionar que esse processo inclusivo citado estaria relacionado à previsão da construção da ENSI, a qual nos termos da PNSI deve ser constituída por módulos, dentre os quais se destaca o de segurança cibernética. Esse módulo deveria ser elaborado com ampla participação dos órgãos e entidades do Poder Público e sociedade, nos termos do parágrafo único do art. 6º da PNSI (BRASIL, 2018e). Além do mais, a avaliação aponta que o setor privado teria sido consultado (OXFORD, 2020b, p. 42).

Encerrando o ciclo do processo de avaliação, o governo apresentou informações em 2020, comunicando a aprovação da E-Ciber e a competência legal ao GSI/PR para coordenar e supervisionar a atividade de SI no âmbito da APF (OXFORD, 2020b, p. 42), com espeque no art. 10, IV e V, da Lei nº 13.844, de 18 de julho de 2019, Lei que estabelece a organização básica dos órgãos da Presidência da República e dos Ministérios (BRASIL, 2019b).

Em decorrência das informações recebidas pela equipe do GCSCC durante o processo de avaliação de maturidade, o Centro desenvolveu um conjunto de recomendações para avaliação do país para cada um dos fatores de cada uma das dimensões do CMM, no intuito de aumentar a capacidade de segurança cibernética. Em relação ao Fator ENSC, as recomendações foram as que seguem:

> R 1.1 Preparar uma complementação do documento da estratégia, compatível com os objetivos nacionais e as prioridades de risco, para sugerir diretrizes aplicáveis com a métrica respectiva, para monitorar o andamento da implementação da estratégia.
> R 1.2 Assegurar que as partes interessadas envolvidas na concepção da estratégia nacional de segurança cibernética incorporem organizações do setor privado que devem fazer parte da IC (especialmente de finanças, energia, telecomunicações, transportes, o SERPRO, Empresa de Tecnologia e Informações da Previdência Social (Dataprev), PMEs, sociedade civil, setor acadêmico e parceiros internacionais.
> R 1.3 Aprimorar a colaboração com a OEA e desenvolver uma taxonomia comum para a segurança cibernética.
> R 1.4 Assegurar que as normas de segurança da informação desenvolvidas pela Administração Pública Federal sejam as normas mínimas a serem adotadas pelas autoridades públicas do Estado, e que sua implementação seja incluída nos programas nacionais de estratégia de segurança cibernética (OXFORD, 2020b, p. 53).

Nota-se que as recomendações foram deveras tímidas e não abarcam as limitações relacionadas ao mandato da entidade e à governança institucional, embora expressamente reconheçam que a competência legal do GSI/PR se limita à APF, talvez pela simples incompreensão do nosso modelo e do sistema jurídico pátrio. De qualquer maneira, as recomendações ressaltam a necessidade de acompanhamento da implementação da E-Ciber e a necessidade de engajamento dos detentores e operadores de infraestruturas críticas do setor

privado, além de mencionar a colaboração com a OEA e primar pela a observância das normas elaboradas pelo GSI/PR, cujos destinatários restringem-se aos órgãos e entidades da APF.

Após a finalização da apresentação dos três modelos traduzidos pela OCDE, UIT e GCSCC, avança-se para as conclusões parciais desse capítulo.

2.4 CONCLUSÕES PARCIAIS

O presente capítulo apresentou três modelos norteadores em matéria de desenvolvimento de capacidades de segurança cibernética. Esses modelos foram elaborados pela comunidade internacional e compreendem conteúdo, desenvolvimento e implementação de uma Estratégia de Nacional de Segurança Cibernética (ENSC).

Como se viu, os modelos tratados foram: Recomendações da Organização para a Cooperação e Desenvolvimento Econômico (OCDE), quais sejam, a Recomendação de 2015 sobre Gerenciamento de Riscos de Segurança Digital para Prosperidade Econômica e Social e as Recomendações de 2022 sobre Gerenciamento de Riscos de Segurança Digital e sobre Estratégias Nacionais de Segurança Digital; o Guia para o Desenvolvimento de uma Estratégia Nacional de Segurança Cibernética coordenado pela União Internacional de Telecomunicações (UIT); e o Modelo de Maturidade de Capacidade de Segurança Cibernética do Centro Global de Capacidade de Segurança Cibernética (GCSCC) da *Oxford Martin School* da Universidade de Oxford.

O primeiro modelo referiu-se às Recomendações OCDE. Como foi demonstrado, desde 1992 a organização está na vanguarda do desenvolvimento de diretrizes relacionadas à segurança da informação. Em 2015 aprovou a sua Recomendação sobre Gerenciamento de Riscos de Segurança Digital para Prosperidade Econômica e Social. Essa recomendação foi revisada e desmembrada, transformando-se, no final de 2022, nas Recomendações sobre Gerenciamento de Riscos de Segurança Digital e sobre Estratégias Nacionais de Segurança Digital, sem alterações de fundo.

O Brasil aderiu à recomendação de 2015 em 2018 e, em 2022, aderiu às novas recomendações, lançadas na Reunião Ministerial do Comitê de Política da Economia Digital da organização, realizada em dezembro de 2022. Embora não vinculantes, existe uma expectativa de implementação por parte dos aderentes, especialmente no curso de um processo de adesão à organização, justamente a situação em que se encontra o Brasil.

Esse modelo fornece uma abordagem principiológica que pode auxiliar na gestão dos riscos de segurança cibernética, bem como o desenvolvimento das estratégias de segurança

cibernética pelos países. Relembra-se que a organização optou pela terminologia segurança digital, com o fim de ressaltar a perspectiva social e econômica do fenômeno.

O segundo modelo introduziu o Guia para o Desenvolvimento de uma Estratégia Nacional de Segurança Cibernética, que foi desenvolvido pela UIT em cooperação com diversas organizações. Esse Guia se insere em um contexto maior de outras iniciativas da organização, como a Agenda Global de Segurança Cibernética e o Índice Global Segurança Cibernética, apresentados e contextualizados nesse Capítulo.

O Guia, que já se encontra na sua segunda edição, traz uma abordagem bastante flexível e amigável que auxilia os países na elaboração da sua estratégia, abrangendo o processo e conteúdo, trazendo uma visão compartilhada por diversos atores que colaboram na iniciativa. O Guia fornece subsídio relevante aos países para a sua estruturação, permanente reavaliação e acompanhamento das suas estratégias. Além disso, comparando-se com o primeiro modelo, o Guia é mais detalhado e fornece uma visão ampla desde o fomento das discussões para a elaboração até o seu processo de constante revisão.

O terceiro e o último modelo, também o mais complexo e detalhado, é do GCSCC. Esse modelo é composto de cinco dimensões: Estratégia e Política de Segurança Cibernética; Cultura de Segurança Cibernética e Sociedade; Construção de Conhecimento e Capacidades em Segurança Cibernética; Arcabouço Legal e Regulatório; e Padrões e Tecnologia. Essas dimensões buscam exprimir a capacidade nacional necessária para um país efetivamente endereçar os desafios relacionados à segurança cibernética.

Metodologicamente, as dimensões são decompostas em fatores e, esses, em aspectos. Por fim, cada aspecto possui uma série de indicadores que refletem o nível de maturidade. Esse último é denominado de estágio. Tal sistematização permite identificar o estágio de maturidade, os quais são cinco: início; formativo; estabelecido; estratégico; e dinâmico — o mais avançado.

Cabe relembrar que a Dimensão de Estratégia e Política de Segurança Cibernética é composta por quatro fatores: Estratégia Nacional de Segurança Cibernética; Gerenciamento de Crise e Resposta de Incidentes; Proteção de Infraestrutura Crítica; e Segurança Cibernética na Defesa e Segurança Nacional. Em função da pertinência temática à pesquisa, o Fator Estratégia e Política de Segurança Cibernética foi abordado no detalhe. Assim, apresentou-se cada um dos aspectos que o integra e os indicadores de cada um dos estágios de maturidade correspondentes.

Desde logo, é forçoso perceber que esse último modelo é o mais hermético entre os três modelos apresentados e fornece uma visão mais abrangente das capacidades de um determinado país, inclusive da perspectiva securitária. A complexidade pode ser justamente um dos motivos

que levam aos países interessados a realizar processo de revisão das capacidades conduzido pelo próprio GCSCC.

Nesse sentido, cabe trazer à baila que as capacidades brasileiras passaram pela avaliação do Centro, atendendo ao convite da Organização dos Estados Americanos, a qual apontou que no Fator Estratégia Nacional de Segurança Cibernética, o Estágio brasileiro seria Formativo – Estabelecido. É importante mencionar que a revisão brasileira já considerou, para fins de avaliação das capacidades, a aprovação da Estratégia Nacional de Segurança Cibernética (E-Ciber), ratificada em fevereiro de 2020.

Percebeu-se que os três modelos possuem abrangência e detalhamento diferenciados, porém sua consideração e utilização não é excludente. Dessa forma, partiu-se de uma abordagem essencialmente principiológica ofertada pelas recomendações da OCDE e passou-se pelo detalhamento do processo de preparação, desenvolvimento e revisão de estratégias nacionais apresentado pelo Guia coordenado pela UIT. Ao final, chegou-se ao Modelo de Maturidade de Capacidade de Segurança Cibernética, com a sua especificação dos níveis de maturidade em cada um dos aspectos que compõe fatores e refletem as dimensões do modelo.

As diferenças supracitadas não impedem a convergência das propostas ao considerar-se o recorte das ENSCs. Nessa esteira, é possível identificar uma grande congruência das iniciativas. Salienta-se que os três modelos convergem e complementam-se, considerando não somente a abrangência e detalhamento supracitados, mas também a perspectiva e o seu objetivo.

Contudo, como se procurou demonstrar, desde o primórdio da tese, é imperioso ressaltar que os modelos não podem e não devem ser utilizados como uma prescrição incondicional a ser perseguida por qualquer administração. Eles traduzem esforços e consensos de determinados grupos que podem assistir aos países na construção das suas capacidades, porém não pode ser desconsiderado o contexto particular de cada Estado e, também, precisam ser considerados os objetivos de cada instrumento e a sua utilidade. Ou seja, os modelos devem ser compreendidos como um ponto de partida do desenvolvimento de qualquer instrumento e, não, como um ponto de chegada, o objetivo final da elaboração de qualquer esforço.

Tal preocupação guarda relação com o objeto desse capítulo. Não se sustenta o processo de exportação de modelos por parte das organizações, porém se defende a importação com a devida e necessária adaptação. Assim, os três modelos podem ser utilizados por países no processo de elaboração dos seus arcabouços, considerando melhores práticas e experiências de sucesso de países que já se estruturaram. Porém, essa utilidade deve ser validada com um olhar de que a sua adoção deve atender aos interesses e as peculiaridades do país, inclusive, no caso do Brasil, da sua extensão territorial, diferenças regionais e do sistema jurídico pátrio.

Resta patente a importância do desenvolvimento de capacidades que permitam qualquer país a estruturar estrategicamente sua visão, não só pelo tamanho do desafio de promover segurança cibernética diante dos riscos que crescem cotidianamente, mas pelo papel habilitador da segurança cibernética para a transformação digital das nossas sociedades e economias.

A utilização consciente dos modelos para o desenvolvimento de políticas públicas permite aportar importantes subsídios para a sua elaboração e implementação, permitindo ao País apoiar-se em orientações existentes e torná-las significativas diante da realidade e conjuntura nacional.

Nesse sentido, reconhece-se a valia de conhecer, estudar e entender cada um desses modelos e defende-se a utilidade da sua consideração nos processos de elaboração, desenvolvimento e revisão das ENSC. No entanto reitera-se que a aplicação dos modelos deve ser conformada com a realidade e necessidade de cada país.

Finalizada a apresentação dos modelos, passa-se à descrição do arcabouço brasileiro que foi construído para o enfrentamento desses desafios.

3 DESCRIÇÃO DO ARCABOUÇO JURÍDICO E DE POLÍTICAS PÚBLICAS DE SEGURANÇA CIBERNÉTICA NO BRASIL

Conforme demonstrado nos Capítulos anteriores, existe uma preocupação crescente com segurança cibernética, a qual motivou o surgimento de diversos esforços na comunidade internacional, com o objetivo de amparar os países no desenvolvimento dos marcos necessários para o enfrentamento desses desafios. Exemplos desses esforços são justamente os três modelos apresentados no Capítulo II, os quais oferecem subsídios aos países na elaboração das suas políticas e estratégias nacionais. Como já visto no Capítulo I, dados da UIT de 2021 demonstram que cento e vinte e sete países à época possuíam estratégias nacionais na matéria ou estavam no processo de elaboração. Isso significa que quase 70% dos países do mundo está elaborando ou já possui um arcabouço na matéria (ITU, 2021b, p. 9).

Assim, no presente Capítulo, foca-se justamente em descrever como o Brasil vem se estruturando, tanto em termos de políticas, quanto em termos de organização institucional. Dessa forma, o texto permite uma compreensão do contexto do país e, com base nisso, viabiliza a almejada prescrição de política pública que será objeto do próximo Capítulo IV.

Nessa esteira, neste Capítulo apresentar-se-á o Arcabouço Nacional Jurídico e de Políticas Públicas existente, incluindo histórico do desenvolvimento dos instrumentos e marcos nessa seara. Será apresentado um panorama dos documentos de Defesa (Política Nacional de Defesa, Estratégia Nacional de Defesa e Livro Branco de Defesa) e de outros documentos que antecederam à E-Ciber, tais como a E-Digital e a PNSI.

Além disso, também serão apresentados outros instrumentos que têm importante intersecção com o tema, como a Política Nacional de Segurança de Infraestruturas Críticas, a Estratégia Nacional de Segurança de Infraestruturas Críticas, o Plano Nacional de Segurança de Infraestruturas Críticas, a Rede Federal de Gestão de Incidentes Cibernético e, até mesmo, a Lei Geral de Proteção de Dados.

Dessa maneira, o presente capítulo é subdivido em oito seções: histórico do desenvolvimento das políticas públicas; normativos de defesa; E-Digital; PNSI; E-Ciber; Rede Federal de Gestão de Incidentes Cibernéticos; legislação correlata; e conclusões parciais do capítulo, cada uma com suas respectivas subseções, quando pertinente.

3.1 HISTÓRICO DO DESENVOLVIMENTO DAS POLÍTICAS PÚBLICAS BRASILEIRAS

Antes de passar à descrição das políticas públicas vigentes, cabe trazer um breve histórico de instrumentos e outros marcos relacionados, utilizados para endereçar as questões relacionadas à segurança cibernética, bem como o processo de desenvolvimento da E-Ciber.

A Estratégia de Segurança da Informação e Comunicações e de Segurança Cibernética da Administração Pública Federal - 2015/2018, versão 1.0 (2015a) contêm uma parte específica que aborda os marcos normativos a partir de anos 2000. Nessa data, verifica-se uma emergência no Brasil e no mundo de instrumentos relacionados a princípios e diretrizes de segurança da informação, decorrentes da crescente utilização das TICs e da expansão do acesso à Internet, que não podem ser comparados com a realidade contemporânea.

Para exemplificar, a pesquisa TIC Domicílios que mapeia o acesso a essas tecnologias nos domicílios urbanos e rurais desde 2005 no Brasil, apontava na sua primeira edição que 21% dos domicílios brasileiros tinham acesso à Internet e 16,6% das famílias tinham um computador (CGI.br, 2005, p. 79 e 83). Em comparação, os últimos dados disponíveis de 2021 apontam acesso à internet para 82% dos domicílios brasileiros[1], já a percentagem de famílias com computador (de mesa, *tablet* ou notebook) cresceu para 39%[2], sendo o *smartphone* o grande responsável pela expansão do acesso à Internet[3]. Esses dados fornecem uma pequena demonstração da diferença conjuntural do início dos anos 2000 para a atualidade, no tocante à conectividade e utilização dessas tecnologias.

Voltando-se aos importantes marcos normativos, já com a ressalva de que serão citados os instrumentos estruturantes, tem-se a Política de Segurança da Informação nos órgãos e entidades da Administração Pública Federal, aprovada pelo Decreto nº 3.505, de 13 de junho de 2000, posteriormente revogada com a aprovação da PNSI que será descrita a seguir ainda nesse capítulo, e que abrangia os pressupostos básicos dessa política, conceitos, objetivos e as atribuições de órgãos e entidades da APF (BRASIL, 2000a).

Já em 2003 tem-se a Lei nº 10.683, de 28 de maio de 2003, que dispunha sobre a organização da Presidência da República e dos Ministérios, posteriormente revogada pela Lei

[1] Tabela da Pesquisa TIC Domicílios 2021 que indica a quantidade de domicílios com acesso à Internet disponível na página do CETIC.br: https://cetic.br/pt/TICS/domicilios/2021/domicilios/A4/. Acesso em: 01 nov. 2022.

[2] Tabela da Pesquisa TIC Domicílios 2021 que indica a quantidade de domicílios com computador disponível na página do CETIC.br: https://cetic.br/pt/TICS/domicilios/2021/domicilios/A1/. Acesso em: 01 nov. 2022.

[3] Tabela da Pesquisa TIC Domicílios 2021 que indica a quantidade de domicílios que possuem equipamento TIC disponível na página do CETIC.br: https://cetic.br/pt/TICS/domicilios/2021/domicilios/A/. Acesso em: 01 nov. 2022.

nº 13.502, de 1º de novembro de 2017, e atribuía ao GSI/PR a competência de coordenar as atividades de inteligência federal e de segurança da informação (BRASIL, 2003a). No mesmo ano, tem-se a criação da Câmara de Relações Exteriores e Defesa Nacional (CREDEN) do Conselho de Governo, com a aprovação do Decreto nº 4.801, de 6 de agosto de 2003[4].

A CREDEN foi instituída com o objetivo de formulação de políticas públicas e diretrizes em matérias que tangenciam questões de defesa nacional e relações internacionais e que ultrapassam as competências de um único Ministério, assim como de promoção de articulação e acompanhamento da implementação das ações (BRASIL, 2003b). Alterações posteriores, ocorridas nos anos 2008 e 2009, acrescentaram menção expressa aos assuntos relacionados à segurança de IECs, da informação e cibernética.

Em 2004 temos um marco, não normativo, importante, com a criação da Equipe de Tratamento de Incidentes em Redes Computacionais do Governo (CTIR Gov), no âmbito da estrutura do GSI/PR (BRASIL, 2015a, p. 21). Ademais, o Decreto nº 5.772, de 8 de maio de 2006, que aprova a Estrutura Regimental e o Quadro Demonstrativo dos Cargos em Comissão e das Gratificações de Exercício em Cargo de Confiança do Gabinete de Segurança Institucional da Presidência da República, e dá outras providências, criou o Departamento de Segurança da Informação e Comunicações (DSIC) no âmbito da Subchefia-Executiva, que é órgão de assistência direta e imediata ao Ministro de Estado do GSI/PR. Também foram detalhadas as competências do DSIC na seara de segurança da informação, destacando-se o planejamento e a coordenação da execução das atividades de segurança da informação e comunicações na APF (BRASIL, 2006).

Em 2008 inicia a produção normativa do GSI/PR com a aprovação da Instrução Normativa nº 1, de 13 de junho de 2008, que disciplinava a Gestão de Segurança da Informação e Comunicações no âmbito da APF, direta e indireta (BRASIL, 2008a) posteriormente revogada pela Instrução Normativa nº 1, de 27 de maio de 2020 (BRASIL, 2020d). Adicionalmente, no mesmo ano, foram aprovadas as Normas Complementares nº 1 e 2, de 13 de outubro de 2008, as quais abordavam, respectivamente, a atividade de normatização e metodologia de gestão de Segurança da Informação e Comunicações (BRASIL, 2015a, p. 23), também posteriormente revogadas pela Instrução Normativa nº 1/2020 supracitada.

Outrossim, no mesmo ano foi ratificada a Estratégia Nacional de Defesa (END) pelo Decreto nº 6.703, de 18 de dezembro de 2008, a qual define o setor cibernético como um dos

[4] A CREDEN foi criada pelo Decreto n.° 4.801, de 6 de agosto de 2003, revogado pelo Decreto n.° 9.819, de 3 de junho de 2019, texto vigente que dispõe sobre a Câmara, disponível em: http://www.planalto.gov.br/ccivil_03/_Ato2019-2022/2019/Decreto/D9819.htm#art11. Acesso em: 12 fev. 2021.

três setores estratégicos que são essenciais para a defesa nacional (BRASIL, 2008b). Já no ano seguinte em 2009, observa-se a continuidade da produção normativa do GSI e a instituição do Grupo Técnico de Segurança Cibernética (GT SEG CIBER) no âmbito da CREDEN, a partir da Portaria do GSI/PR nº 45, de 8 de setembro de 2009. O GT SEG CIBER foi criado com o intuito de proposição de diretrizes e estratégias de segurança cibernética para a APF (BRASIL, 2009).

Como fruto do trabalho do GT SEG CIBER, e que não está citado na Estratégia de 2015, em 2010 foi publicado "*Livro Verde: segurança cibernética no Brasil*", o qual busca apresentar potenciais diretrizes estratégica para a implantação de uma Política Nacional de Segurança Cibernética, expressando visões de curto (2-3 anos), médio (5-7 anos) e longo (10-15 anos) prazos, abrangendo diversas dimensões como de segurança de IECs; de educação; jurídica; de cooperação internacional; social e ambiental; de Ciência, Tecnologia e Inovação; econômica; e de político-estratégia (BRASIL, 2010, p. 17).

Interessante notar que a iniciativa apresenta um interessante *benchmarking* internacional, assim como um mapeamento do engajamento brasileiro nos fóruns internacionais (BRASIL, 2010, p. 20-24). Além disso, o trabalho, datado de 2010, também elenca uma série de tendências para 2020, como a revolução de infraestrutura; explosão de dados; mundo sempre conectado; futuro das finanças; regulamentação; internet múltiplas; e nova identidade e modelo de confiança (BRASIL, 2010, p. 29-30), as quais foram inquestionavelmente confirmadas.

Para cada uma das vertentes examinadas, são apresentados, de maneira não exaustiva, os marcos brasileiros recentes e os desafios relacionados. Considerando o recorte da pesquisa, destaca-se dentre os desafios do campo político-estratégico: o apontamento da falta de clareza sobre a importância e dimensão da segurança cibernética como tema de Estado; governança deficiente reconhecendo a multiplicidade de atores e, por vezes, até a sobreposição de atribuições; e carência de um senso comum e arcabouço conceitual de segurança cibernética (BRASIL, 2010, p. 33-34).

No tocante aos desafios econômicos, salienta-se a ausência de orçamento específico para ações relacionadas e de carreira específica de Estado (BRASIL, 2010, p. 35). Por fim, cita-se ainda os desafios da seara legal, nos quais se aponta a ausência de legislação nacional e internacional específica de segurança cibernética (BRASIL, 2010, p. 39).

Após estabelecer o panorama contemporâneo e identificar os desafios, o Livro preconiza as diretrizes que devem ser abarcadas na Política Nacional de Segurança Cibernética, a fim de endereçar as questões apontadas em cada uma dessas dimensões. Nesse sentido, na vertente político-estratégica são apontadas no curto prazo a caracterização da segurança cibernética

como alta prioridade e urgência com a implementação robusta de uma estratégia nacional; a publicação de uma Política Nacional de Segurança Cibernética; e a criação de um órgão central para coordenação dessa Política (BRASIL, 2010, p. 43).

Continuando a correlação com os desafios identificados, no campo econômico prevê a duplicação sistemática a cada dois anos dos recursos alocados para segurança cibernética a partir de 2011 (BRASIL, 2010, p. 44) e, na dimensão jurídica, a colaboração para atualização e construção do marco legal adequado, nacional e internacional (BRASIL, 2010, p. 45).

Na sua conclusão, o Livro Verde realça a tendência mundial de priorização do tema e do estabelecimento formal de um órgão central com as competências básicas, responsável por integrar esforços e promover a macrocoordenação nacional, exemplificando com as experiências da Austrália, Coreia do Sul, EUA e Reino Unido. O Livro salienta que a situação ideal seria a elaboração e publicação de uma Política Nacional de Segurança Cibernética (BRASIL, 2010, p. 49).

Retomando-se a sequência temporal, em 2012 o Tribunal de Contas da União (TCU) delibera no Acórdão nº 1.233/2012-TCU-Plenário, de 23 de maio de 2012[5], que os normativos elaborados pelo GSI/PR relativos à segurança da informação são mandatórios para os órgãos e entidades da APF, recomendando ao GSI/PR no item 9.8.2. do Acórdão que:

> [...] oriente os órgãos e entidades sob sua jurisdição que a implantação dos controles gerais de segurança da informação positivados nas normas do GSI/PR não é faculdade, mas obrigação da alta administração, e sua não implantação sem justificativa é passível da sanção [...].

Essa recomendação decorre da competência do GSI/PR para coordenar as atividades de inteligência federal e de segurança da informação prevista no art. 6, IV, da Lei nº 10.683, de 28 de maio de 2003 (BRASIL, 2003a). Destaca-se que à época da decisão encontravam-se vigentes uma Instrução Normativa e doze Normas Complementares do GSI/PR no tema[6].

Além da continuidade da produção normativa do GSI/PR, 2012 também é marcado pela promulgação de duas leis de combate à criminalidade cibernética: Lei nº 12.735, de 30 de novembro de 2012, que estabelece a estruturação especializada dos órgãos de polícia judiciária para combate aos crimes cibernéticos (BRASIL, 2012a) e Lei nº 12.737, de 30 de novembro de 2012, a qual dispõe sobre a tipificação criminal de delitos informáticos (BRASIL, 2012b). E,

---

[5] Texto do Acórdão na sua íntegra pode ser consultado em: https://pesquisa.apps.tcu.gov.br/#/documento/ acordao-completo/*/KEY%253AACORDAO-COMPLETO-1233850/DTRELEVANCIA%2520desc/0/sinonimos%253Dfalse. Acesso em: 04 nov. 2022.

[6] Os normativos podem ser consultados na página de legislação do DSI do GSI/PR disponível em: https://www.gov.br/gsi/pt-br/assuntos/dsi/legislacao. Acesso em: 04 nov. 2022.

ainda para finalizar o ano de 2012, a Portaria Normativa nº 3.389, de 21 de dezembro de 2012, do Ministério da Defesa (MD) aprova a primeira edição da Política Cibernética de Defesa, com o objetivo de guiar as atividades, em nível estratégico, de Defesa Cibernética, e, em níveis operacionais e táticos, de Guerra Cibernética (BRASIL, 2012c).

Em 2013 é instituído Grupo de Trabalho Interministerial com a finalidade de elaboração de proposta de plano estratégico focado na promoção e aperfeiçoamento das políticas públicas relacionadas à segurança e à defesa do ambiente cibernético do país (BRASIL, 2015a, p. 28) e o Decreto Legislativo nº 373, de 26 de setembro de 2013, atualiza a Política Nacional de Defesa (PND), a END e o Livro Branco de Defesa Nacional, com o reconhecimento de que a proteção do ambiente cibernético envolve múltiplas dimensões (BRASIL, 2013a).

Por fim, em novembro de 2013, e já no contexto das revelações de espionagem do *Caso Snowden*[7], foi ratificado o Decreto nº 8.135, de 4 de novembro de 2013, que dispunha sobre as comunicações de dados da administração pública federal direta, autárquica e fundacional, e sobre a dispensa de licitação nas contratações que possam comprometer a segurança nacional. O Decreto estabelecia que as comunicações de dados da APF direta, autárquica e fundacional, deveriam ser realizadas pelas redes e serviços fornecidos pela APF direta e indireta, ou seja, incluindo empresas públicas e sociedades de economia mista e suas subsidiárias (BRASIL, 2013b), sendo posteriormente revogado pela própria PNSI (BRASIL, 2018f).

Já em 2014, verifica-se nova deliberação do TCU, Acórdão nº 3.051/2014-TCU-Plenário, de 5 de novembro de 2014, que no item 9.3.1 recomenda ao GSI/PR elaborar e acompanhar planejamento contemplando a estratégia geral de segurança da informação para a sua jurisdição, ou seja, órgãos e entidades da APF. Esse planejamento deveria abranger não apenas os aspectos de tecnologia da informação, mas também a proteção das informações das instituições. Além disso, o Relatório do Acórdão na sua conclusão afirma a existência de uma lacuna para a definição de ações para a promoção de processos e práticas de segurança da informação em nível estratégico, indicando expressamente que *"[...] Ainda não há, por*

[7] Denúncias de Edward Snowden da vigilância massiva e espionagem política e econômica de alvos como a Presidente Dilma Rousseff e a Petróleo Brasileiro S/A (Petrobras) no Brasil e a Chanceler Angela Merkel, na Alemanha, através do programa da Agência Nacional de Segurança (*National Security Agency- NSA*) dos EUA. As denúncias do analista de sistema que trabalhou para a NSA e também para a Agência Central de Inteligência (*Central Intelligence Agency – CIA*) dos EUA foram tornadas públicas em 2013 e motivaram o patrocínio conjunto da Alemanha e do Brasil à Resolução da Assembleia Geral das Nações Unidas n.° 167 da 68° Sessão em 2013, intitulada "*o Direito à Privacidade na Era Digital*". O texto da Resolução pode ser consultado em: https://digitallibrary.un.org/record/764407/files/A_RES_68_167-EN.pdf. Acesso em: 28 out 2022. Para uma análise detalhada da resposta brasileira às denúncias, ver: Canabarro e Borne (2015).

exemplo, um planejamento estratégico do Estado brasileiro que reúna e coordene ações dos diversos atores responsáveis por assuntos ligados a essa área." [8].

No mesmo ano e, ainda sob forte repercussão do escândalo de espionagem cibernética revelado por *Edward Snowden,* tem-se:

a) a promulgação da Lei nº 12.965, de 23 de abril de 2014 (BRASIL, 2014a), que estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil e é conhecida como Marco Civil da Internet (MCI);

b) o Relatório Final da Comissão Parlamentar de Inquérito destinada a investigar a denúncia de existência de um sistema de espionagem, estruturado pelo governo dos EUA, com o objetivo de monitorar e-mails, ligações telefônicas, dados digitais, além de outras formas de captar informações privilegiadas ou protegidas pela Constituição Federal, conhecida como CPI da Espionagem (BRASIL, 2014b); e

c) a aprovação da Portaria Interministerial nº 141, de 2 de maio de 2014, pela qual os Ministros de Estado do Planejamento, Orçamento e Gestão, das Comunicações e da Defesa regulamentam o Decreto nº 8.135, de 4 de novembro de 2013.

Deve-se atentar que essa Portaria Interministerial, ao regulamentar o Decreto nº 8.135, de 4 de novembro de 2013, determinou expressamente no seu art. 5º, § 1º, que na contratação pela APF de órgãos ou entidades da APF, incluindo empresas públicas e sociedades de economia mista da União e suas subsidiárias, para a prestação de serviços de redes de telecomunicações e de tecnologia de informação, deveriam ser observados os normativos do GSI/PR em matéria de segurança da informação (BRASIL, 2014c).

Cabe destaque às conclusões do Relatório Final da CPI da Espionagem no tocante à segurança das comunicações, sempre considerando a delimitação do presente trabalho, que sustenta a necessidade de elaboração de uma ENSC e de centralização institucional da segurança cibernética na estrutura do governo brasileiro, defendendo a discussão sobre a possibilidade de criação de uma agência no âmbito da APF para segurança cibernética.

Alternativamente, admite o aproveitamento de estrutura existente, conferindo-se ao órgão a capacidade para atuar na totalidade do tema em coordenação com as agências reguladoras setoriais, ressaltando que o mandato desse órgão centrar-se-ia na organização do setor cibernético brasileiro, excluindo-se as questões relacionadas à defesa e à guerra cibernéticas (BRASIL, 2014b, p. 141-149).

---

[8] Item 375 do Relatório do Acórdão. Texto na sua íntegra pode ser consultado em: https://pesquisa.apps.tcu.gov.br/#/documento/acordao-completo/3051%252F2014/%2520/DTRELEVANCIA%2520desc%252C%2520NUMACORDAOINT%2520desc/0/%2520. Acesso em: 05 nov. 2022.

Justamente no universo de segurança e defesa nacional, verifica-se também marcos importantes em 2014, com a criação do Comando de Defesa Cibernética (ComDCiber) e a Escola Nacional de Defesa Cibernética (EnaDCiber), pela aprovação da Portaria Normativa do Ministério da Defesa nº 2.777, de 27 de outubro de 2014 (BRASIL, 2014d). Complementando esses marcos, cabe ainda relacionar a publicação da Doutrina Militar de Defesa Cibernética, aprovada pela Portaria Normativa do Ministério da Defesa nº 3.010, de 18 de novembro de 2014 (BRASIL, 2014e).

Chegando ao ano de 2015, tem-se a publicação da Estratégia de Segurança da Informação e Comunicações e de Segurança Cibernética da Administração Pública Federal - 2015/2018, versão 1.0 (2015a), a qual não atende a recomendação supracitada do GT SEG CIBER consubstanciada no Livro Verde (BRASIL, 2010), nem à recomendação do Relatório Final da CPI da Espionagem (BRASIL 2014b). Sua insuficiência decorre da abrangência dessa Estratégia, que é limitada à APF, não abarcando, dessa forma, o setor brasileiro cibernético, utilizando-se aqui a terminologia adotada pelo relatório anteriormente mencionado.

Dentre os objetivos estratégicos da Estratégia 2015/2018 cita-se a institucionalização do tema no planejamento e no orçamento federal, com a inclusão de programa no Plano Plurianual (PPA) e a operacionalização pelos órgãos e entidades da APF das ações temáticas na Lei Orçamentária Anual (LOA); o contínuo aprimoramento do quadro de pessoal na matéria; e a instituição de modelo de governança sistêmica, com coordenação executiva, acompanhamento e avaliação do órgão central, ou seja, do GSI/PR (BRASIL, 2015a, p. 43-47).

Em termos de metas estratégicas relacionadas aos objetivos supracitados e, considerando o recorte da tese, cita-se que a Estratégia 2015/2018 apresentava para 2015 as metas M-III de articulação e estabelecimento de programa no PPA 2016-2019; M-IV de articulação e formalização de função orçamentária específica na Segurança Institucional abarcando segurança da informação e segurança cibernética; e M-V de criação de Câmara Multissetorial temática da APF no âmbito do sistema.

Já para 2016 a Estratégia estabelecera as seguintes ações: M-IX que previa o estabelecimento do Modelo de Governança Sistêmico de nível político estratégico para a APF; M-XIV que pregava a articulação e inserção do tema no Programa Nacional de Gestão Pública e Desburocratização; e M-XVII que estipulava a criação de Comissão para estudo de viabilidade de criação de carreira de Estado de Segurança da Informação e Segurança Cibernética, incluindo estrutura organizacional em nível estratégico no Governo Federal (BRASIL, 2015a, p. 55-57).

Para 2017 não foi prevista nenhuma meta relacionada à governança de segurança cibernética, nem ao modelo institucional e, para 2018, as metas M-XXX tratava da revisão da estratégia para o período de 2019-2022; e a M-XXXI fala do encaminhamento do resultado do estudo de viabilidade de criação da carreira específica. Também foram previstas metas contínuas difusas relacionadas a atividades de capacitação; conscientização; parcerias; e análise e revisão da Estratégia. Todas as metas contêm a identificação do órgão e/ou entidade responsáveis, com a indicação do GSI/PR como responsável pela sua quase totalidade, com assessoramento do Comitê Gestor de Segurança da Informação (CGSI), na sua maioria, e colaboração de outros atores da APF (BRASIL, 2015a, p. 57-60).

A instabilidade política vivenciada pelo país culminando no Impeachment da Presidenta Dilma Rousseff em agosto de 2016 teve profundo impacto nas atividades, o que se confirma com a ausência de marcos e baixa implementação da Estratégia 2015/2018. Como exemplo, evidencia-se que no período de 2015-2017 não há produção normativa (instrução normativa ou normas complementares) pelo GSI/PR.

Ademais, cabe relembrar que o GSI/PR foi extinto como secretaria com *status* de Ministério, passando a integrar a Secretaria de Governo em outubro de 2015. Essa, também com *status* de Ministério, foi resultado da fusão da Secretaria-Geral da Presidência da República, da Secretaria de Relações Institucionais da Presidência da República, da Secretaria da Micro e Pequena Empresa da Presidência da República e do GSI/PR[9]. Já em 2016, no Governo de Michel Temer, o GSI/PR é novamente recriado pela Medida Provisória nº 726, de 12 de maio de 2016, convertida com alterações na Lei nº 13.341, de 29 de setembro de 2016 (BRASIL, 2016c).

Desse período também se recorda que, antes de deixar o governo, a Presidenta Dilma Rousseff ratificou o Decreto nº 8.771, de 11 de maio de 2016, que regulamenta a Lei conhecida como Marco Civil da Internet e traz disposições relacionadas a questões operacionais importantes da Internet como a possibilidade de discriminação ou a degradação para gestão de tráfego, a fim de manter estabilidade, segurança, funcionalidade e integridade da rede. Além disso, o mesmo Decreto estabelece o procedimento para guarda e proteção de registros de conexão e de acesso a aplicações, bem como de requisição por autoridades administrativas de

[9] Medida Provisória n.º 696, de 2 de outubro de 2015, convertida com alterações na Lei n.º 13.266, de 5 de abril de 2016, que extingue e transforma cargos públicos; altera a Lei n.º 10.683, de 28 de maio de 2003, que dispõe sobre a organização da Presidência da República e dos Ministérios, e a Lei n.º 11.457, de 16 de março de 2007; e revoga dispositivos da Lei n.º 10.683, de 28 de maio de 2003. Diário Oficial da União, seção 1, Brasília, DF, 6 abr 2016b. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2016/Lei/L13266.htm. Acesso em: 16 nov. 2022.

dados cadastrais (BRASIL, 2016a). Essas informações são imprescindíveis à persecução penal dos crimes cibernéticos.

Em 2017 o GSI/PR aprova seu Regimento Interno, apontando o Departamento de Segurança da Informação e Comunicações (DSIC) como órgão da Secretaria de Coordenação de Sistemas, um órgão específico singular nos termos do Regimento, sendo composto por três coordenações: Coordenação-Geral do Núcleo de Segurança e Credenciamento (CGNSC); Coordenação-Geral do Centro de Tratamento de Incidentes de Rede do Governo - (CGCTIR); Coordenação-Geral de Gestão de Segurança da Informação e Comunicações - (CGSIC); e Divisão de Apoio (BRASIL, 2017).

Na sequência em 2018, tem-se a primeira edição da simulação nacional de segurança cibernética, denominada Exercício Guardião Cibernético - EGC (LIMA E SILVA, 2020) e a aprovação dos seguintes instrumentos: E-Digital; Lei Geral de Proteção de Dados; PNSI; e Política Nacional de Segurança de Infraestruturas Críticas (PNSIC). Adicionalmente, foi procedida a atualização dos normativos de defesa, que serão brevemente apresentados nas seções subsequentes.

Continuando esse percurso, não se pode olvidar que em 2019 o Decreto nº 9.668, de 2 de janeiro de 2019, aprova a nova estrutura regimental do GSI/PR, mantendo a estrutura organizacional de 2017 e alterando o nome do DSIC para Departamento de Segurança da Informação - DSI (BRASIL, 2019a). Posteriormente em 2020, o Decreto nº 10.363, de 21 de maio de 2020, cria a Assessoria Especial de Segurança da Informação, como órgão de assistência direta e imediata ao Ministro de Estado Chefe do Gabinete de Segurança Institucional da Presidência da República e eleva o DSI à condição de órgão específico e singular (BRASIL, 2020c), estrutura institucional que se manteve até 31 de dezembro de 2022.

Ainda em 2020, menciona-se a aprovação da E-Ciber e a Estratégia Nacional de Segurança de Infraestruturas Críticas (ENSIC), as quais serão abordadas na sequência. Por fim, tem-se a criação de Rede Federal de Gestão de Incidentes Cibernéticos (ReGIC) em 2021; o Plano Nacional de Segurança da Infraestruturas Críticas (PLANSIC) em 2022; e o trabalho de atualização dos normativos do GSI/PR[10], chegando-se à atualidade.

Cumpre um último destaque nesse panorama histórico. Contemporânea à finalização da redação da tese é a nova estrutura regimental do GSI/PR, aprovada pelo Decreto nº 11.331, de 1º de janeiro de 2023. Nessa, a Assessoria Especial de Segurança da Informação foi extinta e

[10] A lista completa dos normativos vigentes e a íntegra dos instrumentos podem ser consultadas na página oficial do DSI do GSI/PR, disponível em: https://www.gov.br/gsi/pt-br/assuntos/dsi/legislacao. Acesso em: 08 jan. 2023.

foi criada a Secretaria de Segurança da Informação e Cibernética, órgão específico e singular, composto pelo Departamento de Segurança da Informação e Cibernética (DSIC). O DSIC mantém a estrutura de três coordenações para endereçar núcleo de segurança e credenciamento; prevenção, tratamento e resposta a incidentes cibernéticos do governo; e segurança da informação, acrescido de divisão de apoio (BRASIL, 2023b). Extrai-se dessa mudança uma elevação do *status* do tema no âmbito do GSI, que agora conta com uma secretaria específica para o assunto.

Finalizada essa visão geral, passa-se a abordar brevemente alguns dos mais importantes e recentes normativos, iniciando-se com os documentos norteadores da defesa nacional.

3.2 NORMATIVOS DE DEFESA

Passado o amplo panorama do desenvolvimento das políticas públicas e outros marcos associados, essa subseção destina-se à análise dos normativos relacionados à defesa. A Lei Complementar nº 97, de 9 de junho de 1999, que dispõe sobre as normas gerais para a organização, o preparo e o emprego das Forças Armadas, com alterações da Lei Complementar nº 136, de 25 de agosto de 2010, determinou no art. 9°, § 3° que o Poder Executivo deve encaminhar ao Congresso Nacional, a cada quatro anos, na primeira metade da sessão legislativa ordinária três instrumentos: PND; END; e Livro Branco de Defesa Nacional. Esse último, caracteriza-se como documento público que possibilita acesso ao amplo contexto da END, apresentando perspectiva de médio e longo prazos e contendo dados estratégicos, orçamentários, institucionais e materiais detalhados sobre as Forças Armadas, nos termos do art. 9°, §§1° e 2°, cabendo ao Ministro de Estado da Defesa a implantação do Livro (BRASIL, 1999).

Consoante os incisos do §2° do art. 9°, o Livro Branco deve abordar oito tópicos: cenário estratégico para o século XXI; PND; END; modernização das Forças Armadas; racionalização e adaptação das estruturas de defesa; suporte econômico da defesa nacional; Forças Armadas; e operações de paz e ajuda humanitária (BRASIL, 1999).

Os documentos atualmente vigentes foram aprovados pelo Congresso Nacional, Decreto Legislativo nº 179, de 14 de dezembro de 2018 (BRASIL, 2018e), tendo sido enviada ao Congresso Nacional em julho de 2020 a proposta de atualização dos documentos (BRASIL, 2020e)[11].

[11] Proposta enviada ao Congresso Nacional pela Mensagem (CN) n.° 9, de 2020 (BRASIL, 2020e). No Congresso tramita como Projeto de Decreto Legislativo nº 1.127, de 2021. O Projeto foi aprovado pelo Senado Federal, em

Desde logo cabe mencionar que é possível verificar o esforço nessa seara ao ser apontado o setor cibernético como prioridade para a defesa do país nos normativos, inclusive motivando o aporte de recursos financeiros consideráveis (AYRES PINTO, GRASSI, 2020, p. 125). Não obstante, o tamanho do desafio impõe considerar que as previsões ainda são tímidas, como será visto a seguir, passando-se à análise de cada um desses documentos que integram essa seção destinada às políticas de defesa, subdividida nas subseções de PND, END e Livro Branco de Defesa.

3.2.1 Política Nacional de Defesa

A parte introdutória da PND, aprovada pelo Decreto Legislativo nº 179, de 14 de dezembro de 2018, ressalta que o instrumento apresenta o posicionamento do país no tocante à sua defesa, estabelecendo os Objetivos Nacionais de Defesa (OND), constituindo-se como documento de mais alto nível em questões de defesa, baseado nos princípios e objetivos constitucionais[12]. Nesse sentido, a PND expressa os objetivos para assegurar a Defesa Nacional e atua para contribuir com a percepção de um estado de Segurança Nacional, salientando a indissociabilidade entre defesa e desenvolvimento (BRASIL, 2018d, p. 190).

Nesse ponto, aproveita-se para apresentar as definições das terminologias "Defesa Nacional" e "Segurança Nacional", constantes do Glossário das Forças Armadas. A primeira é caracterizada como "*conjunto de atitudes, medidas e ações do Estado, com ênfase na expressão militar, para a defesa do território, da soberania e dos interesses nacionais contra ameaças preponderantemente externas, potenciais ou manifestas"* (BRASIL, 2015b, p, 85). Já a última, como *"condição que permite a preservação da soberania e da integridade territorial, a realização dos interesses nacionais, livre de pressões e ameaças de qualquer natureza, e a*

2 de junho de 2022, e remetido à Câmara dos Deputados dia 8 de junho de 2022, onde permanece em tramitação até a presente data. O histórico de tramitação do projeto pode ser consultado em: https://www.congressonacional.leg.br/materias/materias-bicamerais/-/ver/pdl-1127-2021. Acesso em: 08 jan. 2023.

[12] Os objetivos fundamentais e os princípios que regem as relações internacionais da República Federativa do Brasil estão expressos nos arts. 3º e 4º da Constituição Federal, que assim dispõem: "*Art. 3º Constituem objetivos fundamentais da República Federativa do Brasil: I - construir uma sociedade livre, justa e solidária; II - garantir o desenvolvimento nacional; III - erradicar a pobreza e a marginalização e reduzir as desigualdades sociais e regionais; IV - promover o bem de todos, sem preconceitos de origem, raça, sexo, cor, idade e quaisquer outras formas de discriminação. Art. 4º A República Federativa do Brasil rege-se nas suas relações internacionais pelos seguintes princípios: I - independência nacional; II - prevalência dos direitos humanos; III - autodeterminação dos povos; IV - não-intervenção; V - igualdade entre os Estados; VI - defesa da paz; VII - solução pacífica dos conflitos; VIII - repúdio ao terrorismo e ao racismo; IX - cooperação entre os povos para o progresso da humanidade; e X - concessão de asilo político. Parágrafo único. A República Federativa do Brasil buscará a integração econômica, política, social e cultural dos povos da América Latina, visando à formação de uma comunidade latino-americana de nações*." (BRASIL, 1988).

garantia aos cidadãos do exercício dos direitos e deveres constitucionais" (BRASIL, 2015b, p. 250).

No tocante especificamente ao espaço cibernético, a PND aponta a necessidade de especial atenção à segurança e à defesa desse ambiente, alertando para a carência de maiores investimentos em Ciência, Tecnologia e Inovação; e para a não eliminação da dependência externa em áreas fundamentais para a Indústria. Ademais, identifica o acesso não autorizado aos sistemas de informação e comunicações como ameaça crescente, inclusive com eventual interrupção de fluxos de informações de interesse nacional, podendo expor ou paralisar atividades vitais para o funcionamento das instituições do País (BRASIL, 2018e, p. 194-195).

Na Concepção Política de Defesa, o instrumento elenca três pilares: desenvolvimento, diplomacia e defesa, sustentando a autonomia tecnológica do País, posicionamento que é replicado no OND VII, referente à promoção da autonomia produtiva e tecnológica na área de defesa (BRASIL, 2018e, p. 197).

Da leitura da PND e dos trechos supramencionados, extrai-se que o instrumento de mais alto nível relacionado à defesa nacional enfrenta timidamente as ameaças cibernéticas e os desafios relacionados, com destaque à menção genérica sobre a necessidade de defesa e segurança cibernéticas e de redução da dependência tecnológica, com priorização da Ciência, Tecnologia e Inovação.

Embora o texto atualmente vigente date de 2016 (enviado ao Congresso Nacional para apreciação em 2016 e aprovado em 2018), à época da sua elaboração, segurança cibernética, inclusive sob a ótica de defesa cibernética e guerra cibernética, já se colocava como um dos tópicos mais relevantes e urgentes de Segurança Internacional. Soma-se também como elemento significativo que justificaria endereçamento mais assertivo, o contexto da realização dos grandes eventos internacionais, como a Copa FIFA 2014 e os Jogos Olímpicos no Rio de Janeiro no mesmo ano; e do escândalo de espionagem cibernética revelado por Edward Snowden, previamente mencionando.

Em julho de 2020 o Presidente da República encaminhou as propostas de PND, Estratégia Nacional de Defesa e Livro Branco para a apreciação do Congresso Nacional. Em relação à PND, a proposta reitera a necessidade de especial atenção "a *segurança e a defesa do espaço cibernético brasileiro, essenciais para garantir o funcionamento dos sistemas de informações, de gerenciamento e de comunicações de interesse nacional*".

De mais a mais, o documento expande suas considerações nessa temática, visto que além de abordar eventuais bloqueios de fluxo de informações e seus reflexos para as ações de Comando, Controle e Inteligência, adverte que o contexto internacional traz a tendência de

aumento das desigualdades tecnológicas, inclusive com consequências para o equilíbrio de poder regional e mundial. Essa menção capta as disputas geopolíticas que vêm sendo acirradas nos últimos anos e que foram brevemente citadas no Capítulo I do presente trabalho. No mesmo sentido, a proposta insiste que a falta de investimento em inovação e tecnologia (destacando-se as tecnologias disruptivas) implicará na continuidade do papel secundário de países no cenário mundial, não logrando desenvolvimento, nem aumento do bem-estar da população (BRASIL, 2020e, p. 16).

Dessa forma, ainda que a proposta aborde a temática da segurança cibernética de forma sucinta, demonstra aumento da preocupação com o desenvolvimento tecnológico nacional, especialmente associado às tecnologias disruptivas (como os sistemas de comunicações móveis de quinta geração - 5G, por exemplo), e os seus reflexos no Poder Nacional[13], assim como para defesa e segurança nacionais, avançando-se na sequência para a análise da END.

3.2.2 Estratégia Nacional de Defesa

Enquanto a PND coloca-se como o documento de mais alto nível, exprimindo-se através dos OND, a END orienta o Estado nas ações de implementação dos OND. A END vigente foi aprovada conjuntamente com a PND, pelo Decreto Legislativo nº 179, de 14 de dezembro de 2018, sustentando prevalência da ação diplomática como concepção estratégica de defesa no Brasil (BRASIL, 2018e, p. 202-203).

A END reconhece o setor cibernético como um dos setores tecnológicos essenciais para a Defesa Nacional, e, portanto, estratégico, o qual transcende à divisão entre civil e militar, em face da sua própria natureza. A Estratégia atribui ao Exército a responsabilidade pela liderança centralizada, coordenação e integração de vários atores e áreas do conhecimento (BRASIL, 2018e, p. 217).

A END destaca a capacitação de amplo espectro de emprego dual; a interoperabilidade e integração das tecnologias de comunicações das Forças Armadas; o aprimoramento da segurança da informação e das comunicações e segurança cibernética, não somente nas Forças Armadas, mas em todo o Estado, protegendo-se as estruturas críticas; fomento à pesquisa, ao desenvolvimento e à inovação nessa seara, com envolvimento da academia; e fortalecimento da colaboração entre Setor de Defesa, academia, setores público e privado e Base Industrial de

[13] Poder Nacional é definido como a "*capacidade que tem a Nação para alcançar e manter os Objetivos Nacionais, em conformidade com a Vontade Nacional. Manifesta-se em cinco expressões: a política, a econômica, a psicossocial, a militar e a científico-tecnológica*" (BRASIL, 2015b, p. 212).

Defesa (BID), além das parcerias estratégicas e intercâmbio com Forças Armadas de outros países (BRASIL, 2018e, p. 218).

Com relação às Estratégias de Defesa (ED) e às Ações Estratégicas de Defesa (AED) elencadas na END, as quais são vinculadas aos OND apresentados na PND, destaca-se aqui no texto àquelas diretamente relacionadas à segurança cibernética. Nesse sentido, o OND-1 relacionado à garantia de soberania, patrimônio nacional e integridade territorial traz como ED-1 o fortalecimento do Poder Nacional, estabelecendo como AED: AED-1 o desenvolvimento dos setores estratégicos (nuclear, cibernético e espacial); e AEC-2 o incremento da segurança das estruturas estratégicas. O mesmo OND-1 também contempla como ED-2 o fortalecimento da capacidade de dissuasão, definindo como AED: AED-9 o desenvolvimento da capacidade de monitoramento do espaço cibernético; e AED-10 o aumento da capacidade da sua defesa e exploração desse espaço (BRASIL, 2018e, p. 219)

Já o OND-7, relacionado à promoção da autonomia produtiva e tecnológica na área de defesa, apresenta como ED-16 o fortalecimento da área de ciência e tecnologia de defesa, com a respectiva AED-69 de promoção do desenvolvimento tecnológico cibernético (BRASIL, 2018e, p. 227).

A proposta de END mantém as proposições vigentes, limitando-se a incluir a necessidade de conclusão do Sistema Militar de Defesa Cibernética, tanto em termos de estrutura, quanto em termos de marco legal, nos seus fundamentos (BRASIL, 2020e, p. 31). Após a breve síntese da END, na sequência apresenta-se o Livro Branco de Defesa.

3.2.3 Livro Branco de Defesa

Além dos mencionados apontamentos incluídos no PND e na END, tanto no contexto, quanto nos objetivos, estratégias e ações estratégicas, o Livro Branco, também aprovado pelo Decreto Legislativo nº 179, de 14 de dezembro de 2018, ao descrever o Setor Cibernético, aponta para a sua complexidade. Nesse aspecto, ressalta que a proteção do espaço cibernético abarca diversas áreas, abrangendo a proteção dos seus ativos e a capacidade de atuação em rede, sendo essencialmente multidisciplinar. O objetivo da implantação do Setor Cibernético é conferir confidencialidade, disponibilidade, integridade e autenticidade aos dados que trafegam nas redes, representando um esforço de longo prazo, com reflexos positivos em outras áreas, como operacional e ciência e tecnologia (BRASIL, 2018e, p. 55).

O Livro Branco de 2016 relatou avanços em termos de institucionais, de pessoal e de soluções, alavancados pelo Exército Brasileiro, com a ativação do Comando de Defesa

Cibernética (ComDCiber) em abril de 2016, tratando-se de organização militar conjunta na estrutura organizacional do Exército, com a função de concentrar as atividades de planejamento, orientação e supervisão das atividades nessa seara. Como órgãos subordinados, tem-se o Centro de Defesa Cibernética (CDCiber), responsável pelas atividades operacional e de inteligência, e a ENaDCIBER, responsável pela capacitação e conscientização, todos integrados por militares das três Forças (BRASIL, 2018e, p. 55).

Embora não seja objeto de estudo da pesquisa, cabe apontar a existência de críticas quanto à estruturação do ComDCiber, que adicionam complexidade ao desenvolvimento das capacidades brasileiras em matéria de defesa. Nesse sentido, Malagutti alega que se constitui uma "*jabuticaba*", visto que se trata de um comando conjunto, com órgão subordinado operacional, vinculado a uma única força. Ao contrário, o autor defende que se esperaria ligação direta com o Estado-Maior Conjunto das Forças Armadas ou com o próprio Ministério da Defesa. Ademais, o ComDCiber está subordinado a órgão que se refere à pesquisa e ao desenvolvimento de tecnologia, qual seja o Departamento de Ciência e Tecnologia. O autor ainda relaciona a hierarquia relativamente baixa do órgão dentro do organograma do Exército, impactando nos recursos recebidos; e dificuldades relacionadas à carreira de militares no Comando (MALAGUTTI, 2022b).

A proposta de Livro Branco enviada ao Congresso Nacional para apreciação em 2020, no tocante à segurança cibernética, preserva o conteúdo aprovado em 2018 (BRASIL, 2020e).

Essa tríade documental de defesa apresenta os objetivos para a garantia da defesa nacional, as ações para a implementação desses objetivos e contextualização desses documentos, traduzidos, respectivamente na PND, END e Livro Branco. Após a breve síntese dessa trilogia focada nas questões de segurança cibernética, passa-se à análise dos demais instrumentos brasileiros pertinentes, continuando-se com a seção destinada a tratar da E-Digital.

3.3 ESTRATÉGIA BRASILEIRA PARA TRANSFORMAÇÃO DIGITAL

A E-Digital (BRASIL, 2018b), regulamentada em Ato do Ministro de Estado de Ciência, Tecnologia, Inovações e Comunicações (MCTIC), em atendimento ao § 3.º do art. 1.º do Decreto nº 9.319, de 21 de março de 2018 (BRASIL, 2018a), apresenta um amplo diagnóstico dos desafios provocados pela transformação digital, oferecendo uma visão de futuro e as ações estratégicas que devem ser adotadas a fim de concretizar essa visão, também estabelecendo indicadores para avaliação da efetividade dessas ações. Sua elaboração foi

motivada por determinação da Presidência da República e coordenada pelo MCTIC, no sentido de elaboração de estratégia de longo prazo para a Economia Digital (BRASIL, 2018b, p. 5).

A E-Digital foi desenvolvida no seio de Grupo de Trabalho Interministerial, contando com a participação de dezenas de órgãos e entidades da APF, assim como com a participação multissetorial por meio de eventos organizados para sua formulação e da Consulta Pública da sua minuta inicial de texto (BRASIL, 2018b, p. 11-12).

Partindo de um diagnóstico que reconhece a necessidade de coordenação e convergência das ações governamentais direcionadas à transformação digital, a qual demanda, inclusive ambiente normativo e regulatório adequado, o documento elenca as seguintes áreas como arcabouço conceitual: infraestrutura; pesquisa, desenvolvimento e inovação; confiança; educação; e dimensão internacional, as quais são analisadas sob a perspectiva de transformação da sociedade e transformação da economia, sem olvidar a complexidade e transversalidade dos temas (BRASIL, 2018b, p. 8).

Com base nesse arcabouço conceitual, foram estabelecidos eixos habilitadores e eixos de transformação digital. Os primeiros objetivam a criação de um ambiente que possa fomentar a transformação digital da economia do país, dividindo-se em cinco: infraestrutura e acesso às TICs; pesquisa, desenvolvimento e inovação; confiança e ambiente digital; educação e capacitação profissional; e dimensão internacional. Já os eixos de transformação digital englobam quatro temáticas: economia baseada em dados; mundo de dispositivos conectados; novos modelos de negócio; e cidadania e governo (BRASIL, 2018b, p. 9).

Para fins do presente trabalho, concentrar-se-á no eixo habilitador "Confiança no Ambiente Digital", o qual preconiza "*transformar a Internet em um ambiente seguro, confiável, propício aos serviços e ao consumo, com respeito aos direitos dos cidadãos*". Esse eixo subdivide-se em duas grandes categorias: proteção de direitos e privacidade; e defesa e segurança no ambiente digital (BRASIL, 2018b, p. 37).

No tocante à primeira categoria, a garantia de direitos no espaço cibernético é a pedra-de-toque para a confiança no ambiente digital, visto que riscos não mitigados podem atrasar a transformação digital da economia. A E-Digital reconhece os avanços legislativos com aprovação do MCI, embora aponte outros temas que ainda demandam ações normativas, como proteção de dados, direitos do consumidor no comércio eletrônico, crimes cibernéticos, etc., bem como temas novos, como a transparência de algoritmos e Inteligência Artificial. (BRASIL, 2018b, p. 39).

A visão expressa no documento ressalta a necessidade de cooperação entre os setores público e privado para a efetividade da proteção dos direitos no ciberespaço, destacando a

garantia da privacidade; o estímulo à adoção de conceitos como "*privacy by design and default*" e "*security by design and default";* aperfeiçoamento dos mecanismos de proteção ao consumidor no ambiente digital, assim como enfoque especial à proteção de crianças e adolescentes (BRASIL, 2018b, p. 40).

No tocante às ações estratégicas, a E-Digital prescreve sete: aprovação de lei específica de proteção de dados; criação ou designação de uma autoridade nacional de proteção de dados; estímulo a mecanismos de cooperação e parceria entre setores público e privado para assegurar princípios já garantidos no nosso ordenamento, como os previstos no MCI e na Constituição Federal; reforço dos instrumentos de cooperação internacional entre autoridades e provedores (acesso e conteúdo) com o objetivo de garantir a aplicação da lei; disseminação do uso de tecnologia para validação de transações e documentos produzidos no ambiente digital, como a certificação digital; estímulo da adoção dos padrões de "*privacy by design and default*" e "*security by design and default";* e compreensão e adaptação dos marcos consumeristas para o ambiente digital (BRASIL, 2018b, p. 40-41).

Cabe relatar os avanços relacionados às ações estratégicas ocorridos desde a aprovação da E-Digital em 2018, especialmente com a aprovação da Lei Geral de Proteção de Dados Pessoais (LGPD), Lei nº 13.709, de 14 de agosto de 2018 (BRASIL, 2018c); com a criação da Autoridade Nacional de Proteção de Dados (ANPD), nomeação de seus diretores e publicação da estrutura regimental da Agência[14]; com a incorporação do princípio de *privacy by design* em alguns instrumentos normativos, como na E-Ciber[15] e na regulamentação setorial da Anatel[16]; e com a promoção do uso de Assinatura Digital nas contas do Portal gov.br que unifica os canais digitais do governo federal, em atendimento ao Decreto nº 10.543, de 13 de novembro de 2020[17].

Voltando-se para à segunda categoria, referente à defesa e segurança no ambiente digital, o diagnóstico aponta a expansão do acesso à Internet e, como consequência, aumento dos riscos associados, elencando os diversos progressos em matéria de defesa ocorridos no

[14] Decreto n.º 10.474, de 26 de agosto de 2020, que aprova a Estrutura Regimental e o Quadro Demonstrativo dos Cargos em Comissão e das Funções de Confiança da Autoridade Nacional de Proteção de Dados e remaneja e transforma cargos em comissão e funções de confiança. Disponível em: https://www.in.gov.br/web/dou/-/decreto-n-10.474-de-26-de-agosto-de-2020-274389226. Acesso em: 15 jan. 2021.

[15] Ação Estratégia 2.3.1. que trata do fortalecimento das ações de governança cibernética da Estratégia Nacional de Segurança Cibernética (BRASIL, 2020a).

[16] Art. 5, VIII, do Regulamento de Segurança Cibernética aplicada ao Setor de Telecomunicações, aprovado pela Resolução n.º 740, de 21 de dezembro de 2020. Disponível em: https://www.anatel.gov.br/legislacao/resolucoes/2020/1497-resolucao-740. Acesso em: 14 jan. 2021.

[17] Decreto n.º 10.543, de 13 de novembro de 2020, que dispõe sobre o uso de assinaturas eletrônicas na administração pública federal e regulamenta o art. 5º da Lei nº 14.063, de 23 de setembro de 2020, quanto ao nível mínimo exigido para a assinatura eletrônica em interações com o ente público. Disponível em: http://www.planalto.gov.br/ccivil_03/_Ato2019-2022/2020/Decreto/D10543.htm. Acesso em: 14 jan. 2021.

passado recente da edição da E-Digital, como a criação do CDCiber e do ComDCiber e priorização no tema na END, nos termos já abordados no início deste capítulo. Ademais, relata o papel das vulnerabilidades nas condutas ilícitas e os prejuízos causados pelos crimes cibernéticos à economia, ainda que não existam estatísticas confiáveis e o Brasil seja apontado como um dos maiores alvos e origem das ameaças (BRASIL, 2018b, p. 41).

O documento traz a classificação do Brasil no GCI, o qual foi apresentado em detalhe na subseção 2.2 no Capítulo II, e que à época da elaboração da E-Digital, colocava o Brasil como país de maturidade intermediária. Nesse sentindo, a E-Digital identifica que a análise dos componentes do índice demonstra a existência de grandes desafios para país, destacando a necessidade de aprimoramento da estrutura normativa e institucional (BRASIL, 2018b, p. 41-42).

Cabe chamar atenção para a menção específica da elaboração da Política Nacional de Segurança da Informação (PNSI), a qual está destacadamente citada na E-Digital. A Estratégia explicita a formulação de projeto de lei, a qual estaria sendo liderada pelo GSI/PR para apresentação ao Congresso Nacional. Esse projeto enfocaria segurança cibernética como um dos aspectos de gestão de segurança da informação e apostaria na coordenação dos entes da Federação, bem como no engajamento do setor privado. No entanto, conforme será explanado no item a seguir, o projeto de lei transformou-se em Decreto Presidencial[18], inexistindo até o presente, lei para endereçar a problemática da segurança cibernética (BRASIL, 2018b, p. 42).

A visão estabelecida ratifica a necessidade de se encarar o tema como prioridade nacional, defendendo a ampla revisão e integração das leis endereçadas à persecução penal dos crimes cibernéticos; e o investimento em formação de recursos humanos e na capacidade de pesquisa, desenvolvimento e inovação, objetivando a aplicação dual e autonomia tecnológica brasileira. Nesse último ponto caberia ao Estado a alavancagem como o seu poder de compra (BRASIL, 2018b, p. 42).

O maior desafio anunciado é a instituição da adequada estrutura de governança institucional, com a elaboração de uma estratégia nacional nessa seara e planos de mobilização abrangendo as diversas esferas e níveis de governo. A Estratégia precisaria incluir especialmente o tema da proteção de IEC e o sucesso da sua implementação estaria vinculado ao fomento de expertise no âmbito do Estado, com a capacitação dos agentes e servidores públicos e aumento do nível de conscientização, sendo imprescindível o estabelecimento de uma instância no governo federal especializada (BRASIL, 2018b, p. 42).

[18] Trata-se da Política Nacional de Segurança da Informação que foi aprovada pelo Decreto n.º 9.637, de 16 de dezembro de 2018 (BRASIL, 2018f).

Os avanços e esforços do país poderiam ser mensurados com a melhoria da posição do país em índices internacionais, notadamente no GCI, assim como na cooperação público-privada para a construção de indicadores relacionados aos ataques e incidentes, partindo-se dos indicadores nacionais construídos pelo Centro Regional de Estudos para o Desenvolvimento da Sociedade da Informação (CETIC.br) e pelo Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil (CERT.br) (BRASIL, 2018b, p. 43-44), ambos mantidos pelo Núcleo de Informação e Coordenação do Ponto BR (NIC.br). O NIC.br foi criado para implementar as decisões e os projetos do Comitê Gestor da Internet no Brasil (CGI.br)[19].

A E-Digital estabelece oito ações estratégicas para defesa e segurança no ambiente digital: edição de política nacional de segurança cibernética, contemplando a definição de uma instância nacional; adequação e harmonização da legislação penal e processual penal a fim de viabilizar a persecução penal dos crimes cibernéticos; elaboração de planos nacionais e subnacionais para tratamento de incidentes, inclusive focando nas IECs; estabelecimento de mecanismos de cooperação entre setores público e privado, entre entes da Federação e entre órgãos e entidades governamentais; capacitação de agentes públicos e de recursos humanos do setor privado; conscientização dos usuários; investimento em pesquisa e desenvolvimento, a fim de promover a autonomia tecnológica; e reforço dos instrumentos de cooperação internacional entre autoridades e provedores (acesso e conteúdo) de diversos países para garantir a aplicação da lei (BRASIL, 2018b, p. 43-44).

Voltando-se aos esforços verificados desde a elaboração da E-Digital nessa categoria, cita-se, por exemplo, a elaboração e aprovação da E-Ciber (BRASIL, 2020a), com a indicação do Gabinete de Segurança Institucional da Presidência da República como órgão coordenador de segurança cibernética em âmbito nacional[20]; a aprovação da ENSIC (BRASIL, 2020f); o convite ao Brasil para aderir à Convenção de Budapeste, início e finalização do seu processo de adesão[21]; e investimento em pesquisa e desenvolvimento. Neste último ponto, exemplifica-

[19] As atribuições do GCI.br constam do art. 1º do Decreto n.º 4.829, de 3 de setembro de 200, que dispõe sobre a criação do Comitê Gestor da Internet no Brasil – CGI.br, sobre o modelo de governança da Internet no Brasil, e dá outras providências. Disponível em: http://www.planalto.gov.br/ccivil_03/decreto/2003/d4829.htm. Acesso em: 08/01/2023. Maiores informações sobre a estrutura, atividades, atribuições e estatuto do NIC.br podem ser consultadas em: https://nic.br/quem-somos/. Acesso em: 08 jan. 2023.

[20] Ver Ação Estratégia 2.3.2. da Estratégia Nacional de Segurança Cibernética (BRAIL, 2020a).

[21] Mensagem n.º 412, de 22 de julho de 2020 do Presidente da República encaminha ao Congresso Nacional o texto da Convenção sobre o Crime Cibernético, celebrada em Budapeste, em 23 de novembro de 2001, com fins de adesão brasileira ao instrumento. Disponível em:https://www.in.gov.br/web/dou/-/despachos-do-presidente-da-republica-268441788. Acesso em: 24 jul. 2020. Salienta-se que o processo de adesão foi finalizado em 30 de novembro de 2022, durante a 27º Plenária do Comitê da Convenção de Crimes Cibernéticos, com o depósito pelo Brasil da carta de adesão à Convenção, consoante informações da página do Conselho da Europa, disponível em: https://www.coe.int/en/web/cybercrime/-/brazil-accedes-to-the-convention-on-cybercrime-and-six-states-sign-the-new-protocol-on-e-evidence. Acesso em: 31 dez. 2022.

se com a Seleção Pública MCTI/FINEP/FNDCT – Desafio Cibernético – Startups e empresas de base tecnológica[22].

Importa trazer à baila que no final de 2022, em 16 de novembro de 2022, o Ministério da Ciência, Tecnologia e Inovações aprovou a Estratégia Brasileira para a Transformação Digital para o ciclo 2022-2026 (E-Digital 2022-2026), atendendo intempestivamente à previsão de atualização quadrienal estabelecida no Decreto nº 9.319, de 21 de março de 2018, que instituiu o Sistema Nacional para a Transformação Digital e estabelece a estrutura de governança para a implantação da Estratégia Brasileira para a Transformação Digital (BRASIL, 2018a).

A E-Digital 2022-2026 mantém a metodologia da E-Digital e o conjunto de eixos habilitadores e de transformação digital. Especificamente no Eixo Habilitador de Confiança no Ambiente Digital, a categoria de defesa e segurança apresenta como contexto a evolução do Brasil no Índice Global de Segurança Cibernética da UIT; a percepção de risco dos usuários de internet no Brasil, ilustrando o sentimento de desconfiança da população no sentido de que os riscos podem superar os benefícios; e também a estatística do Brasil figurar como quinto maior destino de ataques de *ransomware* segundo dados de 2021 (BRASIL, 2022c, p. 35).

Em termos de ações estratégicas, a E-Digital 2022-2026 traz quatorze iniciativas, dentre as quais metade é destinada a ações relacionadas à proteção de dados pessoais. No tocante à segurança cibernética o documento identifica como ações estratégicas:

a) promoção de compartilhamento de informações via ReGIC, a qual será apresentada futuramente nesse capítulo;
b) edição de uma política nacional de segurança cibernética, incluindo a definição de instância nacional responsável pela articulação de um sistema nacional na matéria;
c) fortalecimento do ecossistema de segurança no país com a criação de um Conselho Nacional;
d) edição de planos nacionais e subnacionais de tratamento de incidentes; *v*) fomento a campanhas educacionais para fins de conscientização da população em geral; e
e) consolidação e harmonização do marco legal sobre crimes cibernéticos, tanto em direito material quanto processual. Ademais, também deve ser citada disposição relacionada à adequada regulação de tecnologias digitais disruptivas proporcional aos riscos que possam causar ao tratamento de dados de titulares, especialmente no

[22] Subvenção Econômica à Inovação – 09/2020 - Programa Desafio FINEP Desafio Cibernético - Startups e Empresas de Base Tecnológica, em parceria com o Exército Brasileiro. Edital e informações disponíveis em: http://www.finep.gov.br/chamadas-publicas/chamadapublica/657. Acesso em: 19 jan. 2021.

> tocante à segurança da informação, à segurança cibernética e à privacidade (BRASIL, 2022c, p. 36).

Ainda deve ser mencionado que, além de apontar as ações estratégicas, a edição 2022-2026 apresenta um balanço dos resultados de ações que foram realizadas para o eixo habilitador de confiança desde a aprovação da E-Digital em 2018, apontado as seguintes atividades no quadriênio passado: aprovação da LGPD; iniciativas do Comitê Gestor da Internet (CGI.br) e publicações da ANPD; criação da ANPD; convite do Brasil à adesão à Convenção de Budapeste em 2019; Acordo de Reconhecimento Mútuo de Certificados de Assinatura Digital do Mercosul (2019/2020); aprovação da PNSI e E-Ciber; instituição da ReGIC; e desenho do Programa Hacker do Bem para qualificação de jovens profissionais em segurança cibernética pelo Senai-SP e pela Softex (BRASIL, 2022c, p. 37).

Outrossim, são citados adicionalmente o desenvolvimento pela Rede Nacional de Pesquisa (RNP) de modelo de qualificação de profissionais em segurança de dados, bem como a realização de atividades de capacitação; a disponibilização de cursos pela Escola Nacional de Administração Pública (Enap); a criação do Grupo de Cibersegurança das Redes de Pesquisa e Educação da América Latina em 2021; as atividades de formação de recursos humanos especializados e investimento em capacitação desenvolvidas pela RNP, Laboratório Nacional de Computação Científica (LNCC) e a Empresa Brasileira de Pesquisa e Inovação Industrial (Embrapii); e as ações de conscientização, como, por exemplo, eventos realizados pelo Ministério de Ciência, Tecnologia e Inovações (MCTI) e RNP, boletins informativos do GSI/PR e campanhas com colaboradores organizadas pelo LNCC (BRASIL, 2022c, p. 37).

Recorda-se que ao analisar as ações estratégicas previstas na primeira E-Digital foram abordados alguns avanços e esforços nacionais, tanto na categoria de proteção de direitos e privacidade, quanto de defesa e segurança no ambiente digital, com grande associação ao inventário realizado pela E-Digital 2022-2026.

No entanto, ressalva-se que o documento claramente ressalta as iniciativas e ações realizadas no âmbito do MCTI ou de suas entidades vinculadas e/ou ligadas, como Embrapii, LNCC, RNP e Softex, e não apresenta qualquer referência que permita verificar do andamento dessas ações. Isso demonstra a fragmentação das atividades no âmbito nacional e a ausência de mapeamento dos esforços relacionados, bem como dificulta o acompanhamento da implementação da E-Digital. Também se denotam poucas menções às ações do GSI/PR entidade indicada como coordenadora nacional do tema pela E-Digital, consoante será futuramente abordado na subseção 3.5.2.1.

Deve-se atentar para o fato de que embora o MCTI tenha conduzido o processo da elaboração da E-Digital e da sua atualização, o trabalho é fruto do Comitê Interministerial para a Transformação Digital (CITDigital) e, como tanto, deveria refletir não só as ações do MCTI, mas apresentar um panorama nacional, tendo em vista a transversalidade do tema e o envolvimento de diversos ministérios.

Após a breve explanação sobre a E-Digital e seu novo ciclo, passa-se à seção destinada à apresentação de um dos principais marcos normativos estratégicos relacionados à segurança cibernética no país, qual seja, a PNSI.

3.4 POLÍTICA NACIONAL DE SEGURANÇA DA INFORMAÇÃO

A PNSI foi aprovada pelo Decreto nº 9.637, de 26 de dezembro de 2018 (BRASIL, 2018f), que institui a PNSI e dispõe sobre governança da segurança da informação, cuja abrangência está expressamente delimitada no seu art. 1º, visto ser aplicável tão somente no seio da APF, até mesmo pela espécie normativa adotada. Aqui se ressalva que embora documentado na própria E-Digital o trabalho de desenvolvimento de projeto de lei para o tratamento do tema, consoante pontuado anteriormente, a opção de lei formal (capaz de estabelecer obrigações a particulares e vincular todos os poderes e entes federativos) foi substituída pela adoção de decreto presidencial. Assim, vincula tão somente a APF, ou seja, todos órgãos e entidades que compõe a APF, direta e indireta.

A finalidade também está expressa no art. 1º, no sentido de assegurar a disponibilidade, integridade, confidencialidade e autenticidade da informação no âmbito nacional. Um dos pontos importantes é a definição do escopo de segurança da informação, que abrange nos termos do art. 2º: segurança cibernética; defesa cibernética; segurança física e proteção de dados organizacionais; e ações destinadas a assegurar a disponibilidade, integridade, confidencialidade e autenticidade da informação, nos termos dos incisos I, II, III e IV, respectivamente. Dessa forma, segurança cibernética é uma das quatro grandes categorias da segurança da informação (BRASIL, 2018f).

Insiste-se que Segurança Cibernética deve ser compreendida na PNSI, com base no Glossário de Segurança da Informação do DSI do GSI/PR (BRASIL, 2019d) como:

> [...] ações voltadas para a segurança de operações, de forma a garantir que os sistemas de informação sejam capazes de resistir a eventos no espaço cibernético capazes de comprometer a disponibilidade, a integridade, a confidencialidade e autenticidade dos dados armazenados, processados ou transmitidos e dos serviços que esses sistemas ofereçam ou tornem acessíveis.

Já segurança da informação é definida no Glossário como "*ações que objetivam viabilizar e assegurar a disponibilidade, a integridade, a confidencialidade e a autenticidade das informações*" (BRASIL, 2019d). Como princípios, o art. 3.º, além de soberania nacional e respeito e promoção dos direitos humanos e das garantias fundamentais (incisos I e II), destaca a visão sistêmica de segurança da informação (III); intercâmbio científico e tecnológico dentro da APF (V); conscientização e cultura de segurança da informação (VII); gestão de riscos (VIII); prevenção e tratamento dos incidentes (IX); garantia do sigilo de informações classificadas (XI); e cooperação interagência e internacional XIV e XVI), dentre outros (BRASIL, 2019).

Como objetivos, a PNSI elenca no art. 4º: contribuição para segurança individual, da sociedade e do Estado; fomento à pesquisa, desenvolvimento e inovação; aprimoramento do arcabouço legal; fomento à formação e qualificação de recursos humanos; fomento à cultura da segurança da informação; orientação de ações relacionadas à segurança de dados custodiados pela APF, à segurança da informação das IECs, à proteção de informações de pessoas físicas e tratamento de informações restritas; e contribuição para preservação da memória cultural do país (BRASIL, 2018f).

A PNSI é instrumentalizada na Estratégia Nacional de Segurança da Informação (ENSI) e nos planos nacionais, com fulcro no art. 5º. Ademais, o art. 6º estabelece que a ENSI conterá ações estratégicas e objetivos relacionados à segurança da informação e que será constituída de módulos, dentre os quais a PNSI expressamente cita: segurança cibernética; defesa cibernética; segurança das IECs; segurança da informação sigilosa; e proteção contra vazamento de dados, devendo ser construída com ampla participação da sociedade e do setor público (BRASIL, 2018f).

É justamente em resposta à PNSI que é elaborada a E-Ciber, como um dos módulos que integra a ENSI, tratando-se do primeiro apresentado à sociedade brasileira. Nesse ponto, traz-se à baila a entrega do segundo módulo da ENSI, referente à segurança das IECs, Decreto nº 10.569, de 9 de dezembro de 2020, o qual aprova a Estratégia Nacional de Segurança de Infraestruturas Críticas (BRASIL, 2020f).

Aqui cabe o interessante alerta de Malagutti, no sentido de que embora fale em módulos, a PNSI não fala em instrumentos apartados, assim a ENSI poderia constituir-se como um mesmo documento, abordando esses tópicos distintos e suas interdependências. No entanto, não foi essa a opção adotada e o autor aponta como hipóteses: a pendência do módulo de defesa; o objetivo de destacar a segurança em detrimento à defesa; ou a publicação para fins de

consideração e pontuação no processo de revisão das capacidades brasileiras pelo GCSCC (2022c, 3-19).

Ao lado da ENSI figuram os planos nacionais, os quais, por sua vez, são instrumentos da PNSI e focam na implementação da ENSI, visto que conterão detalhamento da execução das ações estratégicas, incluindo seu planejamento, organização, coordenação e recursos, assim como atribuição de responsabilidades e cronograma, com espeque no art. 7º (BRASIL, 2018f).

A PNSI também institui o Comitê Gestor da Segurança da Informação (CGSI), com o objetivo de assessorar o GSI/PR nessa seara e, é por ele coordenado. O CGSI é composto por representantes titular e suplente dos Ministérios e Secretarias e Órgãos com status de ministério[23], totalizando à época 22 órgãos. Os membros são indicados pelos titulares desses órgãos e designados em Ato do Ministro de Estado Chefe do GSI/PR, ressaltando-se que a indicação deve recair na figura do seu Gestor de Segurança da Informação (arts. 8.º e 9.º do Decreto nº 9.637, de 26 de dezembro de 2018).

Em termos de funcionamento, o CGSI deve se reunir semestralmente, de forma ordinária, e, extraordinariamente, sob convocação do coordenador (art. 10, *caput*), podendo instituir grupos de trabalhos ou câmaras técnicas e convidar representantes dos setores público e privado, bem como especialistas para tratamento de temas específicos. Suas deliberações são aprovadas por maioria simples, atendido o *quórum* mínimo de presença de um terço dos membros em segunda chamada. Ademais, o voto do coordenador (representante do GSI/PR), além de voto regular, possui voto de desempate. Ou seja, considerando o quórum mínimo, 5 votos seriam necessários para aprovar alguma deliberação no CGSI (§§ 1.º, 2.º, 3.º e 4.º do art. 10).

Além de instituir a PNSI e o CGSI, o Decreto nº 9.637, de 26 de dezembro de 2018, também destaca as competências do GSI/PR nos temas referentes à segurança da informação, com o assessoramento do CGSI. As competências expressamente relacionadas no art. 12 são:

a) estabelecimento de norma de requisitos metodológicos para implementação de gestão de risco na APF (art. 12, I);
b) aprovação de diretrizes, estratégias, normas e recomendações (art. 12, II);

[23] Composição alterada pelo Decreto n.º 9.832, de 12 de junho de 2019, que altera o Decreto n.º 9.637, de 26 de dezembro de 2018, e o Decreto n.º 7.845, de 14 de novembro de 2012, para dispor sobre o Comitê Gestor da Segurança da Informação. Disponível em: http://www.planalto.gov.br/ccivil_03/_Ato2019-2022/2019/Decreto/D9832.htm#art1. Acesso em: 19 jan 2021. A totalização de apenas 22 órgãos reflete a composição no final do Governo de Jair Bolsonaro, a qual já apresentava desatualização quanto ao desmembramento do Ministério da Ciência, Tecnologia, Inovações e Comunicações em Ministério da Ciência, Tecnologia e Inovações e Ministério das Comunicações, determinado pela Medida Provisória n.º 980, de 10 de junho de 2020, convertida na Lei n.º 14.074, de 14 de outubro de 2020, disponível em: http://www.planalto.gov.br/ccivil_03/_ato2019-2022/2020/Lei/L14074.htm. Acesso em: 19 jan. 2021.

c) elaboração e implementação de programas voltados à conscientização e capacitação de servidores da APF e da sociedade (art. 12, III);
d) acompanhamento da evolução do tema, nacional e internacionalmente (art. 12, IV);
e) elaboração da ENSI, em articulação com o Comitê Interministerial para a Transformação Digital[24](art. 12, V);
f) apoio à elaboração dos respectivos planos nacionais (art. 12, VI);
g) definição de critérios para avaliar a implementação da PNSI e dos seus instrumentos;
h) proposição de atos normativos necessários (art. 12, VII);
i) definição de requisitos mínimos de segurança para uso de produtos, ressalvadas as competências específicas de outros órgãos (art. 12, IX), caso em que caberá ao GSI/PR propor as atualizações relacionadas à segurança da informação (parágrafo único do art. 12); e
j) engajamento com CIRTS/CSIRTS/CERTS nacionais (BRASIL, 2018f).

Ao Ministério da Defesa cabe o apoio ao GSI/PR no tocante à segurança cibernética e à elaboração de diretrizes, dispositivos e procedimentos referente à defesa nacional contra ataques cibernéticos, nos termos do art. 13, I e II. Já ao Ministério da Transparência e Controladoria-Geral da União compete auditar a execução da PNSI pela APF, no que lhe compete, conforme o art. 14 (BRASIL, 2018f).

Finalmente, o Decreto traz nos arts. 15 a 18 uma série de competências para a APF e para a alta administração desses órgãos e entidades relacionadas à governança da segurança da informação nas suas unidades. Cita, por exemplo, a implementação da PNSI; a elaboração de sua política de segurança da informação; a designação de gestor de segurança da informação; a instituição de comitê de segurança da informação ou estrutura análoga; e instituição e implementação de equipe de tratamento e resposta a incidentes em redes de computadores (competência elencadas no art. 15). Além disso, os §§ 1.º, 2.º e 3.º do art. 15 tratam da composição e das atribuições do comitê de segurança da informação desses órgãos e entidades, que devem editar ato sobre o funcionamento dessa estrutura, consoante art. 16 (BRASIL, 2018f).

O art. 17 lista as competências da alta administração na área e o art. 18 salienta o caráter mandatório das normas de segurança da informação editadas pelo GSI/PR, bem como dos normativos relacionados do Ministério do Planejamento, Desenvolvimento e Gestão, os

[24] Criado pelo Decreto n.º 9.319, de 21 de março de 2018 (BRASIL, 2018a).

quais devem ser incorporados nos respectivos atos administrativos dos órgãos e entidade da APF direta, autárquica e fundacional (BRASIL, 2018f).

Como disposições finais, o art. 19 do Decreto nº 9.637, de 26 de dezembro de 2018, determina a edição, no prazo de noventa dias, de glossário das terminologias empregadas em segurança da informação (BRASIL, 2019d) e o art. 21 altera o art. 1º do Decreto nº 2.295, de 4 de agosto de 1997[25], a fim de permitir a dispensa de licitação referente à "*aquisição de equipamentos e contratação de serviços técnicos especializados para as áreas de inteligência, de segurança da informação, de segurança cibernética, de segurança das comunicações e de defesa cibernética*" (BRASIL, 2018f).

Interessante trazer um breve apanhado histórico sobre a aprovação da PNSI, relembrando a existência anterior de Política de Segurança da Informação para a APF, aprovada pelo Decreto nº 3.505, de 13 de julho de 2000 (BRASIL, 2000a), o qual foi expressamente revogado pela PNSI, distinguindo-se claramente do texto atual. Em primeiro lugar, cabe destacar o grande lapso temporal entre os dois textos, de quase duas décadas. Nesse ínterim, a conectividade, a Internet e a interdependência das IECs mudaram profundamente a sociedade, a economia e as relações internacionais, fazendo com que o tema ganhasse prioridade nacional e internacional, nos termos extensivamente abordados no Capítulo I.

Assim, passa-se de uma abordagem limitada de gestão de segurança da informação nos órgãos e entidade da APF, ou seja, de uma política para os órgãos e entidades federais, para uma política nacional, embora limitada pela espécie normativa utilizada[26]. Essa política nacional carrega a determinação de edição de diversos normativos para o tratamentos das diversas perspectivas relacionadas à segurança da informação (ENSI com seus módulos e os planos nacionais); atribui a responsabilidade ao GSI/PR de elaboração e publicação da ENSI; e, finalmente, destaca as obrigações dos órgãos e entidade da APF de gestão da segurança da informação nas suas respectivas unidades.

Cronologicamente, após a edição da PNSI no final de 2018, a sequência normativa tem a sua continuidade com a elaboração e aprovação do primeiro módulo da ENSI, que será apresentado na próxima seção, qual seja a E-Ciber.

---

[25] Decreto n.º 2.295, de 4 de agosto de 1997, que regulamenta o disposto no art. 24, inciso IX, da Lei n.º 8.666, de 21 de junho de 1993, e dispõe sobre a dispensa de licitação nos casos que possam comprometer a segurança nacional. Disponível em: http://www.planalto.gov.br/ccivil_03/decreto/D2295.htm. Acesso em 19 jan. 2021.

[26] Nos termos do art. 84, VI, da Constituição Federal, compete ao Presidente da República dispor mediante decreto sobre alguns temas administrativos referentes ao Poder Executivo, como a organização e funcionamento da administração federal, quando não implicar em aumento de despesa, nem criação ou extinção de órgãos públicos (BRASIL, 1988).

3.5 ESTRATÉGIA NACIONAL DE SEGURANÇA CIBERNÉTICA

Essa seção destina-se à apresentação da E-Ciber e é composta por quatro subseções que abordam os quatro grandes tópicos do instrumento, quais sejam, diagnóstico; eixos temáticos relacionados à proteção e segurança; eixos transformadores; e ações estratégicas. Considerando a inexistência de um arcabouço estratégico e o marco estabelecido na PNSI, com a diretriz de construção modular da ENSI, o Brasil elaborou a sua primeira Estratégia Nacional de Segurança Cibernética (E-Ciber), aprovada da forma de Anexo ao Decreto nº 10.222, de 5 de fevereiro de 2020 (BRASIL, 2020a). Conforme já retratado anteriormente, a E-Ciber foi antecedida e contextualizada pela E-Digital e pela PNSI.

Faz-se apenas uma ressalva inicial no sentido de que a presente seção dedicar-se-á a fazer uma apresentação da E-Ciber, a fim de viabilizar uma ampla visão de todo o arcabouço normativo, e que o próximo capítulo (Capítulo IV) será destinado a uma análise da E-Ciber, conjugando-a com os modelos estudados no Capítulo II, à luz do recorte das prescrições normativas para o aprimoramento do arcabouço jurídico e da governança institucional do tema no Brasil.

Conforme já mencionado anteriormente, a E-Ciber constitui o primeiro módulo da ENSI entregue à sociedade brasileira, apresentando a visão do Governo Federal para quadriênio 2020-2023, de tornar o Brasil um país de excelência em segurança cibernética, cabendo aos órgãos e entidades da APF a sua implementação (art. 2.º do Decreto nº 10.222, de 5 de fevereiro de 2020). Como objetivos estratégicos, a E-Ciber estabelece: tornar o Brasil mais próspero e confiável no ambiente digital; aumentar a resiliência brasileira às ameaças cibernéticas; e fortalecer a atuação brasileira em segurança cibernética no cenário internacional (BRASIL, 2020a).

Metodologicamente, a E-Ciber utilizou o Modelo do GCSCC da *Oxford Martin School* da Universidade de Oxford[27], estudado no Capítulo III, levando à identificação na E-Ciber de sete eixos temáticos. Esses eixos abrangem a área de proteção e de segurança e os eixos transformadores, assim denominados pelo poder de transformação dos temas por eles influenciados. Os primeiros abrangem três eixos: governança da segurança cibernética nacional; universo conectado e seguro; e proteção estratégica. Já os eixos transformadores são quatro e dizem respeito à dimensão normativa; pesquisa, desenvolvimento e inovação;

[27] Relembra-se que esse modelo é centrado em cinco dimensões: Estratégia e Política de Segurança Cibernética; Cultura de Segurança Cibernética e Sociedade; Construção de Conhecimento e Capacidades em Segurança Cibernética; Arcabouço Legal e Regulatório; e Padrões e Tecnologia (OXFORD, 2021).

dimensão internacional e parcerias estratégicas; e educação, totalizando sete eixos (BRASIL, 2020a).

Dessa forma, em termos de estrutura do documento, a Estratégia contém uma parte destinada às considerações preliminares, composta de sumário executivo, introdução e metodologia; e a uma outra parte para tratar especificamente da estratégia em si, com a visão para o país, objetivos e ações estratégicas. Na sequência, o documento traz mais duas partes, identificadas como Partes I e II, as quais se destinam à elaboração de diagnóstico e análise dos eixos temáticos, respectivamente (BRASIL, 2020a).

Com base no diagnóstico (Parte I) e na análise desses setes eixos avaliados na Parte II do Anexo, a E-Ciber apresenta um conjunto de dez ações estratégicas, que por sua vez, identificam iniciativas, ações e medidas que podem ser adotadas para a sua implementação. As dez ações estratégicas são:

a) fortalecimento de ações de governança cibernética;
b) estabelecimento de um modelo centralizado de governança no âmbito nacional;
c) promoção de ambiente participativo, colaborativo, confiável e seguro, entre setores público e privado, bem como sociedade;
d) elevação do nível de proteção do Governo;
e) elevação do nível de proteção de IEC nacional;
f) aprimoramento do arcabouço legal sobre segurança cibernética;
g) incentivo à concepção de soluções inovadoras em segurança cibernética;
h) ampliação da cooperação internacional do Brasil em Segurança cibernética;
i) ampliação da parceria, em segurança cibernética, entre setores público e privado, academia e sociedade; e
j) elevação do nível de maturidade da sociedade em segurança cibernética (BRASIL, 2020a).

É interessante notar que todo o diagnóstico, constante da Parte I, e a análise dos eixos temáticos, constante da Parte II, os quais fundamentam as ações estratégicas elencadas, foram publicados integralmente junto com a Estratégia, no Anexo ao Decreto, sendo a seguir detalhados. Uma das críticas ao documento reside justamente nessa estrutura, tornando o texto excessivamente extenso e dissonante das demais políticas públicas estratégicas brasileiras, aproximando-se a um texto acadêmico, não estratégico (MALAGUTTI, 2022b).

Passa-se assim às quatros subseções da tese que abordarão diagnóstico, eixos temáticos de proteção e segurança, eixos temáticos transformadores e ações estratégicas.

3.5.1 Diagnóstico

Quanto à Parte I, o diagnóstico destaca o cenário de progressiva conectividade e, como consequência, de crescente aumento da superfície de ataque, apresentando diversas estatísticas e índices utilizados para tecer um panorama nacional e internacional, os quais podem ser agrupados em dados referentes aos uso das TICs; ao impacto financeiro dos crimes cibernéticos; às capacidades em segurança cibernética; e à origem e ao destino dos ataques (BRASIL, 2020a).

Nesse sentindo, com relação ao uso das TICs, o diagnóstico relaciona o acesso à Internet de quase 75% dos domicílios brasileiros, 100% dos órgãos federais e estaduais e 98% das empresas, alcançando o país o 66º lugar em ranking das Nações Unidas que avalia o índice de desenvolvimento das TICs. No tocante aos prejuízos causados, estima perdas em 2017 de mais de vinte e dois bilhões de dólares e mais de setenta bilhões de vítimas. Cita que em 2018, 89% de executivos foram vítimas de fraudes cibernéticas, ano em que foi verificado um aumento de quase 96% de crescimento dos ataques no Brasil, em comparação com o primeiro semestre do ano anterior. Desses, mais de 57% dos ataques referiram-se a *phishing*[28](BRASIL, 2020a).

Já com relação às capacidades, cita a septuagésima posição do Brasil no GCI; o baixo nível de governança de Tecnologia da Informação nos órgãos federais; e a falha legislação para o enfrentamento dos crimes cibernéticos. Por fim, especificando os incidentes de segurança, o Brasil seria o segundo país com maior prejuízo com crimes cibernéticos, sendo alvo número um e a principal fonte de ataques on-line na América Latina. Ademais, o Brasil seria um dos principais hospedeiros de sites de *phishing* (BRASIL, 2020a).

Destaque importante é dado à progressiva adoção do governo eletrônico, com a disponibilização de serviços de todos os entes da Federação na Internet, com forte processo de digitalização do Governo Federal, o qual é consubstanciado na Política de Governança Digital[29]; na E-Digital, anteriormente apresentada; e nas diretrizes de Compartilhamento de

[28] Termo não definido pelo Glossário de Segurança da Informação do GSI/PR (BRASIL, 2019d). Adota-se a definição do Glossário de Resposta a Incidentes da ENISA, que sustenta que o ataque de *phishing* pode ser compreendido como uma maneira de fazer com que a vítima forneça informações confidenciais (dados bancários, por exemplo), por meio de uma combinação de fraude e engenharia social. O ataque pode ser instrumentalizado por *spam*, site malicioso, mensagens de e-mail ou SMS, as quais tentam figurar como de uma fonte legítima. Elementos característicos são a utilização de táticas de urgência e intimidação e, geralmente, não são personalizadas (ENISA, [201?]).

[29] Aprovada pelo Decreto n.º 8.638, de 15 de janeiro de 2016, que instituiu a Política de Governança Digital no âmbito dos órgãos e das entidades da administração pública federal direta, autárquica e fundacional. Disponível em: http://www.planalto.gov.br/ccivil_03/_Ato2015-2018/2016/Decreto/D8638.htm. Acesso em: 21 jan. 2021. Cabe ressaltar que esse decreto foi expressamente revogado pelo Decreto nº 10.332, de 28 de abril de 2020, que institui a Estratégia de Governo Digital para o período de 2020 a 2022, no âmbito dos órgãos e das entidades da administração pública federal direta, autárquica e fundacional e dá outras providências. Disponível em:

Dados no âmbito da APF[30]. Nesse contexto, a proteção das redes e sistemas da administração pública reveste-se de fundamental importância, da mesma forma que a proteção das empresas que detêm e operam IECs no país, avaliando-se como principais tipos de ameaças os ataques de *phishing*; negação de serviço em larga escala; vazamentos de dados; espionagem e terrorismo cibernéticos; e interrupção de serviços (BRASIL, 2020a).

Diante do diagnóstico sintetizado, passa-se a apresentação dos eixos temáticos, os quais foram concebidos após a consideração das cinco dimensões do CMM, modelo utilizado e expressamente mencionado no texto da E-Ciber.

3.5.2 Eixos Temáticos: Proteção e Segurança

Conforme já exposto anteriormente, a Parte II da Estratégia apresenta os eixos temáticos, sendo que o de proteção e segurança subdivide-se em três temas: governança da segurança cibernética nacional; universo subconectado e seguro: prevenção e mitigação de ameaças cibernéticas; e proteção estratégica, que se passa a estudar na sequência.

3.5.2.1 Governança da Segurança Cibernética Nacional

O eixo temático destinado a tratar da governança da segurança cibernética nacional, enfatiza a especial relevância da adoção do conjunto de processos de gestão, a fim de garantir o alinhamento do planejamento às ações estratégicas, com a otimização do emprego de recursos. Nessa linha, a governança da segurança cibernética abarca o fortalecimento da capacidade institucional; o desenvolvimento e aplicação de normas (regras e princípios) e procedimentos; o monitoramento das políticas públicas; a gestão de riscos; a comunicação de incidentes; e a ações de elaboração e adoção de boas práticas, requisitos mínimos e recomendações (BRASIL, 2020a).

Como premissas balizadoras do eixo temático nas suas três perspectivas, tem-se a confiança nos serviços públicos digitais; a garantia de proteção das redes e sistemas dos órgãos e entidades da APF; investimento na transformação digital do governo; o cumprimento pelos

http://www.planalto.gov.br/ccivil_03/_Ato2019-2022/2020/Decreto/D10332.htm#art14. Acesso em: 21 jan. 2021.

[30] As Diretrizes de Compartilhamento de Dados no âmbito da APF foram aprovadas pelo Decreto n.º 10.046, de 9 de outubro de 2019, que dispõe sobre a governança no compartilhamento de dados no âmbito da administração pública federal e institui o Cadastro Base do Cidadão e o Comitê Central de Governança de Dados. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2019-2022/2019/Decreto/D10046.htm. Acesso em: 22 jan. 2021.

fornecedores do governo das normas de segurança cibernética; e a necessidade de dados atualizados que possam subsidiar política pública e planejamento de novas diretrizes e programas (BRASIL, 2020a).

Especificamente quanto aos produtos e serviços, a análise ressalta a importância da adoção de padrões nacionais e internacionais no seu desenvolvimento, inclusive dos princípios de *privacy by design and default* e *security by design and default*, ao mesmo tempo que salienta o papel do Estado de garantir um ambiente que permita a inovação, a fim de possibilitar o desenvolvimento de novas soluções de segurança e proteção dos usuários (BRASIL, 2020a).

O exame também reconhece que em termos nacionais, a governança cibernética não se limita ao setor público, orientando os direitos e obrigações de todos setores da sociedade, levando aos setores público e privado a priorizar o uso seguro, sem olvidar o papel dos usuários do país, os quais precisam elevar sua participação no ecossistema digital (BRASIL, 2020a).

Com relação à gestão de riscos, identificada como um dos pontos-chave da governança cibernética, engloba princípios, objetivos, estruturas, competências e processos para identificação e mitigação das vulnerabilidades, permitindo a identificação dos ativos mais importantes que devem ser protegidos. Nesse ponto, o documento relembra as Normas Complementares emitidas pelo GSI/PR relacionadas à gestão de riscos e que são mandatórias para APF direta, autárquica e fundacional, quais sejam as Normas Complementares nº 02 e 04/IN01/DSIC/GSI/PR[31] (BRASIL, 2020a).

Traz-se à baila o conceito de Gestão de Riscos de Segurança da Informação definido pelo Glossário de Segurança da Informação do GSI/PR como:

> [...] processo de natureza permanente, estabelecido, direcionado e monitorado pela alta administração, que contempla as atividades de identificação, avaliação e gerenciamento de potenciais eventos que possam afetar a organização, destinado a fornecer segurança razoável quanto à realização de seus objetivos (BRASIL, 2019d).

[31] Norma Complementar n.º 02/IN01/DSIC/GSI/PR, de 13 de outubro de 2008, que dispõe sobre a metodologia de gestão de segurança da informação e dá orientações acerca de definição de riscos, de procedimentos para identificar os riscos e seus níveis aceitáveis, da análise de impactos e de probabilidades e de opções de tratamento dos riscos. Essa norma foi revogada em 27 de maio de 2020 pela Instrução Normativa GSI/PR n.º 01, disponível em: https://www.in.gov.br/en/web/dou/-/instrucao-normativa-n-1-de-27-de-maio-de-2020-258915215. Acesso em: 21 jan 2021; e Norma Complementar nº 04/IN01/DSIC/GSI/PR, de 15 de fevereiro de 2013, que estabelece diretrizes para o processo de gestão de riscos de segurança da informação e comunicações nos órgãos ou entidades da Administração Pública federal, direta e indireta. Essa norma também foi revogada posteriormente à edição da E-Ciber, pela Instrução Normativa GSI/PR n.° 3, de 28 de maio de 2021. Disponível em: https://www.in.gov.br/en/web/dou/-/instrucao-normativa-gsi/pr-n-3-de-28-de-maio-de-2021-322963172. Acesso em: 09 jan. 2023.

A Norma Complementar nº 04/IN01/DSIC/GSI/PR, de 15 de fevereiro de 2013, facultava aos órgãos e entidades da APF a adoção de metodologias de gestão de riscos diversas pela APF, desde que observados os objetivos, diretrizes gerais e escopo, assim como os critérios de avaliação e aceitação de risco. Tal premissa foi mantida na norma sucessora[32] e essa diversidade metodológica adotada pelos setores público e privado é identificada como fator que dificulta a avaliação do grau de maturidade em segurança cibernética no país, demandando a padronização de melhores práticas (BRASIL, 2020a).

Ao mesmo tempo, a análise também prescreve que a adoção de um padrão único e excludente não seria inevitavelmente frutífero, em face da transversalidade do tema, assim como da necessidade de abarcar todos os setores da sociedade e de continuidade do processo. Nesse sentido, o documento propõe como patamar inicial de padronização a adoção das normas emitidas pelo GSI/PR, cuja observância hoje limita-se à APF direta, autárquica e fundacional, citando também as normas da ISO e outros padrões metodológicos, como do NIST (BRASIL, 2020a).

Além de especificar outras organizações que produzem padrões, o documento também aborda soluções, como a existência de plataformas que permitem fazer a macrogestão de diversos ativos e diferentes tecnologias, também realçando a importância de certificação de produtos e soluções em segurança cibernética, como um objetivo a ser buscado. Outra questão que pode ser acrescida nessa discussão é o recurso do certificado digital, o qual pode contribuir para uso mais seguro e confiável do ambiente digital, uma vez que a utilização do certificado acarreta a garantia de confidencialidade, de autenticidade e de comprovação de autoria nas transações. Nesse ponto, a análise relembra que a certificação já é utilizada em alguns setores no País, como no Sistema de Pagamentos Brasileiros; no Poder Judiciário e nos serviços prestados pela Receita Federal do Brasil[33] (BRASIL, 2020a).

No que diz respeito à coordenação das ações de segurança cibernética, ou seja, da governança propriamente dita, o instrumento destacou que a gestão envolve múltiplos atores e o sucesso está associado à inclusão do setor privado e sociedade, tanto nacional quanto internacionalmente (BRASIL, 2020a).

Dessa forma, a criação de um sistema reunindo atores estatais e não estatais é fundamental para o alinhamento das ações, cabendo ao Governo Federal a condução,

[32] Instrução Normativa GSI/PR n.° 3, de 28 de maio de 2021. Disponível em: https://www.in.gov.br/en/web/dou/-/instrucao-normativa-gsi/pr-n-3-de-28-de-maio-de-2021-322963172. Acesso em: 09 jan. 2023.

[33] A Infraestrutura de Chaves Públicas Brasileira – ICP-Brasil foi instituída pela Medida Provisória n.º 2.200, de 28 de junho de 2001, disponível em: http://www.planalto.gov.br/ccivil_03/mpv/antigas_2001/2200.htm . Acesso em: 24 jan. 2021.

incentivando a discussão e propondo alternativas. Essa premissa é corroborada pelo trabalho da Comissão Parlamentar de Inquérito da Espionagem de 2012, que no quesito de governança, apontou a dificuldade do governo deter uma visão geral nessa seara. E, como consequência, dificuldade de adotar ações eficazes, o que decorre das ações individualizadas dos órgãos públicos, com adoção de definições, ações e critério diferentes, e sem o compartilhamento de informações. Assim o Sistema endereçaria essas dificuldades (BRASIL, 2020a).

Ademais também se reveste de extrema importância a definição de um órgão como responsável para orientar o tema nacionalmente, excluindo-se os temas de defesa e segurança cibernéticas, de responsabilidade do Ministério da Defesa, sendo necessária a interação dessas esferas (BRASIL, 2020a).

A Análise cita que o modelo centralizado de gestão adotado em vários países é considerado viável e eficaz. Sustenta que o estabelecimento de estruturas centrais apresenta bons resultados. Outro ponto é o reconhecimento de que, no Brasil, o GSI/PR, por meio do Departamento de Segurança da Informação (DSI), tem trabalhado desde 2006 para estudar e elaborar diversos normativos como as Instruções Normativas e Normas Complementares, além de estratégias e políticas direcionadas à APF. Nessa toada, dispensa-se, portanto, a criação de novo órgão e/ou entidade, uma vez que o redimensionamento da estrutura do GSI/PR permitiria sua atuação (BRASIL, 2020a).

Além do redimensionamento, o documento destaca a urgência de lei temática. Essa lei permitiria ao GSI/PR tornar-se macrocoordenador estratégico, com a especificação de atribuições e a definição de mecanismos de diálogo com a sociedade. Como exemplo de mecanismo de diálogo estruturado com a sociedade, a Estratégia recomenda a criação de um Conselho Nacional de Segurança Cibernética, com a institucionalização da participação de atores não estatais, além dos estatais. Outrossim, menciona a continuidade do debate com a criação de uma espécie de grupo técnico, como uma forma de envolver profissionais especializados e de diferentes setores, permitindo uma visão abrangente dos desafios (BRASIL, 2020a).

Tal organização garantiria a alinhamento das ações e a evolução convergente e estruturada do país nessa seara, não se olvidando a análise da questão dos recursos, para os quais defende a urgência de priorização (BRASIL, 2020a).

Um dos últimos apontamentos do eixo de governança, refere-se ao constante monitoramento e avaliação da eficácia de instrumentos normativos, assim como dos centros de tratamento e resposta aos incidentes computacionais. Para tanto, relaciona a elaboração de indicadores e métricas que possam mensurar o desempenho do país em segurança cibernética e

o estabelecimento de rotinas de conformidade nos órgãos e entidades dos setores público e privado, na busca do aprimoramento contínuo, recordando-se das diretrizes de governança pública instituídas pelo Decreto nº 9.203, de 22 de novembro de 2017[34] (BRASIL, 2020a).

Após a apresentação do eixo temático destinado a tratar da governança da segurança cibernética nacional, passa-se ao segundo eixo destinado a abordar a conectividade e a segurança.

3.5.2.2 Universo conectado e seguro: prevenção e mitigação de ameaças cibernéticas

Nesse eixo temático, a análise volta-se para a gestão dos incidentes computacionais, que assume especial importância no contexto de transformação digital e de novas tecnologias disruptivas (Computação Quântica, 5G, Internet das Coisas, Inteligência Artificial, etc). Como o risco não pode ser totalmente eliminado com atividades preventivas, a detecção, resposta e recuperação são fundamentais para tornar o ambiente mais seguro, com destaque para o aprimoramento dos mecanismos de compartilhamento de informações, em diferentes níveis, esferas e setores, nacional e internacionalmente. Um ponto importante elencado reside na simplificação do processo de compartilhamento entre todos os centros que realizam gestão de incidentes, especialmente considerando a crescente ampliação do número de centros, tanto no setor público, quanto no privado (BRASIL, 2020a).

A gestão desses incidentes é feita nas organizações públicas e privadas por equipes de tratamento e resposta aos incidentes, as quais são denominadas como Equipe de Tratamento e Resposta a Incidentes em Redes Computacionais (ETIR)[35]e também conhecidas como *Computer Security Incident Response Team* (CSIRT)[36]. A análise apresenta um panorama dessas organizações no Brasil, que são agrupadas em oito tipos. O primeiro grupo refere-se aos Centros com responsabilidade nacional, existindo no País o Centro de Prevenção, Tratamento e Resposta a Incidentes Cibernéticos de Governo (CTIR Gov), subordinado ao DSI do GSI/PR, e o CERT.br. Além disso, tem-se os centros de coordenação internacional; das IECs; de provedores; da academia; corporativos; do Poder Público; e militares (BRASIL, 2020a).

---

[34] Decreto n.º 9.203, de 22 de novembro de 2017, que dispõe sobre a política de governança da administração pública federal direta, autárquica e fundacional. Disponível em: http://www.planalto.gov.br/ccivil_03/_Ato2015-2018/2017/Decreto/D9203.htm . Acesso em: 24 jan. 2021.

[35] Definida como "*grupo de pessoas com a responsabilidade de receber, analisar e responder às notificações e atividades relacionadas a incidentes de segurança em redes de computadores*" (BRASIL, 2019d).

[36] Definido como "*acrônimo internacional para designar um grupo de resposta a incidentes de segurança, responsável por tratar incidentes de segurança para um público alvo específico*" (BRASIL, 2019d).

A responsabilidade nacional está expressamente subdividida no CERT.br, voltado para redes comerciais e instituições privadas, enquanto que o CTIR Gov foca nas redes governamentais e executa as ações de notificação de incidentes; análise; suporte à resposta; coordenação da resposta; distribuição de alertas, recomendações e estatísticas; e cooperação com outros centros (BRASIL, 2020a).

Especificamente quanto ao CTIR Gov, além de ressaltar as suas capacidade de monitoramento de vulnerabilidades, indisponibilidades e de anúncios de vazamentos de dados, também integrando rede internacional de CSIRTs, prenuncia a oportunidade de aprimoramento do modelo, com *benchmarking* de padrões globais e participação em foros internacionais como o *Forum of Incident Response and Security Teams* (FIRST)[37]; o *Antiphising Working Group* (APWG); e o *Latin America and Caribbean Anti-abuse Working Group* (LAC-AAWG). Ademais, a análise recomenda outorgar ao CTIR Gov atuação em âmbito nacional e fortalecer o órgão (BRASIL, 2020a).

Em termos de reporte de incidentes, as três maiores categorias de notificações recebidas pelo CTIR Gov entre 2011 e 2018 referem-se à abuso de sítio, vazamento de dados e fraude. Já com relação ao CERT.br, em 2018, 98% das notificações referiram-se a servidores que tiveram suas páginas desfiguradas, sem olvidar que os casos são reportados de forma voluntária. Considerando a possibilidade de ataques semelhantes, a criação de ambiente colaborativo é essencial, e o EGC, já citado anteriormente nas subseções 2.2 do Capítulo II e 3.1 deste Capítulo, é um exemplo de ação colaborativa. Outrossim, a existência de uma plataforma de compartilhamento coloca-se como outra abordagem de iniciativa de colaboração, permitindo a troca de informações com relação a vulnerabilidades, ameaças e tendências (BRASIL, 2020a).

Último ponto desse eixo temático aborda a interceptação ilegal, a qual pode ser efetivada por diversas maneiras e, pontualmente, não pode ser repelida com políticas de segurança, ressalvando o importante recurso da criptografia, que pode fornecer camada adicional de segurança (BRASIL, 2020a).

Segue-se para o último eixo do tema de proteção e segurança, que contempla a proteção estratégica.

[37] Interessante apontar que durante o ano de 2022 o CTIR Gov foi admitido como membro do FIRST. Maiores informações podem ser consultadas em: https://www.gov.br/ctir/pt-br/assuntos/noticias/2022/o-ctir-gov-foi-admitido-como-membro-do-forum-of-incident-response-and-security-teams-first. Acesso em: 09 jan. 2023.

3.5.2.2 Proteção Estratégica

Nesse eixo, aborda-se a proteção do governo e das IECs. Assim, um dos primeiros pontos de destaque da análise é a transformação digital com a crescente digitalização dos serviços públicos, cujas redes e sistemas tornam-se cada vez mais críticos. Dessa forma, para dar suporte à transformação e proteger esses ativos, é necessário mitigar as vulnerabilidades, o que demanda a articulação de diversos atores nacionais e internacionais (BRASIL, 2020a).

Uma das lacunas identificadas é a carência de atividades de capacitação abarcando todas as esferas de governo, e especialmente em relação às IECs. Ademais, sistemas e redes governamentais demandam a implementação de recursos adequados de proteção, os quais precisam englobar conjunto estruturado de investimentos em conhecimento, políticas, profissionais e tecnologias (BRASIL, 2020a).

Considerando que bases de dados custodiados pela Administração Pública estão relacionadas à prestação de serviços públicos, a análise recomenda cópias de segurança com atualização frequente, automaticamente segregadas e com armazenamento em local seguro, a fim de mitigar riscos de ataques e evitar solução de continuidade dos serviços. Outro ponto relevante é a segurança dos dispositivos finais (*endpoint*s) conectados à rede, que hoje representam uma variedade de dispositivos como *tablets, smartphones e notebooks*, os quais são alvo de mais de nove milhões de novos casos *malwares* todos os meses, conforme apontado na E-Ciber (BRASIL, 2020a).

Da mesma forma, ataque às cadeias de suprimentos também já era destacado quando da elaboração do documento como uma das preocupações de segurança, recomendando-se o estabelecimento de requisitos mínimos de segurança cibernética para a APF, aprimorando a segurança cibernética do setor público e alavancando o mercado com o poder de compra do Estado, que deveria atentar para inclusão dessa temática nos seus instrumentos de contratação (BRASIL, 2020a).

O eixo traz algumas estatísticas sobre o custo de violação de dados e incidentes, apontando que nacionalmente uma violação tem custo médio de um milhão duzentos e quarenta mil dólares e, internacionalmente, em 2018, de quase quatro milhões, ano em que foi constatado aumento de 350% dos ataques de *ransomware*, 250% de ataques *spoofing* e 70% de ataques *spear-phishing*[38] (BRASIL, 2020a).

[38] Termo não definido pelo Glossário de Segurança da Informação do GSI/PR (BRASIL, 2019d). Adota-se a definição do Glossário de Resposta a Incidentes da ENISA, que sustenta que se trata de uma versão mais sofisticada de *phishing*, com foco específico a organizações ou indivíduos. Assim como no *phishing*, o atacante

As IECs exigem proteção específica, incluindo o setor de saúde e a indústria farmacêutica, agora ainda mais importantes em face da Pandemia da COVID-19. Segundo a análise, os principais tipos de ameaças sofridos são ataques de *phishing*, ataque de negação de serviço (*Denial of Service – DoS*), vazamento de dados, espionagem e interrupção de serviços, ressaltando-se o desafio imposto pelos dispositivos de Internet das Coisas (IoT). Tendo em vista que ataques às IECs figuram na lista das maiores ameaças à segurança nacional, a sua proteção exige uma larga abordagem, incluindo avaliação de riscos; planejamento, coordenação e desenvolvimento de ações de segurança cibernética; e definição de normativos e requisitos metodológicos para implementação de ações de segurança cibernética (BRASIL, 2020a).

Importante notar que a análise revela algumas constatações emergidas do processo de elaboração do E-Ciber, dentre as quais: inexistência de arcabouço próprio e abrangente de segurança cibernética; os normativos, orientações e padrões em vigor não foram devidamente absorvidos pelos setores público e privado; recursos de segurança cibernética evoluíram; necessidade de incrementar a articulação de representantes de IECs; modelos precisam compreender os riscos e avaliar o custo de um incidente; e a necessidade das organizações criarem uma cultura de segurança cibernética (BRASIL, 2020a).

A última parte do eixo refere-se à relevância das Agências Reguladoras, lembrando a existência de regulamentação setorial emitida pelo Banco Central do Brasil[39] para estimular a adoção de procedimentos de segurança cibernética no seu setor com determinações relacionadas à criação de estrutura de governança de segurança nas empresas de IECs; à realização de auditorias anuais nessa seara; à adoção de práticas e requisitos no desenvolvimento de ações, produtos e projetos; à criação de CSIRTs por empresas e setor; à adoção de mecanismos de compartilhamento de informações; à capacitação contínua de colaboradores; à notificação do CTIR Gov em caso de incidentes; à notificação dos consumidores; à promoção de campanhas de conscientização; à exigência para a cadeia de suprimentos; e à elaboração de planos de resposta e recuperação a incidentes (BRASIL, 2020a).

Especificamente quanto aos procedimentos de segurança cibernética, aspectos técnicos e operacionais podem ser detalhados pelas Agências Reguladoras com o apoio do

---

utiliza-se de impersonificação e de informações disponíveis nas redes sociais para personalizar a sua mensagem ou impersonificar usuários, a fim de que a vítima se sinta compelida a cair no golpe (ENISA, [201?]).

[39] Resolução n.º 4.658, de 26 de abril de 2018, que dispõe sobre a política de segurança cibernética e sobre os requisitos para a contratação de serviços de processamento e armazenamento de dados e de computação em nuvem a serem observados pelas instituições financeiras e demais instituições autorizadas a funcionar pelo Banco Central do Brasil. Disponível em: https://www.in.gov.br/materia/-/asset_publisher/Kujrw0TZC2Mb/content/id/12378900/do1-2018-04-30-resolucao-n-4-658-de-26-de-abril-de-2018-12378896. Acesso em: 14 fev. 2021.

GSI/PR. Adicionalmente, as políticas de segurança cibernética, que serão elaboradas pelos gestores das IECs, devem: focar em resultado e na continuidade dos serviços; ser flexíveis e baseadas em análises de riscos; e estar alinhadas a padrões nacionais e internacionalmente reconhecidos, inclusive no tocante aos processos de certificação, os quais devem ser equilibrados e transparentes (BRASIL, 2020a).

Finalizada a apresentação dos três temas que compõe o eixo temático de proteção e segurança, caminha-se à descrição dos eixos transformadores.

3.5.3 Eixos Temáticos: Transformadores

Conforme já exposto anteriormente, a Parte II da Estratégia contempla os eixos temáticos. Os eixos relacionados à proteção e segurança foram explanados na subseção anterior. Nesta seção, passa-se a descrever os eixos que potencialmente podem transformar de forma significativa os temas em que se refletem. Dentre os quais, abriga-se quatro temas: dimensão normativa; pesquisa, desenvolvimento e inovação; dimensão internacional e parcerias estratégicas; e educação. Dessa forma, a subseção ainda se subdivide nessas quatro perspectivas, que serão estudadas na continuação.

3.5.3.1 Dimensão Normativa

Da mesma forma que os eixos temáticos de proteção e segurança, a subseção dos eixos transformadores também se subdivide em temas, sendo o primeiro deles a dimensão normativa. O crescimento exponencial de usuários e do comércio on-line expandiu a superfície para ataques e cometimentos de crimes cibernéticos, os quais lesionam os mais diferentes bens jurídicos tutelados pelo Direito Penal (BRASIL, 2020a).

Nessa esteira, esse eixo aponta vários esforços de tipificação desses crimes, tais como a Lei nº 12.737, de 30 de novembro de 2012 (BRASIL, 2012b), popularmente conhecida como "*Lei Carolina Dieckmann*" e a Lei nº 12.735, de 30 de novembro de 2012 (BRASIL, 2012a)[40], além de outras importantes leis como o MCI e a LGPD.

[40] Projeto de Lei que propunha alterar o Decreto-Lei n.º 2.848, de 7 de dezembro de 1940 - Código Penal, o Decreto-Lei n.º 1.001, de 21 de outubro de 1969 - Código Penal Militar, e a Lei n.º 7.716, de 5 de janeiro de 1989, para tipificar condutas realizadas mediante uso de sistema eletrônico, digital ou similares, que sejam praticadas contra sistemas informatizados e similares; e dá outras providências. O texto aprovado limitou-se a dispor sobre a existência de setores especializados no âmbito dos órgãos de polícia judiciária. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2012/lei/l12735.htm. Acesso em: 14 fev. 2021.

Outrossim, ressalta o desafio do estabelecimento de legislação para o ambiente virtual, especialmente em face do rápido desenvolvimento tecnológico, requerendo ação coordenada entre o setor público e a própria sociedade em geral para o avanço legislativo, não se olvidando também das normas infralegais e setoriais. Neste ponto, a análise relembra os instrumentos do DSI do GSI/PR, que desde 2008 já tinha publicado mais de duas dezenas de normas complementares e instruções normativas[41] sobre segurança da informação e segurança cibernética (BRASIL, 2020a).

Um ponto relevante é que embora exista o reconhecimento da importância da PNSI, recomenda a edição de lei específica para tratar de segurança cibernética. Essa lei teria condições de dispor sobre segurança cibernética para todos os entes da Federação, assim como para todos os setores. Ou seja, não se limitaria à APF. A análise assenta a insuficiência do arcabouço normativo existente, justamente pela abrangência e pela característica infralegal de muitos instrumentos. Além disso, recomenda que o processo de elaboração dos normativos seja multissetorial, conferindo legitimidade ao processo (BRASIL, 2020a).

Após a breve, porém assertiva, citação da imprescindibilidade do marco legal trazida na E-Ciber, move-se ao próximo eixo temático transformador, qual seja pesquisa, desenvolvimento e inovação.

3.5.3.2 Pesquisa, Desenvolvimento e Inovação

Esse eixo reconhece as transformações e os impactos na sociedade causados pela revolução tecnológica, especialmente nos campos da comunicação, interação e acesso às informações, demonstrando a importância do estímulo à pesquisa e inovação para o desenvolvimento, bem como do papel do Estado nesse contexto, especialmente na busca de crescimento econômico, inclusivo e sustentável. Nessa esteira, as ações de fomento em Pesquisa, Desenvolvimento e Inovação (PD&I) em segurança cibernética precisam ser elevadas a prioridade, com o objetivo de atrair investimento, pesquisadores e novos projetos, como por exemplo, no campo da criptologia, para incentivar soluções de segurança para o ambiente cibernético (BRASIL, 2020a).

A análise relembra o texto da E-Digital de estímulo a PD&I, especialmente em campos como microeletrônica, robótica, supercomputadores e tecnologias disruptivas, recomendando investimento em criptografia. Ademais, reconhece a existência de centros de excelência

[41] Disponíveis em: https://www.gov.br/gsi/pt-br/assuntos/dsi/legislacao. Acesso em: 14 fev. 2021.

altamente capacitados e reconhecidos, porém com pouca repercussão em termos inovação em segurança cibernética. Nesse ponto, ressalta a importância de uma indústria nessa seara, suportada por pesquisa de alto nível e com a capacidade de retenção de talentos (BRASIL, 2020a).

A falta de convergência entre projetos das universidades e as necessidades do setor produtivo em segurança cibernética demanda estreito diálogo entre setor privado e academia, recomendando-se a formação de parcerias com o Ministério da Educação para implementar programas de desenvolvimento de capacidades na educação básica. Sem ser olvidada a necessidade de desenvolvimento de projetos nas universidades alinhados às necessidades do setor produtivo, inclusive com programas de pós-graduação *stricto sensu* (BRASIL, 2020a).

Em termos de inovação, incentiva a adoção de padrões globais e voluntários de tecnologia, e, por consequência, interoperáveis, que podem servir de modelo para cooperação internacional. Como indicador relacionado à inovação, cita o Anuário de Competitividade Mundial (*World Competitiveness Yearbook)*, no qual o Brasil em 2019 figurou na quinquagésima nona posição de sessenta e três, sendo que em 2010 o país situava-se na trigésima oitava posição (BRASIL, 2020a).

No tocante aos recursos, relembra que o Fundo Nacional de Desenvolvimento Científico e Tecnológico (FNDCT) poderia ser destinado para projetos em segurança cibernética. Ainda no contexto de inovação, enfatiza a relevância de programas de apoio a *startups*, visto a centralidade do seu papel como fonte de inovação (BRASIL, 2020a).

Por fim, o último tópico deste eixo é destinado aos aspectos de segurança cibernética referentes ao 5G, recomendando requisitos mínimos de segurança para a comercialização de equipamentos vinculados às redes 5G (BRASIL, 2020a).

No curso de apresentação dos eixos transformadores, o próximo é a dimensão internacional e as parceiras estratégicas, que serão contempladas no próximo subitem.

3.5.3.3 Dimensão Internacional e Parcerias Estratégicas

A Análise desse eixo inicia com a ressalva do Brasil experimentar o fenômeno da Quarta Revolução Industrial, o qual foi contextualizado no Capítulo I. De forma análoga, a análise identifica como padrão de reconhecimento desse fenômeno a integração das tecnologias, alta interação entre realidades física e virtual e a proliferação de dispositivos de IoT, em apoio aos processos produtivos. Nesse sentindo, relata as possibilidades de ganhos de produtividade com a utilização de dispositivos de IoT, robótica avançada, impressão 3D, *Big Data*, computação

em nuvem, Inteligência Artificial, e sistemas de simulação virtual, configurando o cenário de Indústria 4.0 (BRASIL, 2020a).

Além disso, também constata a crescente incorporação de tecnologias em diversas atividades do cotidiano, fazendo com que também cresça o fenômeno da criminalidade cibernética, que por suas características é transnacional e, portanto, demanda cooperação internacional para sua efetiva persecução. Considerando a necessidade de concertação internacional para a construção de um ciberespaço seguro e confiável, recomenda que o país adote medidas de construção de confiança, buscando a cooperação, compartilhamento de informações, transparência, previsibilidade de ações, reafirmação da paz internacional e estabilidade (BRASIL, 2020a).

Internacionalmente, sustenta que o Brasil deve continuar a se pautar pelos princípios constitucionais brasileiros e valores fundamentais, considerando normativos como o MCI e LGPD, assim como as políticas de desenvolvimento da Internet no Brasil. Tendo em vista o contexto de espionagem cibernética, interceptação de dados em massa, operações ofensivas, crimes cibernéticos e ataques cibernéticos às IECs, o Brasil deve reforçar sua atuação na elaboração e revisão de instrumentos internacionais (BRASIL, 2020a).

Na mesma linha, o País deve alavancar debates e cooperação internacional nessa temática, frisando a necessidade de integração com os países Latino Americanos e o existente desejo de formalização de acordo bilaterais com o maior número de países. Ponto adicional relevante, em termos de cooperação bilateral, é o estímulo à negociação de tratados de assistência jurídica mútua, salientando o papel do GSI/PR nas negociações e no acompanhamento de dezenas de atos internacionais referentes ao tratamento de informações classificadas (BRASIL, 2020a).

Cabe relatar a ênfase nas iniciativas de compartilhamento de informações, com a recomendação de que o país também participe de esforços para construção de procedimento para compartilhamento em casos de grandes crises transnacionais e estimule setores público e privado a engajar-se com exercícios regionais e internacionais, sem se olvidar de esforços de estruturação normativa futura, como por exemplo, relacionados a padrões referentes ao 5G (BRASIL, 2020a).

Por fim, o eixo destaca o papel de parcerias estratégicas, visto que segurança cibernética é um tema transversal e que a integração e cooperação entre os vários setores trazem resultados positivos. Ademais, nenhum ator isoladamente consegue enfrentar todo os desafios colocados pelas novas tecnologias e grande parte da IEC é detida e operada pelo setor privado, cabendo, assim, ao governo o papel central de orquestração. Nesse tópico, a análise pontua o

diagnóstico de que os processos de coordenação correspondem a uma variedade de arranjos, nem sempre institucionalizados, nem vinculados a mecanismos tradicionais de regulação (BRASIL, 2020a).

Outrossim, o tema abarca uma série de instituições, adicionando grau de dificuldade ao processo de coordenação. Dessa forma, recomenda a criação de canais de comunicação adequados, para que seja feita a oitiva multissetorial, tanto para elaboração quanto para implementação de políticas no tema. Ao final, reitera que as parcerias nessa seara se baseiam em confiança, interesses e objetivos comuns, tornando-se cada vez mais relevante a organização de fóruns e reuniões, assim como mecanismos de compartilhamento de informações (BRASIL, 2020a).

Ainda resta o último eixo de transformação que aborda a questão, eixo transformador da educação, o qual não é menos importante e será examinado na próxima e última subseção.

3.5.3.4 Educação

O último eixo transformador reconhece os desafios impostos pela rápida expansão de acesso à Internet pela população brasileira conjugada à falta de cultura de segurança cibernética, revelando a importância do conceito de alfabetização digital (*digital literacy*). Assim, recomenda o desenvolvimento da cultura de segurança cibernética por meio da educação, abrangendo todos setores e níveis de ensino e abarcando a conscientização da sociedade.

Também defende a formação via educação formal e a capacitação profissional, sendo a responsabilidade por essas três perspectivas (capacitação, formação e conscientização) compartilhada entre vários atores dos setores público e privado (BRASIL, 2020a).

As iniciativas de conscientização são ferramentas fundamentais e, além de possibilitarem a compreensão sobre riscos e ameaças, estimulam a adoção de comportamento responsável e seguro pelos usuários, tendo o público amplo como alvo e devendo ser conduzidas com periodicidade. Cita como exemplo de iniciativa nos EUA o "Mês Nacional de Conscientização em Segurança Cibernética" que ocorre anualmente em outubro (BRASIL, 2020a).

Já as ações de formação são apontadas como incipientes, quando não inexistentes, nas escolas brasileiras. Mesmo no Ensino Superior não é um tópico acadêmico isolado, fazendo parte do currículo de cursos como Ciência da Computação, embora já existam iniciativas diferenciadas (BRASIL, 2020a).

Em termos de capacitação, o eixo ressalta a existência de alguns milhões de empregos não preenchidos, sendo que instituições de Ensino Superior não são capazes de formar especialistas suficientes para atender a demanda crescente do setor. Nesse ponto, recomenda a ênfase em segurança cibernética nos cursos técnicos. Estimativas apresentadas pela Associação Brasileira das Empresas de Tecnologia da Informação e Comunicação (BRASSCOM) indicam déficit de profissionais na área de quarenta e cinco mil até 2024, sendo que as especializações mais requeridas e mão de obra necessitada de forma mais imediata abarcam segurança cibernética (BRASIL, 2020a).

Dessa maneira, ações do setor público, através de parcerias multissetoriais nacionais e internacionais, para formação e capacitação de profissionais, pode garantir a força de trabalho, sendo que a retenção desses profissionais também é um desafio. Não obstante, são necessárias oportunidades para aprimoramento dos conhecimentos e desenvolvimento de novas habilidades. Ademais, a análise traz a impressionante estimativa da OCDE de que até 2021, haveria três milhões e quinhentas mil vagas específicas para o mercado de segurança cibernética, não preenchidas no mundo (BRASIL, 2020a).

Outro ponto que merece destaque é a conscientização de pequenas e médias empresas, cujas previsões as colocam como próximos alvos de ataques, inclusive em ataques à cadeia de suprimento, assim como de gestores dos setores público e privado, para conformidade e observância da LGPD. Finalmente, os últimos apontamentos fazem referência à necessidade de profissionais com capacitação contínua para o enfrentamento dos crimes cibernéticos (BRASIL, 2020a).

Com o tópico da educação finaliza-se o detalhamento dos eixos temáticos que traduzem as cinco dimensões do CMM e são a base da elaboração das dez ações estratégicas, que serão a seguir apresentadas.

3.5.4 Ações Estratégicas

Após a apresentação do diagnóstico e dos eixos temáticos (proteção e segurança; e transformadores), passa-se nesta subseção à apresentação das ações estratégicas contidas no normativo. O diagnóstico apresentado no subitem 3.5.1 e os sete eixos temáticos levaram ao estabelecimento de dez ações estratégicas, cuja materialização depende de ações de implementação dos setores público e privado, de acordo com suas competências. Nesse sentido, cada uma das dez ações é acompanhada por um rol exemplificativo de medidas e iniciativas que podem ser adotadas, a fim de concretizar a visão idealizada.

A primeira Ação Estratégia (AE) refere-se ao fortalecimento das ações de governança cibernética, englobando gestão de pessoas, atendimento de requisitos de segurança cibernética, bem como a gestão de ativos de informação. Exemplifica-se o escopo dessa AE com as seguintes ações:

a) realização de fóruns de governança;
b) criação de controles para o tratamento de informações restritas;
c) estabelecimento de requisitos mínimos de segurança cibernética para contratações públicas;
d) implantação de programas e projetos sobre governança cibernética;
e) adoção, além dos normativos de governança emitidos pelo GSI/PR, de normas, padrões e modelos de governança reconhecidos mundialmente;
f) adoção pela indústria de padrões internacionais no desenvolvimento de novos produtos desde sua concepção;
g) recomendação da adoção de soluções nacionais de criptografia;
h) intensificação do combate à pirataria de *software*;
i) adoção de soluções de segurança cibernética que abordem iniciativas integradoras;
j) designação de gestor de segurança da informação;
k) *xi*) recomendação de certificação em segurança cibernética, segundo padrões internacionais; e
l) ampliação da utilização do certificado digital (BRASIL, 2020a).

Já a segunda AE trata do estabelecimento de um modelo centralizado de governança no âmbito nacional, incluindo a criação de um sistema nacional de segurança cibernética, com as atribuições de:

a) promoção da coordenação dos diversos atores (além da APF);
b) promoção da análise conjunta dos desafios de combate à criminalidade cibernética;
c) assistência na formulação de políticas públicas;
d) criação de um conselho nacional;
e) criação de grupos de debate multissetorial sob coordenação do GSI/PR; e
f) estabelecimento de rotina de verificações de conformidade em segurança cibernética, tanto nos setores público quanto privado (BRASIL, 2020a).

Por fim, a AE também sustenta que o sistema precisa permitir a convergência dos esforços e de iniciativas, atuando complementarmente no tratamento de incidentes e conscientização da sociedade. Nesse sentido, a coordenação da segurança cibernética em

âmbito nacional fica atribuída ao GSI/PR, alinhada às ações de defesa cibernética, de responsabilidade do Ministério da Defesa (BRASIL, 2020a).

A terceira AE é de promoção de ambiente participativo, colaborativo, confiável e seguro, entre setores público e privado, bem como sociedade e academia, através de acompanhamento, contínuo e proativo, das ameaças e ataques cibernéticos, com os seguintes objetivos:

a) estímulo ao compartilhamento de informações sobre incidentes e vulnerabilidades;
b) realização de exercícios cibernéticos multissetoriais;
c) estabelecimento de mecanismos que permitam a interação e o compartilhamento de informações em diferentes níveis;
d) fortalecimento do CTIR Gov;
e) destaque para o papel dos CSIRTs nacionais;
f) aperfeiçoamento da infraestrutura nacional de investigação da criminalidade cibernética;
g) estímulo à criação e à atuação de ETIRs, inclusive com foco no uso de tecnologias emergentes;
h) emissão de alertas e recomendações; e
i) estímulo ao uso de criptografia pela sociedade em geral (BRASIL, 2020a).

A quarta AE fala de elevação do nível de proteção do Governo, instrumentalizada com as seguintes iniciativas:

a) inclusão de requisitos de segurança cibernética nas contratações do setor público;
b) aperfeiçoamento e incentivo ao uso dos dispositivos de comunicação segura do Governo;
c) aperfeiçoamento e constante atualização dos sistemas informacionais, infraestruturas e sistemas de comunicação dos órgãos públicos;
d) recomendação para que o setor público possua cópia de segurança atualizada, automática e segregada;
e) elaboração de requisitos específicos de segurança cibernética relativos ao uso de *endpoints* no setor público;
f) inclusão de requisitos relativos à gestão da cadeia de suprimentos;
g) inclusão de requisitos de segurança cibernética nos processos de desestatização quando relacionados a serviços essenciais; e
h) monitoramento da implementação dos requisitos mínimos de segurança cibernética pelos fornecedores da cadeia de suprimentos (BRASIL, 2020a).

A Quinta AE diz respeito à elevação do nível de proteção das IECs Nacionais, a fim proporcionar maior resiliência para garantir a continuidade dos serviços essenciais, com a promoção da interação entre as agências reguladoras de IEC; estímulo à adoção de ações de segurança cibernética pelas IECs; incentivo para implementação de políticas de segurança cibernética; incentivo à constituição de ETIRs; estímulo à notificação do CTIR Gov; e incentivo à participação das IECs em simulações (BRASIL, 2020a).

A sexta AE ressalta o aprimoramento do arcabouço legal sobre segurança cibernética, com a revisão e atualização dos instrumentos vigentes, assim como a elaboração de novos, a qual será materializada com a identificação e abordagem de temas não endereçados; com esforço de incluir as novas tipificações de crimes cibernéticos no Código Penal; com a elaboração de normativos sobre tecnologias emergentes; com a criação de políticas de incentivo para contratação de recursos humanos especializados em segurança cibernética; com a definição de requisitos para trabalho remoto; e com a elaboração de um anteprojeto de lei na matéria, sob coordenação do GSI/PR. Esse deve contemplar as diretrizes que permitirão promover o alinhamento macroestratégico nessa seara (BRASIL, 2020a).

A sétima AE refere-se ao incentivo ao desenvolvimento de soluções inovadoras em segurança cibernética, buscando alinhamento entre academia e as necessidades da área produtiva, e assim, incentivando pesquisa e desenvolvimento de soluções nessa seara, e, consequentemente, inovação aos produtos nacionais. Cita-se como iniciativas:

a) proposta de inclusão do tema nos programas de fomento à pesquisa;
b) incentivo à criação de centros de pesquisa e desenvolvimento específicos no âmbito do Poder Executivo federal e no setor privado;
c) viabilização de investimentos em pesquisa, por meio de fundos públicos e privados;
d) criação de programas de incentivo ao desenvolvimento de soluções;
e) estímulo à criação de *startups* com esse foco;
f) estímulo do desenvolvimento e inovação de soluções de segurança cibernética nas tecnologias emergentes;
g) incentivo à adoção de padrões globais de tecnologia, com interoperabilidade;
h) incentivo ao desenvolvimento de competências e de soluções em criptografia;
i) estímulo à pesquisa sobre o uso de inteligência espectral; e
j) estabelecimento de requisitos mínimos de segurança cibernética para o 5G (BRASIL, 2020a).

A oitava AE fala da ampliação da cooperação internacional do Brasil com o maior número possível de países e do reforço da sua posição, seguindo a tradição diplomática

brasileira. Para tanto, podem ser adotadas as medidas de: incentivo às discussões temáticas nos organismos, fóruns e grupos internacionais; ampliação do relacionamento internacional com os países da América Latina; promoção de eventos e exercícios internacionais; participação de eventos internacionais de interesse; ampliação de acordos de cooperação; ampliação do uso de mecanismos internacionais de combate à criminalidade cibernética; estímulo a iniciativas futuras de estruturação normativa (como por exemplo, as referentes ao estabelecimento de padrões de segurança para tecnologias emergentes); e identificação, estímulo e aproveitamento de novas oportunidades comerciais (BRASIL, 2020a).

A nona AE é de ampliação da parceria multissetorial em segurança cibernética, abrangendo setores público e privado, academia e sociedade, a fim de elevar o nível de segurança cibernética. Nessa AE é vislumbrada a cooperação do setor produtivo com a academia, por meio de recursos financeiros e materiais. Traduz-se nas ações de: ampliação da cooperação entre setores público e privado e academia para a implementação da E-Ciber; manutenção de ambiente colaborativo a fim de permitir o estudo e largo uso de tecnologias emergentes; estabelecimento de parcerias de incentivo do setor privado a investir em medidas de segurança cibernética; incentivo a organização de reuniões com atores relevantes; estímulo à criação de grupos de trabalho e de fóruns, caso necessário; incentivo à criação de mecanismos de compartilhamento de informações; e realização de parcerias entre todos os entes da Federação (União, Estados e municípios), Ministério Público e a academia, para a implantação de iniciativas que englobem a toda sociedade (BRASIL, 2020a).

Finalmente, a décima AE trata da elevação do nível de maturidade da sociedade em segurança cibernética, a fim de oportunizar a compreensão das ameaças e riscos no ambiente cibernético, bem como o uso seguro das tecnologias. Nessa esteira, o documento identifica as seguintes iniciativas: incentivo aos setores público e privado para realização de campanhas de conscientização internas; promoção de ações e políticas públicas de conscientização da população; inclusão do tema em todos os níveis educativos (educação infantil, ensino fundamental e ensino médio); estímulo à criação de cursos de nível superior; proposição de programas de incentivo para graduação e pós-graduação no Brasil e no exterior; fomento à pesquisa e desenvolvimento; criação de programas de capacitação continuada para profissionais dos setores público e privado; incentivo à formação de profissionais para atuação na persecução penal da criminalidade cibernética; realização de eventos de capacitação; incentivo à participação em fóruns e eventos temáticos nacionais e internacionais; aperfeiçoamento dos mecanismos de integração, de colaboração e de incentivos entre instituições de ensino superior

e setor privado; incentivo às simulações; e promoção da gestão de conhecimento, otimizando a identificação, a seleção e o uso de talentos (BRASIL, 2020a).

Concluída a análise descritiva da E-Ciber, ainda é necessário apresentar a política específica criada para o tratamento de incidentes cibernéticos, trata-se do Decreto nº 10.748, de 16 de junho de 2021, que será apresentado na sequência.

3.6 DECRETO N.° 10.748, DE 16 DE JULHO DE 2021, QUE INSTITUI A REDE FEDERAL DE GESTÃO DE INCIDENTES CIBERNÉTICOS

O Decreto n° 10.748, de 16 de julho de 2021, institui a Rede Federal de Gestão de Incidentes Cibernéticos (ReGIC), a qual será integrada obrigatoriamente pelos órgãos e entidade da APF direta, autárquica e fundacional e voluntariamente pelas empresas públicas e sociedades de economia mista federais e suas subsidiárias, acrescida da Secretaria Especial de Desburocratização, Gestão e Governo Digital do Ministério da Economia, nos termos do art. 1º e seus parágrafos (BRASIL, 2021b).

A finalidade da ReGIC está centrada no aprimoramento e na coordenação entre todos esses órgãos e entidades da APF para prevenção, tratamento e resposta de incidentes cibernéticos, e assim, aumentando a resiliência cibernética dos ativos envolvidos. Como objetivo, o Decreto expressamente fala na divulgação de medidas de prevenção, tratamento e resposta aos incidentes cibernéticos; compartilhamento de alertas sobre ameaças e vulnerabilidades; divulgação de informações de ataques; e promoção de cooperação entre os integrantes e celeridade na resposta aos incidentes (arts. 2º e 3º) (BRASIL, 2021b).

O Decreto apresenta uma série de definições, especialmente sobre as ETIRs; equipes de coordenação setorial; equipes principais; áreas prioritárias; incidente cibernético; plano de gestão de incidentes cibernéticos para a APF; e planos setoriais de gestão de incidentes cibernéticos. A participação na ReGIC dos órgãos e entidades da APF por meio das suas ETIRs é obrigatória e a coordenação da Rede será de responsabilidade do DSI do GSI/PR por meio do CTIR Gov (art. 5º) (BRASIL, 2021b).

Cumpre desde logo esclarecer que não há grande inovação para os órgãos e entidades da APF que já notificam o CTIR Gov sobre incidentes cibernéticos, sendo formalizada via Decreto uma prática já existente. No entanto, a grande inovação está centrada na atribuição de competência às agências reguladoras, ao Banco Central e à Comissão Nacional de Energia Nuclear. Essas entidades devem instituir ou designar uma equipe de coordenação setorial (ETIR Setorial), que será responsável por elaborar o plano setorial de gestão de incidentes cibernéticos;

coordenar as atividades; e centralizar as notificações de incidentes recebidas das ETIRs que estão sob a sua coordenação. Ou seja, a ETIR Setorial coloca-se como elo entre as equipes que compõe o setor e o CTIR Gov, como coordenador da ReGIC, prática inexistente no âmbito da APF, até a edição do Decreto e para qual foi estabelecido prazo de dezoito meses. Dessa forma, a estrutura setorial precisa estar implementada até janeiro de 2023, consoante arts. 13, 14 e 16 (BRASIL, 2021b).

Veja-se para esse recorte específico de entidades da APF (agências reguladoras, Banco Central e Comissão Nacional de Energia Nuclear), existe um duplo papel a ser desempenhado, visto que além de uma ETIR da entidade, a qual já reporta ao CTIR Gov e foca nas redes, sistemas e dados dessa instituição, precisará deter uma ETIR finalística que focará no negócio, ou seja, no setor regulado. Não existe previsão regulamentar sobre a obrigatoriedade de ser uma ETIR única com esses dois papéis, já havendo movimentos documentados de existência de duas ETIRs de uma mesma entidade. Essa duplicidade representa os distintos papéis que devem assumir, sendo que o setor de telecomunicações já aprovou sua opção pela existência de duas ETIRs apartadas no âmbito da Anatel[42].

Ainda sobre a ReGIC cabe mencionar que, considerando o interesse do Estado, outras entidades públicas e privadas poderão ser convidadas a integrá-la (art. 5º, § 3º). Além disso, a ETIR Setorial do ComDCiber, na condição de órgão central do Sistema Militar de Defesa Cibernética, será responsável pela articulação com o CTIR Gov, como elo do Ministério da Defesa e das Forças Singulares. Assim, a articulação desse Ministério e das Forças diretamente com o CTIR Gov cabe apenas em casos excepcionais, consoante art. 6º, § 1º (BRASIL, 2021b).

Outrossim, o Decreto ainda trata sobre o processo de adesão e seus requisitos, bem como as competências do GSI/PR; do CTIR Gov; dos órgãos e entidade que compõe a APF; das Agências Reguladoras, Banco Central e Comissão Nacional de Energia Nuclear, conforme os dispositivos dos arts. 10 a 13 do Decreto (BRASIL, 2021b).

Relacionando o Decreto com as demais políticas públicas anteriormente apresentadas, verifica-se que a PNSI no seu art. 15, VII, já estabelecia a competência dos órgãos e entidades da APF, no seu âmbito de atuação, para instituir e implementar uma ETIR, a qual deve compor a rede de ETIRs da APF, coordenada pelo CTIR Gov (BRASIL, 2018f). Já a E-Ciber, a AE de promoção de um ambiente participativo, colaborativo, confiável e seguro, entre setores público e privado, bem como sociedade, destaca o intuito de fortalecimento do CTIR Gov; de incentivo

[42] Nesse sentido ver o Plano Setorial de Gestão de Incidentes: Setor de Telecomunicações. Versão 1.0. Disponível para consulta em: https://sei.anatel.gov.br/sei/modulos/pesquisa/md_pesq_documento_consulta_externa.php?8-74Kn1tDR89f1Q7RjX8EYU46IzCFD26Q9Xx5QNDbqYFCya2oAzHQYNhzkRRsnLjD-tN64mWeskgcU_hr34jetvMQ5TiPf52bMeBtGks3PGeZDvuAiDx4c81YqwzKpgd. Acesso em: 31 dez. 2022.

ao estabelecimento e atuação de ETIRs; de ressaltar o papel dos CSIRTs nacionais; de estímulo ao compartilhamento de informações; de estabelecimento de mecanismos que permitam a interação e o compartilhamento; etc (BRASIL 2020a).

Na mesma linha, a AE que abrange a elevação do nível de proteção das IECs Nacionais salienta como iniciativas que proporcionarão maior resiliência cibernética a promoção de interação entre agências reguladoras de IEC em temas de segurança cibernética; incentivo à constituição de ETIRs; e estímulo de notificação de incidentes cibernéticos ao CTIR Gov. Dessa forma, demonstra-se que o Decreto que institui a ReGIC concretiza rede já prevista na PNSI e implementa as medidas citadas em duas ações estratégicas da E-Ciber, nos termos supracitados, colocando em prática as políticas públicas nessa seara.

Após o detalhamento das políticas relacionadas à segurança da informação e segurança cibernética, passa-se à breve apresentação de legislação e de políticas relacionadas, agrupadas na próxima seção.

3.7 LEGISLAÇÃO CORRELATA

Nessa seção, apresentar-se-á nas suas subseções, legislação que detém importante intersecção com segurança cibernética e abarca aspectos do tema, quais sejam, Política Nacional de Segurança de Infraestruturas Críticas (PNSIC), Estratégia Nacional de Segurança de Infraestruturas Críticas (ENSIC), Plano Nacional de Segurança de Infraestruturas Críticas (PLANSIC) e LGPD.

3.7.1 Política Nacional de Segurança de Infraestruturas Críticas

A primeira legislação relacionada a ser apontada é o Decreto nº 9.573, de 22 de novembro de 2018, que aprova a PNSIC (BRASIL, 2018d). Embora não seja um tema exclusivo de segurança cibernética, a proteção das IECs tem uma intersecção bastante importante com a temática da segurança da informação e da segurança cibernética. É justamente por isso que a menção às IECs figura na E-Digital, na PNSI, na E-Ciber e, mais recentemente, na ENSIC, também se configurando como um módulo da ENSI (BRASIL, 2020f).

Nos termos do art. 1°, § 1°, I, da PNSIC, IECs são definidas como "*instalações, serviços, bens e sistemas cuja interrupção ou destruição, total ou parcial, provoque sério impacto social, ambiental, econômico, político, internacional ou à segurança do Estado e da sociedade*". Compete ao GSI/PR o acompanhamento dos assuntos relacionados às IECs no âmbito da APF,

cabendo aos órgãos e entidades (APF direta, autárquica, fundacional e empresas estatais que dependam de recurso do Tesouro Nacional) a adoção de ações que promovam a segurança dessas infraestruturas (arts. 2° e 3° do Decreto) (BRASIL, 2018d).

Deve-se ter presente que a PNSIC extrapola as esferas de segurança da informação e segurança cibernética, uma vez que aborda a proteção dessas infraestruturas sob todas as perspectivas, ou seja, segurança cibernética é apenas mais uma faceta de riscos e ameaças a serem considerados.

É de extrema importância compreender que a segurança das IECs abrange, como ressaltado, todos as esferas, inclusive de proteção física. Cita-se, por exemplo, a proteção física de cabos marinos, de antenas de telefone móvel, de estações de tratamento de água, de estações de distribuição de energia elétrica e de radares de controle aéreo. No entanto, a preocupação da perspectiva de proteção cibernética dessas infraestruturas é crescente, tendo em vista o aumento dos riscos dessa esfera, especialmente causados pela transformação digital que se reflete em todas as infraestruturas.

Não é possível pensar em uma IEC que não tenha processos de digitização e digitalização associados e, portanto, vulneráveis aos riscos cibernéticos. Para demonstrar a exploração de vulnerabilidade em IECs, não limitadas ao setor de telecomunicações, relaciona-se o caso da estação de tratamento de água na Flórida, nos EUA. Nesse ataque, os níveis de componentes químicos foram alterados, com aumento tóxico dos níveis de hidróxido de sódio[43]. Outro exemplo recente também vem do solo americano, com a interrupção do oleoduto da *Colonial Pipeline Company*[44].

Dessa maneira, embora a proteção física seja necessária, pois um ataque físico poderia, por exemplo, causar os mesmos efeitos alcançados pelos ataques cibernéticos supracitados, não é mais necessária qualquer proximidade física para perpetrar um ataque. Agora uma infinidade de ataques pode ser realizada à distância, e, portanto, essa nova conjuntura demanda novas ações e estratégias, a fim de gerir adequadamente esses novos e crescentes riscos.

Voltando-se à PNSIC, o art. 2° estabelece os seguintes princípios: a prevenção e precaução com base em análise de riscos; integração multissetorial; redução de custos no investimento em segurança; e salvaguarda do interesse da defesa e da segurança nacional. Já os

---

[43] Maiores detalhes sobre o ataque podem ser consultados na revista especializada *Wired*, "*A Hacker Tried to Poison a Florida City's Water Supply, Officials Say*", de fevereiro de 2021. Disponível em: https://www.wired.com/story/oldsmar-florida-water-utility-hack/. Acesso em 18 dez. 2022.

[44] Da mesma forma, o caso do ataque à *Colonial Pipeline Company* pode ser consultado na matéria da *Wired* de maio de 2021, "*The Colonial Pipeline Hack Is a New Extreme for Ransomware*", disponível em: https://www.wired.com/story/colonial-pipeline-ransomware-attack/. Acesso em 18 dez. 2022.

objetivos estão expressos no art. 3° e abrangem a prevenção de eventual interrupção e, em caso de ocorrência, a redução dos seus impactos; o estabelecimento de diretrizes e instrumentos para salvaguardar IEC indispensáveis à segurança nacional; integração de dados sobre ameaças, tecnologias de segurança e gestão de riscos; identificação das relações de interdependência; conscientização sobre a segurança das IECs; e estabelecimento e prevalência da defesa e segurança nacional na proteção, conservação e expansão de IEC (BRASIL, 2018d).

Além disso, a PNSIC estabelece as seguintes diretrizes no art. 4°: integração com outras políticas de Estado; cooperação entre órgãos e entes da Federação nas ações de implementação; integração com o Sistema Brasileiro de Inteligência; incentivo à cooperação e à realização de parcerias entre setores público e privado, a fim de elevar o nível de segurança das IECs; promoção do intercâmbio de conhecimentos entre órgãos e entidades público e privadas das áreas prioritárias de IECs; acompanhamento do funcionamento das IECs; e atualização das atividades de segurança de IECs, nos âmbito nacional e internacional (BRASIL, 2018d).

De maneira semelhante à PNSI, a PNSIC é constituída de alguns instrumentos: ENSIC; PLANSIC; e Sistema Integrado de Dados de Segurança de Infraestruturas Críticas (art. 5°, I, II e III). Especificamente quanto à ENSIC, a PNSIC define que o instrumento identificará os principais desafios, com a definição dos eixos estruturantes e dos objetivos estratégicos (art. 6°), servindo de orientação estratégica e de referência para a formulação do PLANSIC (art. 7°) (BRASIL, 2018d).

Já o PLANSIC deve abordar as orientações para implementação de segurança e os fundamentos para elaboração de planos setoriais e atribuição de responsabilidades (art. 8°), definindo áreas prioritárias de aplicação da PNSIC; prevendo o envolvimento de todos entes da Federação e sociedade; atribuindo responsabilidades; estabelecendo requisitos de inserção de dados no Sistema Integrado; e definindo prazo de sua revisão (art. 9°) (BRASIL, 2018d).

O Sistema Integrado tem como objetivo o registro das condições de segurança das IEC, incluindo coleta, tratamento, armazenamento e recuperação das informações. Ademais, além de cadastro, o sistema conterá metodologia de seleção e priorização, bem com os níveis de riscos, auxiliando nas decisões relacionadas à segurança e na elaboração de relatórios (art. 10, 11 e 12), cuja competência de implementação e gestão é do GSI/PR (art. 14). Por fim, a PNSIC estabelece que compete à CREDEN analisar, discutir e propor ao Presidente da República a ENSIC e o PLANSIC, no prazo de dois anos da publicação da PNSIC (art. 14) (BRASIL, 2018d).

Continuando no esforço de correlacionar os instrumentos relacionados, será apresentada no próximo item a ENSIC que busca traduzir os princípios da PNSIC em ações estratégicas para orientar a sua implementação.

3.7.2 Estratégia Nacional de Segurança de Infraestruturas Críticas

A ENSIC é um dos instrumentos da PNSIC, que foi brevemente apresentada no item anterior, e também um dos módulos da ENSI, visto que além do módulo referente à segurança cibernética, instrumentalizado na E-Ciber, a segurança das IECs também é um dos outros quatro módulos, nos termos do art. 6°, III, da PNSI (Brasil, 2018f).

A ENSIC foi aprovada pelo Decreto nº 10.569, de 9 de dezembro de 2020, e sua introdução destaca o papel essencial das IECs para a segurança e soberania nacionais, demandando esforço conjunto do Estado e da sociedade para sua implementação. A Estratégia cita expressamente, porém não taxativamente, cinco setores: comunicações, energia, transporte, finanças e águas. Ademais, aponta que desde os atentados terroristas aos Estados Unidos, ocorridos em 11 de setembro de 2001, a segurança dessas infraestruturas passou a ser tendência mundial (BRASIL, 2020f).

Nacionalmente os ataques realizados por uma organização criminosa contra instalações no Estado de São Paulo em 2006 impulsionaram o tema, cabendo à CREDEN "*aprovar, promover a articulação e acompanhar a implementação dos programas e ações cujas competências ultrapassem o escopo de apenas um Ministério*" no tocante às IECs[45] e ao GSI/PR o acompanhamento de "*assuntos pertinentes às infraestruturas críticas, com prioridade aos relacionados à avaliação de riscos*"[46].

Nessa esteira, o GSI/PR instituiu Grupos Técnicos no âmbito da CREDEN para as áreas prioritárias (expressamente mencionadas na ENSIC), que além de representantes de órgãos e entidades, pode contar com especialistas, com as seguintes atribuições: melhoria contínua do processo de identificação e classificação de IECs; identificação de vulnerabilidades e ameaças; e medidas de controle para redução dos riscos (BRASIL, 2020f).

Além de detalhar os princípios da PNSIC, a ENSIC apresenta os desafios para que os objetivos da PNSIC sejam alcançados, tratando-se se texto de abordagem abrangente, para

[45] Art. 2°, II, "*j*" do Decreto n.° 9.819, de 3 de junho de 2019, *Op. Cit*.
[46] Art. 10, XI, da Lei n.º 13.844 (BRASIL, 2019b). A competência foi mantida com a Medida Provisória n.º 1.154, de 1º de janeiro de 2023 (BRASIL, 2023a).

aplicação a vulnerabilidades e ameaças de toda ordem. A temática da segurança cibernética aparece de forma bastante tímida ao ser mencionada como desafio a "*implementação de tecnologias e dispositivos voltados para a segurança da informação, com o objetivo de permitir o compartilhamento seguro de dados sobre infraestruturas críticas*" (BRASIL, 2020f).

Veja-se que a menção à segurança da informação está restrita às tecnologias e dispositivos utilizados para o compartilhamento seguro de dados, sem qualquer outra menção à segurança da informação e à segurança cibernética dessas infraestruturas como desafios de implementação da PNSIC.

A ENSIC apresenta quatro eixos estruturantes: articulação institucional; conscientização e capacitação; fomento às ações; e gestão de dados e informações, os quais são desmembrados em objetivos estratégicos, que representam o foco para direcionamento dos esforços de implementação, e iniciativas estratégicas, para emprego efetivo desses esforços (BRASIL, 2020f).

Com relação ao último eixo estruturante, Gestão de Dados e Informações, tem-se três objetivos estratégicos. O primeiro deles versa sobre a promoção tanto nos setores público e privado da geração, disponibilização e atualização periódica de dados sobre IEC de forma íntegra, consistente e padronizada. Esse objetivo subdivide-se nas seguintes iniciativas estratégicas: *i*) orientação da coleta e armazenamento de dados; e *ii*) acompanhamento da evolução da segurança (BRASIL, 2020f).

Já o segundo objetivo versa sobre o desenvolvimento de sistema dedicado para gestão de informações de IECs, desmembrando-se também em duas iniciativas: disposição de um sistema dedicado central; e promoção do compartilhamento de informações. Por fim, o último objetivo estratégico trata especificamente do incentivo à adoção de recursos e procedimentos para a segurança cibernética das IECs, traduzindo-se em duas iniciativas estratégicas: estímulo aos responsáveis por IECs para ampliação de investimentos em recursos avançados de segurança cibernética; e orientação às IECs para atendimento da E-Ciber, especialmente à quinta AE (BRASIL, 2020f).

Cabe relembrar que a quinta AE destina-se exclusivamente à elevação do nível de proteção das IECs Nacionais, com o fim de proporcionar maior resiliência para garantir a continuidade dos serviços essenciais. Nessa esteira, retoma-se que propõe ações como promoção de interação entre as agências reguladoras de IEC; estímulo à adoção de ações de segurança cibernética pelas IECs; incentivo para implementação de políticas de segurança cibernética; incentivo à constituição de ETIRs; estímulo à notificação do CTIR Gov; e incentivo à participação das IECs em exercícios cibernéticos (BRASIL, 2020a).

Dessa forma, embora a introdução, o detalhamento dos princípios da PNSIC e os desafios da ENSIC não abordem questões específicas de segurança cibernética, o terceiro objetivo do Eixo Estruturante de Gestão de Dados e Informações, e as suas duas iniciativas estratégicas, expressamente abarcam segurança cibernética e vinculam a ENSIC à E-Ciber, guiando o emprego efetivo dos esforços.

Salienta-se que os eixos estruturantes e os objetivos e iniciativas estratégicos devem orientar a elaboração do PLANSIC, fase executiva de implementação da PNSIC, consoante disposições finais da ENSIC e dos arts. 8° e 9° da PNSIC (BRASIL, 2020f).

Nesse sentido, a fim de finalizar o ciclo relacionado à implementação da política pública associada à segurança das IECs, o próximo item aborda justamente o PLANSIC, que foi aprovado em setembro de 2022, e busca a operacionalização das ações estratégicas elencadas na ENSIC.

3.7.3 Plano Nacional de Segurança de Infraestruturas Críticas

O Decreto nº 11.200, de 15 de setembro de 2022, aprovou o PLANSIC, um dos instrumentos da PNSIC, responsável pelo desdobramento dos objetivos e iniciativas estratégicos contidos na ENSIC. A elaboração do PLANSIC foi expressamente determinada pelo PNSIC, cujo art. 13 determinava à CREDEN analisar, discutir e propor ao Presidente da República o texto, no prazo de dois anos, a contar da publicação da PNSIC, em 23 de novembro de 2018. Aponta-se assim, um intervalo de quase trinta e quatro meses entre as publicações da PNSIC e do PLANSIC (BRASIL, 2018d; 2022a).

Nos termos da ENSIC, o PLANSIC deve contemplar as ações que serão adotadas para a concretização das iniciativas estratégicas previstas na Estratégia, com a identificação da(s) entidade(s) e/ou órgão(s) responsável(is), bem como mecanismos de acompanhamento das ações. Nesse sentido, denota-se inicialmente uma importante diferença de outros normativos relacionadas aqui já referidos, visto que o PLANSIC é o primeiro documento que especifica a responsabilidade para cada ação estratégica, identifica o responsável, estabelece o prazo e a meta associada (BRASIL, 2022a). Tal prática certamente possui mérito próprio visto que a clara e inequívoca atribuição dos responsáveis, bem como a estipulação de prazos e metas, auxilia o processo de implementação e de acompanhamento das ações relacionadas à proteção e resiliência das IECs, também promovendo a transparência e facilitando o controle social.

O PLANSIC destaca a criação de um Sistema Integrado de Dados de Segurança de Infraestruturas Críticas, o qual viabilizará o monitoramento e acompanhamento permanente das

IECs do país, a partir de visão setorial. O articulador do tema de segurança de IECs é o GSI/PR, o qual irá orientar o desenvolvimento e implantação do sistema, que abrangerá metodologias de identificação; compartilhamento de informações e alertas de riscos; e análise de riscos e interdependências (BRASIL, 2022a).

Ademais, o PLANSIC detalha as atribuições do GSI/PR, que deve realizar o acompanhamento do tema; implementar e gerir o Sistema supramencionando; promover a cooperação nacional e internacional nas atividades com pertinência temática; articular e cooperar com setores público e privado na identificação dessas infraestruturas; coordenar os grupos técnicos; realizar visitas técnicas; e integrar grupo de gerenciamento de crise para tratamento de eventos relevantes (BRASIL, 2022a).

O PLANSIC também atribui aos Ministérios responsáveis pelas áreas prioritárias (águas; energia; transporte; comunicações; finanças; biossegurança e bioproteção; e defesa) a elaboração de planos setoriais, em cooperação com setores público e privado, e a implementação das ações estratégicas de sua responsabilidade, sob pena de responsabilização (BRASIL, 2022a).

Em termos de atribuições, o PLANSIC também lista o rol da Agência Brasileira de Inteligência (ABIN), no sentido de cooperar para a proteção das IECs; e monitorar e realizar o enfrentamento eficaz de ações adversas, bem como dos demais órgãos e entidades do setor público federal de participar dos esforços nas três esferas de governo e cooperar na execução e planejamento das atividades (BRASIL, 2022a).

Voltando-se aos planos setoriais, esses instrumentos serão elaborados pelo Ministérios para as áreas prioritárias de IECs, com conteúdo mínimo listado no PLANSIC. Cabe a ressalva de que o PLANSIC expressamente menciona a necessidade de alinhamento desses planos ao previsto na E-Ciber e legislação correlata (BRASIL, 2022a).

Um ponto de destaque é a expressa menção no texto do Plano da busca de cooperação entre os a APF e os governos estaduais, distrital e municipais para o planejamento e execução de atividades e programas, assim como para a elaboração dos respectivos planos, para os quais destinam uma parte específica que orienta o desenvolvimento desse instrumento. Somando-se à perspectiva de abrangência, o Plano também busca fomentar o incentivo ao engajamento do setor privado e da academia, enfatizando que a sociedade civil e os cidadãos poderão apoiar as atividades nessa seara (BRASIL, 2022a).

O PLANSIC enfrenta a questão do gerenciamento da segurança dessas infraestruturas, endereçando a avaliação, acompanhamento e a resposta a incidentes, e, por fim, aponta as ações estratégicas com os respectivos prazos (contados da publicação do Decreto) e metas, além da

indicação do órgão da APF responsável. As ações estratégicas focam no estabelecimento da governança da segurança das IECs; na conscientização e capacitação dos atores; e em sistema de gestão de dados e informações. Antecipa-se que, naturalmente, o PLANSIC manteve os eixos estruturantes e os objetivos estratégicos listados na ENSIC, porém apresenta as iniciativas estratégicas da ENSIC com novos contornos e detalhamentos, porém sem alteração da sua essência (BRASIL, 2022a).

Por exemplo, no eixo estruturante de articulação institucional da ENSIC, o objetivo estratégico de promoção de integração e articulação entre setores público e privado, para troca de informações e realização de ações conjuntas, desdobra-se na iniciativa estratégica de propiciar as trocas de informações, visando inclusive a orientação do planejamento futuro, no âmbito do Sistema de Governança de Segurança de Infraestruturas Críticas (BRASIL, 2020f). Já no PLANSIC, esse mesmo objetivo estratégico desdobra-se em quatro iniciativas estratégicas:

a) estabelecimento de protocolo de intercâmbio de informações;
b) estabelecimento de normativos que internalizem o protocolo de intercâmbio de informações;
c) estabelecimento de canal de comunicação para fornecimento de informações do Programa Vigidesastres[47] ao Comitê Gestor de Segurança de Infraestruturas Críticas (CGSIC), quando envolver infraestruturas críticas; e
d) estabelecimento de canal de comunicação para fornecimento de informações do Centro Nacional de Gerenciamento de Riscos e Desastres ao CGSIC (BRASIL, 2022a).

Interessante notar que o PLANSIC traz um rol de trinta e cinco ações estratégicas com prazos de implementação que variam de um mês a quatro anos. Nota-se que a única ação que seria implementada dentro do mandato do governo responsável pela política pública seria a indicação, no prazo de trinta dias, pelos diversos Ministérios, dos responsáveis dos respectivos órgãos internos que deverão implementar e prestar contas sobre a execução das ações que lhes foram atribuídas pelo Plano (BRASIL, 2022a).

Mais da metade das ações listadas tem como prazo de duração prevista o final do próximo mandato, visto que dezessete ações têm prazo de implementação de quatro anos e uma

[47] Para mais informações sobre o Programa Vigidesastres, consultar página dedicada do Ministério da Saúde, disponível em: https://www.gov.br/saude/pt-br/composicao/svs/saude-ambiental/vigidesastres/vigidesastres. Acesso em: 24 out. 2022.

ação tem prazo de implementação de três anos. Para este último caso, a ação é justamente o estabelecimento de protocolo de cooperação com as agências reguladoras, ou, na sua inexistência, com operadores das IECs, para compartilhamento de informações, abrangendo dados dessas infraestruturas e eventuais ameaças. A respectiva meta é o estabelecimento do protocolo entre Ministério e regulador ou operador (BRASIL, 2022a).

Embora o PLANSIC seja o primeiro instrumento que detalhe prazos, responsabilidade e metas, a sua edição no final do mandato do governante traz uma carga de incerteza quanto à sua implementação. A troca de governo confirmada pelos resultados das eleições presidenciais de 2022 poderia, por si só, provocar alterações importantes e provocar um retrocesso no esforço realizado de edição da PNSIC, ENSIC e, agora, o PLANSIC. Nota-se a sua aprovação intempestiva em relação ao mandato que o legitima, uma vez que se trata de política pública, sendo que os desdobramentos serão percebidos somente após a conclusão desse trabalho.

Em relação à segurança cibernética, cumpre exemplificar a Ação Estratégica 2.2.5., dentro do eixo estruturante de conscientização e capacitação, a qual estipula a participação de dois ou mais setores (áreas prioritárias de IECs) no EGC. Importa ressaltar que essa meta já está atendida desde a primeira edição do EGC ocorrida em 2018, com a participação do setor e defesa e financeiro (LIMA E SILVA, 2020). Portanto, a meta só pode ser compreendida como a continuação do engajamento dos setores nessas atividades, as quais continuam a ser identificadas como responsabilidade do Ministério da Defesa nos termos do PLANSIC, porém sem trazer qualquer novidade ou efetividade em termos de elevação dos níveis de conscientização.

Ademais, o Objetivo Estratégico da ENSIC que incentiva a adoção de recursos e procedimentos voltados para a segurança cibernética nas IECs é traduzido em duas AE. A primeira diz respeito à realização de ações de conscientização sobre a importância do investimento em prevenção, com o objetivo de minimizar os custos decorrentes de ataques cibernético. Já a segunda, ao estabelecimento de um protocolo de integração entre o Sistema Integrado de Segurança de Infraestruturas Críticas e o CTIR Gov. Esse protocolo deve ser desenvolvido pelo GSI/PR no prazo de dois anos (BRASIL, 2022a).

Veja-se que as disposições expressamente relacionadas à segurança cibernética são bastante tímidas no PLANSIC e, suas metas insuficientes, visto que as ações de conscientização, por exemplo, têm como objetivo a realização de uma "*ação anual realizada por meio de inserção da temática em palestras, simpósios, apresentações e outros*", sendo de responsabilidade do GSI/PR (BRASIL, 2022a). Ou seja, basta que em algum evento do GSI/PR seja realizada uma palestra e a meta estaria alcançada, o que reflete uma total desconexão com

os riscos que as ameaças cibernéticas impõem às IECs, bem como com o papel da conscientização na prevenção dos incidentes e com as previsões da E-Ciber.

Após a breve explanação sobre o PLANSIC, passa-se à uma síntese da Lei Geral de Proteção de Dados, a fim de correlacioná-la com o tema.

3.7.4 Lei Geral de Proteção de Dados

A última legislação a ser citada no presente capítulo, porém não menos importante, é a LGPD, aprovada pela Lei nº 13.709, de 14 de agosto de 2018 (BRASIL, 2018c), com alterações da Lei nº 13.853, de 8 de julho de 2019 (BRASIL, 2019c), e da Lei nº 14.460, de 25 de outubro de 2022 (BRASIL, 2022b), já mencionada ao longo da apresentação de instrumentos anteriores. Em que pese os campos da proteção de dados pessoais e da segurança cibernética não se confundam, possuem uma área clara de intersecção (WIMMER, 2021).

Nesse sentido, salienta-se que um dos princípios de tratamento de dados pessoais, legalmente definidos como "*informação relacionada a pessoa natural identificada ou identificável*"[48] é a segurança. Esse princípio é definido, nos termos do art. 6°, VII da LGPD, como "*utilização de medidas técnicas e administrativas aptas a proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou difusão"*. Ademais, o Capítulo VII da Lei é destinado a tratar da segurança e das boas práticas (BRASIL, 2019d).

Dessa maneira, ao expressamente reconhecer segurança como um dos princípios do tratamento de dados pessoais e determinar que agentes de tratamento devem adotar as medidas de segurança aptas para a proteção desses dados, a LGPD reconhece a estreita relação desses campos, visto que não há como falar em proteção de dados, sem falar da segurança dos mesmos, tanto em termos de segurança da informação, quanto em termos de segurança cibernética. Reitera-se que a primeira refere-se à ações que buscam assegurar os atributos da informação (disponibilidade, integridade, confidencialidade e autenticidade) e a última, ações voltadas para a segurança das operações, a fim de que os sistemas tenham condições de resistir a incidentes capazes de comprometer a segurança da informação desses dados e dos serviços viabilizados por esses sistemas, consoante definições do Glossário do GSI/PR (BRASIL, 2019d).

Portanto, a observância das disposições legais da LGPD promove a segurança da informação e a segurança cibernética, as quais, por sua vez, promovem uma faceta da proteção

[48] Art. 5°, I, da LGPD (BRASIL, 2022a).

de dados pessoais. No entanto, cumpre salientar que a proteção de dados pessoais não se limita à manutenção dos atributos da informação.

Ressalta-se também que a LGPD impõe uma série de obrigações relacionadas ao tratamento de dados, inclusive com a previsão de sanção administrativa de multa simples de até 2% (dois por cento) do faturamento da pessoa jurídica, nos termos do art. 52, II, da LGPD, além de diversas outras sanções (BRASIL, 2019d). Dessa maneira, a LGPD carrega um incentivo para o tratamento legal dos dados pessoais, o que pressupõe a observância dos princípios de tratamento.

Assim, a existência de marco legal de proteção de dados pessoais contribui sobremaneira para a segurança cibernética, como campos que se reforçam mutuamente, sendo inclusive mensurada no questionário do GCI, que busca medir o desenvolvimento de capacidades dos países em segurança cibernética, apresentado no subitem 2.2 do Capítulo II da tese. Na mesma esteira, existência de legislação relacionada à proteção de dados pessoais também é valorada no âmbito do CMM, que foi detalhado no subitem 2.3 do Capítulo II.

Com essa breve, porém importante menção à LGPD, encerra-se o ciclo de descrição do arcabouço brasileiro destinado a endereçar segurança cibernética, direta ou indiretamente.

3.8 CONCLUSÕES PARCIAIS

O presente Capítulo apresentou um histórico do desenvolvimento do arcabouço brasileiro em matéria de segurança cibernética, narrando as políticas específicas e as que possuem estreita relação com a temática. Tomou-se como ponto de partida os anos 2000, quando os temas de segurança da informação e segurança cibernética começam a ganhar monta em face da ampliação do acesso à Internet.

Esse panorama permitiu identificar, domesticamente, períodos de maior atividade e desenvolvimento de esforços, bem como períodos em que houve claramente um retrocesso no avanço do tema, o que pode ser exemplificado na edição de determinadas políticas públicas. Antecipa-se como dois exemplos claros de retrocesso, a aprovação da Política Nacional de Segurança da Informação (PNSI) e da Estratégia Nacional de Segurança Cibernética (E-Ciber) por decreto presidencial, com as limitações inerentes ao instrumento, mesmo que involuntárias. Aqui cabe ressaltar que, documentadamente, a PNSI estava sendo concebida como projeto de lei, consoante Estratégia Brasileira para a Transformação Digital (E-Digital). Transcorridos mais de quatro anos da PNSI e da E-Digital, subsiste o debate sobre o marco legal.

Foi realizado um percurso de mais de duas décadas. Narrou-se os marcos em matéria de defesa nacional, quais sejam, a Política Nacional de Defesa, a Estratégia Nacional de Defesa e o Livro Branco de Defesa. Conquanto seja positiva a inclusão dos aspectos de segurança cibernética nos textos, é forçoso concluir que a abordagem é extremamente tímida diante dos riscos e desafios associados. Os textos limitam-se a alertar que o tema transcende à dicotomia civil e militar, e, portanto, demandam uma coordenação de esforços e interlocução permanente de ambas as esferas. Ademais, o texto também pontua questões relacionadas à dependência tecnológica e desenvolvimento, especialmente em face da emergência das tecnologias disruptivas, como o 5G.

Além da esfera de defesa, foram apresentados os outros documentos da perspectiva civil, os quais expõem as diversas políticas públicas, que diretamente endereçam o tema ou com ele detêm importante intersecção. Nesse sentido, iniciou-se com uma abordagem ampla de transformação digital, contextualizando segurança cibernética nessa perspectiva mais abrangente de eixo habilitador da transformação na E-Digital.

Nesse instrumento, um marco legal nacional em segurança cibernética e a necessidade de uma instituição nacional responsável são apontados em uma das suas ações estratégicas. Já na E-Digital atualizada para o ciclo 2022-2026, publicada em novembro de 2022, tem-se a reinserção da mesma ação estratégica, em face da ausência de qualquer avanço nesses quesitos. Como foi visto, o Brasil não aprovou lei na matéria e não criou ou designou órgão ou entidade como responsável nacional nessa seara, problemática que será confrontada no Capítulo IV.

Na sequência, endereçou-se os instrumentos específicos, tais como a PNSI e E-Ciber. Embora os próprios nomes indiquem nos seus títulos que são instrumentos que devam alcançar a toda nação, como antecipado, a Política e a Estratégia foram aprovadas por decreto presidencial e, portanto, têm abrangência limitada aos órgãos e entidades que compõe a Administração Pública Federal (APF).

A PNSI é o primeiro instrumento intitulado como nacional na matéria e identifica segurança cibernética como um dos subconjuntos de segurança da informação. Nos termos do Decreto nº 9.637, de 26 de dezembro de 2018, segurança da informação abarca segurança cibernética, defesa cibernética, segurança física e proteção de dados organizacionais; e ações para assegurar a disponibilidade, integridade, confidencialidade e autenticidade da informação.

São identificados como instrumentos dessa Política os Planos Nacionais e a Estratégia Nacional de Segurança da Informação. Essa será composta por módulos que devem abordar segurança cibernética, defesa cibernética, segurança das infraestruturas críticas (IEC), segurança da informação sigilosa e proteção contra vazamento de dados. Embora já transcorrido

mais de quatro anos, até a presente data, somente os módulos de segurança cibernética e de segurança das IECs foram entregues à sociedade.

O Primeiro módulo aprovado foi justamente a E-Ciber que é traduzida em dez ações estratégicas. Essas ações são:

a) fortalecimento das ações de governança cibernética;
b) estabelecimento de um modelo centralizado de governança no âmbito nacional;
c) promoção de um ambiente participativo, colaborativo, confiável e seguro, entre setores público e privado, assim como sociedade;
d) elevação do nível de proteção do Governo;
e) elevação do nível de proteção das IECs Nacionais;
f) aprimoramento do arcabouço legal sobre segurança cibernética;
g) incentivo à concepção de soluções inovadoras em segurança cibernética;
h) ampliação da cooperação internacional do Brasil em segurança cibernética;
i) ampliação da parceria em segurança cibernética, entre setores público e privado, academia e sociedade; e
j) elevação do nível de maturidade da sociedade em segurança cibernética.

No detalhamento das ações estratégicas, dois pontos de destaque entrelaçados são a necessidade de elaboração de marco legal adequado, bem como o estabelecimento de uma autoridade competente na matéria, assuntos que serão retomados em profundidade no próximo Capítulo.

Até o momento, o instrumento adotado para a PNSI e para a E-Ciber, qual seja decreto do Presidente da República, contém limitações que inviabilizam a efetividade dessas políticas. Portanto, existe uma inerente limitação que justifica a restrição da abrangência à APF e a impossibilidade do Gabinete de Segurança Institucional da Presidência da República (GSI/PR) exercer o seu indicado papel de macrocoordenador nacional. Papel esse que foi expressamente vislumbrado para o GSI/PR e, permanece, não materializado.

Também foi exposto o Decreto nº 10.748, de 16 de julho de 2021, que institui a Rede Federal de Gestão de Incidentes Cibernéticos. Essa rede formaliza a cooperação e o reporte de incidentes no âmbito da APF. Com ela, inovou-se ao buscar o diagnóstico setorial por intermédio dos órgãos reguladores (agências reguladoras, Banco Central do Brasil e Comissão Nacional de Energia Nuclear).

Para tanto, esses órgãos reguladores devem instituir uma equipe de prevenção, tratamento e resposta a incidentes cibernéticos setorial, denominada equipe de coordenação setorial. Além disso, precisam continuar a reportar sobre os incidentes sofridos pela instituição,

como entidades ou órgãos que integram a APF. Embora novamente limitado em sua abrangência, ou seja, abarcando tão somente a APF, o Decreto vale-se das competências desses órgãos reguladores para alcançar o setor privado e, assim, viabilizar um diagnóstico mais abrangente dos incidentes no país, não se restringindo aos incidentes ocorridos nos órgãos e entidades da APF.

Veja-se que ao determinar o reporte pelos órgãos reguladores, o Decreto consegue abarcar o setor privado detentor de IEC, regulado pelos órgãos reguladores federais, não se limitando assim ao setor público. Tendo em vista que o prazo de implementação setorial coincide com a finalização desse trabalho (início de 2023), não foi possível ainda avaliar sua eficácia e efetividade, que somente poderá ser examinada nos próximos anos.

Após a apresentação desses instrumentos específicos de segurança da informação, segurança cibernética e incidentes cibernéticos, cumpre aqui enfatizar um conjunto de três instrumentos relacionados à segurança das IEC. Esse conjunto é composto da Política Nacional de Segurança de Infraestruturas Críticas (PNSIC), Estratégia Nacional de Segurança de Infraestruturas Críticas (ENSIC) e Plano Nacional de Segurança de Infraestruturas Críticas (PLANSIC).

Sustentou-se que essas três políticas centradas na segurança das IECs têm uma estreita e importante conexão com segurança cibernética, visto que os riscos cibernéticos têm se tornado uma perspectiva cada mais relevante na proteção dessas infraestruturas.

Embora de forma novamente tímida, a ENSIC também expressamente inclui a problemática de segurança cibernética em duas das suas ações estratégicas. Dessa forma, duas ações estabelecem o estímulo à ampliação de investimentos em recursos avançados de segurança cibernética e orientação às IECs para atendimento da E-Ciber. Nesse último ponto, é expressamente mencionando o vínculo com a ação estratégica de elevação do nível de proteção das IECs nacionais.

Já o PLANSIC incorpora trinta e cinco ações estratégicas, com prazo de execução projetado para o próximo mandato presidencial, uma vez que trinta e quatro ações (de um total de trinta e cinco) possuem prazos de implementação que variam de um a quatro anos. Essa intempestividade do Plano, aprovado somente nos últimos meses do Governo de Jair Bolsonaro, traz incerteza quanto à sua futura implementação. Ainda sobre o plano, cabe frisar um último aspecto. Restou atestada, novamente, a timidez das previsões em face dos desafios de proteção cibernética dessas infraestruturas.

Além da segurança das IEC, outro tópico correlato e que também detém relevante intersecção com segurança cibernética é a proteção de dados pessoais. Segurança é princípio

que deve nortear o tratamento de dados pessoais e não é possível falar de proteção de dados, sem falar de segurança cibernética. Ademais, em função dos riscos associados ao tratamento de dados e, especialmente, aos potenciais danos causados aos titulares e possíveis sanções administrativas relacionadas aos incidentes cibernéticos, a Lei Geral de Proteção de Dados (LGPD) movimentou todos os setores da sociedade na proteção desse bem jurídico, motivando, assim, a adoção de medidas técnicas e administrativas de segurança da informação e de segurança cibernética. Essas medidas contribuem sobremaneira para a construção de uma cultura de segurança cibernética estipulada na E-Ciber.

Embora relativamente recente, visto que a LGPD foi aprovada em 2018, resta patente que essa legislação trouxe para os holofotes a preocupação relacionada à segurança da informação desses dados, ainda que sob o temor de eventual sancionamento da Autoridade Nacional de Proteção de Dados. Da mesma forma que as IEC, a segurança dos dados não se limita à perspectiva cibernética. No entanto, essa dimensão ganha cada vez mais importância em face da transformação digital de toda sociedade e de todos os setores da economia.

Por todo exposto, evidenciou-se o esforço de produção e estruturação das políticas pelo governo federal. No entanto, com a ressalva da LGPD, os instrumentos padecem do mesmo vício que impedem a efetiva atuação nacional coordenada no tema.

Conforme antecipado no desenho de pesquisa, retoma-se a conclusão da timidez, limitação e insuficiência do arcabouço vigente. O Arcabouço Nacional Jurídico e de Políticas Públicas é tímido na forma como enfrenta os riscos que precisam ser geridos e mitigados, bem como o crescente e dinâmico desafio imposto. É limitado visto que foi demonstrado que o Arcabouço está restrito à APF, não abarcando os demais Poderes, nem entes da Federação. Também não englobando atores não estatais, os quais, necessariamente, precisam ser engajados. E, finalmente, é insuficiente, tendo em vista que é incapaz de prover a resposta eficiente.

Antes de finalizar o Capítulo propriamente, apresenta-se uma síntese dos principais documentos estudados, a fim de facilitar a compreensão do mapeamento e análise aqui operacionalizados.

Quadro 2 - Síntese do Arcabouço Nacional Jurídico e de Políticas Públicas

Ano	Documento	Título	Contextualização do tema de Segurança Cibernética no instrumento
2000	Decreto nº 3.505, de 13 de junho de 2000	Política de Segurança da Informação nos órgãos e entidades da Administração Pública Federal	Não há qualquer menção à segurança cibernética no texto. Elenca pressupostos básicos, conceitos, objetivos e as atribuições de órgãos e entidades da APF em segurança da informação.
2010	Livro fruto do trabalho do Grupo Técnico de Segurança Cibernética (GT SEG CIBER) no âmbito da CREDEN do Conselho de Governo, a partir da Portaria do GSI/PR nº 45, de 8 de setembro de 2009	Livro Verde: segurança cibernética no Brasil	Apresenta potenciais diretrizes estratégica para a implantação de uma Política Nacional de Segurança Cibernética, expressando visões de curto (2-3 anos), médio (5-7 anos) e longo (10-15 anos) prazos. Abrange diversas dimensões como de segurança de IECs; de educação; jurídica; de cooperação internacional; social e ambiental; de Ciência, Tecnologia e Inovação; econômica; e de político-estratégia.
2015	Portaria do Conselho de Defesa Nacional n.° 14, de 11 de maio de 2015	Estratégia de Segurança da Informação e Comunicações e de Segurança Cibernética da Administração Pública Federal - 2015/2018	Não atende à recomendação do Livro Verde. Limitada às APF, não abarcando o setor brasileiro cibernético. Destaca-se os objetivos estratégicos de institucionalização do tema no planejamento e no orçamento federal; contínuo aprimoramento do quadro de pessoal na matéria; e a instituição de modelo de governança sistêmica, com coordenação executiva, acompanhamento e avaliação do órgão central (GSI/PR).
2018	Portaria MCTIC nº 1.556, de 21 de março de 2018.	Estratégia Brasileira para a Transformação Digital (E-Digital)	Confiança no Ambiente Digital é um dos eixos habilitadores da transformação. Subdivide-se em duas grandes categorias: proteção de direitos e privacidade; e defesa e segurança no ambiente digital. Enfatiza o processo de formulação de projeto de lei instituindo a PNSI, liderado pelo GSI/PR. Salienta-se como AE a edição de política nacional de segurança cibernética, contemplando a definição de uma instância nacional.
2018	Lei nº 13.709, de 14 de agosto de 2018	Lei Geral de Proteção de Dados (LGPD)	Importante intersecção. Segurança é princípio que informa o tratamento de dados pessoais. Não há como falar em proteção de dados, sem falar de segurança dos mesmos, tanto em termos de segurança da informação, quanto em termos de segurança cibernética. Observância da LGPD promove segurança cibernética.
2018	Decreto nº 9.573, de 22 de novembro de 2018	Política Nacional de Segurança de Infraestruturas Críticas (PNSIC)	Outro tema com relevante intersecção. Os riscos cibernéticos configuram uma crescente categoria de riscos que

Ano	Documento	Título	Contextualização do tema de Segurança Cibernética no instrumento
			precisam ser geridos para promover a segurança das IECs.
2018	Decreto Legislativo nº 179, de 14 de dezembro de 2018	Política Nacional de Defesa (PND)	Abordagem tímida das ameaças cibernéticas e dos desafios relacionados, com destaque à menção genérica sobre a necessidade de defesa e segurança cibernéticas e de redução da dependência tecnológica, com priorização da Ciência, Tecnologia e Inovação.
2018	Decreto Legislativo nº 179, de 14 de dezembro de 2018	Estratégia Nacional de Defesa (END)	Reconhece o setor cibernético como um dos setores tecnológicos essenciais para a Defesa Nacional, e, portanto, estratégico, o qual transcende à divisão entre civil e militar, em face da sua própria natureza. A END atribui ao Exército a responsabilidade pela liderança centralizada, coordenação e integração de vários atores e áreas do conhecimento. Salienta a capacitação de amplo espectro de emprego dual; a interoperabilidade e integração das tecnologias de comunicações das Forças Armadas; o aprimoramento da segurança da informação e das comunicações e segurança cibernética em todo o Estado; fomento à pesquisa, ao desenvolvimento e à inovação; e fortalecimento da Base Industrial de Defesa (BID), além das parcerias estratégicas.
2018	Decreto Legislativo nº 179, de 14 de dezembro de 2018	Livro Branco de Defesa Nacional	Preconiza que a proteção do espaço cibernético abarca diversas áreas, abrangendo a proteção dos seus ativos e a capacidade de atuação em rede, sendo essencialmente multidisciplinar. O objetivo da implantação do Setor Cibernético é conferir confidencialidade, disponibilidade, integridade e autenticidade aos dados que trafegam nas redes, representando um esforço de longo prazo, com reflexos positivos em outras áreas, como operacional e ciência e tecnologia. Relata os avanços alavancados pelo Exército Brasileiro, com a ativação do ComDCiber, em abril de 2016.
2018	Decreto nº 9.637, de 26 de dezembro de 2018	Política Nacional de Segurança da Informação (PNSI)	Dispõe sobre governança da segurança da informação no âmbito da APF. Segurança cibernética é apresentada como um dos quatro subconjuntos de segurança da informação. Introduz o conceito de ENSI modular, a ser composta pelos seguintes módulos: segurança cibernética; defesa cibernética; segurança das IECs;

Ano	Documento	Título	Contextualização do tema de Segurança Cibernética no instrumento
			segurança da informação sigilosa; e proteção contra vazamento de dados.
2020	Decreto nº 10.222, de 5 de fevereiro de 2020	Estratégia Nacional de Segurança Cibernética (E-Ciber)	Primeiro módulo da ENSI. Visão do Governo Federal para quadriênio 2020-2023, de tornar o Brasil um país de excelência em segurança cibernética. Apresenta como objetivos estratégicos: tornar o Brasil mais próspero e confiável no ambiente digital; aumentar a resiliência cibernética; e fortalecer a atuação brasileira internacionalmente. Os objetivos são desdobrados em 10 AEs, cabendo à APF a sua implementação. Vislumbra o GSI/PR como coordenador nacional.
2020	Decreto nº 10.569, de 9 de dezembro de 2020	Estratégia Nacional de Segurança de Infraestruturas Críticas (ENSIC)	Segundo módulo da ENSI. Embora a introdução, o detalhamento dos princípios da PNSIC e os desafios da ENSIC não abordem questões específicas de segurança cibernética, o terceiro objetivo do Eixo Estruturante de Gestão de Dados e Informações, bem como as suas duas iniciativas estratégicas, expressamente abarcam segurança cibernética e vinculam a ENSIC à E-Ciber, guiando o emprego efetivo dos esforços.
2020	Mensagem do Congresso Nacional n.° 9, de 2020	Encaminha, para apreciação, os textos da proposta da Política Nacional de Defesa, da Estratégia Nacional de Defesa e o Livro Branco de Defesa Nacional	Proposta de PND demonstra aumento da preocupação com o desenvolvimento tecnológico nacional, especialmente associado às tecnologias disruptivas (como os sistemas de comunicações móveis de quinta geração - 5G, por exemplo), e os seus reflexos no Poder Nacional. Já a proposta de END mantém as proposições vigentes, limitando-se a incluir a necessidade de conclusão do Sistema Militar de Defesa Cibernética, tanto em termos de estrutura, quanto em termos de marco legal. Por fim, a minuta do Livro Branco preserva o conteúdo aprovado em 2018 nessa seara.
2021	Decreto n.° 10.748, de 16 de julho de 2021	Rede Federal de Gestão de Incidentes Cibernéticos (ReGIC)	Formaliza prática já existente no âmbito da APF e abarca o setor privado por meio da atuação dos órgãos reguladores, os quais integrarão a rede e serão o elo de ligação entre seus regulados e o CTIR Gov.
2022	Decreto n.° 11.200, de 15 de setembro de 2022	Plano Nacional de Segurança de Infraestruturas Críticas (PLANSIC)	Identifica o responsável para cada AE, com o respectivo prazo e meta associada. Disposições específicas de segurança cibernética são bastante tímidas e, suas metas, insuficientes.

Ano	Documento	Título	Contextualização do tema de Segurança Cibernética no instrumento
2022	Lei nº 14.460, de 25 de outubro de 2022	Transforma a Autoridade Nacional de Proteção de Dados (ANPD) em autarquia de natureza especial e transforma cargos comissionados; altera as Leis nºs 13.709, de 14 de agosto de 2018 (Lei Geral de Proteção de Dados Pessoais), e 13.844, de 18 de junho de 2019; e revoga dispositivos da Lei nº 13.853, de 8 de julho de 2019.	Altera a natureza jurídica da ANPD que foi instituída como órgão da APF, integrante da Presidência da República. Transforma a ANPD em autarquia de natureza especial.
2022	Portaria MCTI nº 6.543, de 16 de novembro de 2022	Estratégia Brasileira para a Transformação Digital (E-Digital) para o Ciclo 2022-2026	Mantém a metodologia da E-Digital. Reitera como AE a instituição de uma política nacional de segurança cibernética, incluindo definição de instância nacional responsável pela articulação de um sistema nacional.
2023	Medida Provisória nº 1.154, de 1º de janeiro de 2023	Estabelece a organização básica dos órgãos da Presidência da República e dos Ministérios	Define as competências do GSI/PR. Destaca-se: coordenar as atividades de segurança da informação e das comunicações; e planejar, coordenar e supervisionar a atividade de segurança da informação no âmbito da administração pública federal, incluídos a segurança cibernética, a gestão de incidentes computacionais, a proteção de dados, o credenciamento de segurança e o tratamento de informações sigilosas.
2023	Decreto n.° 11.331, de 1° de janeiro de 2023	Aprova a Estrutura Regimental e o Quadro Demonstrativo dos Cargos em Comissão, das Funções de Confiança e das Gratificações do Gabinete de Segurança Institucional da Presidência da República	Institui no âmbito do GSI/PR a Secretaria de Segurança da Informação e Cibernética e altera a nomenclatura do DSI para Departamento de Segurança da Informação e Cibernética.

Fonte: elaborado pela autora.

Dessa forma, cumpre adentrar na perspectiva normativa e abordar a prescrição de políticas públicas em duas áreas críticas: Marco Legal e Autoridade Nacional de Segurança Cibernética, as quais buscam equacionar os problemas acima relatados e serão objeto do próximo capítulo.

4 ANÁLISE E PRESCRIÇÃO DE POLÍTICA PÚBLICA

Diferentemente dos Capítulos anteriores, o presente e último capítulo do trabalho fundamenta-se nos acúmulos dos três capítulos: marco teórico; modelos que podem assistir aos países no desenvolvimento das capacidades necessárias para mitigar riscos e maximizar as oportunidades; e Arcabouço Nacional Jurídico e de Políticas Públicas, para focar especificamente em duas áreas consideradas centrais para a governança do tema no país e que dialogam e se retroalimentam: Marco Legal e Autoridade Nacional de Segurança Cibernética.

Essas duas vertentes estão intrinsecamente conectadas, pois não é possível falar em governança institucional efetiva em segurança cibernética sem falar da existência de uma Lei, assim como não é possível implementar uma lei sem que exista a organização institucional mínima necessária. Dessa forma, com base na pesquisa, passa-se a propor uma contribuição para o estabelecimento do Marco Legal essencial e para a governança institucional de segurança cibernética no Brasil, por meio de uma Autoridade Nacional de Segurança Cibernética.

4.1 MARCO LEGAL

Retomando o diagnóstico apresentado no Capítulo III, que busca descrever o Arcabouço Nacional Jurídico e de Políticas Públicas, a elaboração do marco jurídico adequado foi expressamente indicada em dois instrumentos: E-Digital e E-Ciber. Naquela, cujo texto foi aprovado em 2018, relata-se que estava sendo gestado, à época no âmbito do GSI/PR, projeto de lei para o enfrentamento do tema. Sobre o assunto, a E-Digital traz em destaque um quadro no corpo do documento (BRASIL, 2018b, p. 41-42) com o seguinte conteúdo:

> Política Nacional de Segurança da Informação – PNSI
> O Governo federal, sob liderança do Gabinete de Segurança Institucional (GSI), está finalizando a formulação da Política Nacional de Segurança da Informação (PNSI) em forma de projeto de lei a ser apresentado ao Congresso Nacional. A PNSI enfoca a segurança cibernética pela dimensão da gestão de segurança da informação e reconhece o valor econômico e social das informações numa economia de dados.
> A Política é abertamente orientada pelo respeito aos direitos humanos e aposta na coordenação federativa, na parceria entre estado e agentes privados, na cooperação internacional e nas práticas de prevenção e educação para promover maior segurança no ambiente digital.

Ademais, a E-Digital aponta como maior desafio o estabelecimento de uma estrutura institucional adequada, também sendo necessária uma estratégia nacional abrangente e a mobilização dos diferentes níveis e esferas de governo, indicando como ponto de atenção a

proteção das IECs nacionais, incluindo tanto as infraestruturas relacionadas à conectividade, quanto as de outros setores estratégicos.

Outro quesito adicional constante da E-Digital diz respeito à implementação da estratégia e à necessidade de desenvolvimento de expertise no seio do Estado, que precisa contar com uma instância no governo federal especializada, cuja tarefa principal será promover a cooperação entre setores público e privado, indispensável para efetividade das ações nessa seara.

Especificamente ao abordar as Ações Estratégicas, repisa-se que a E-Digital relaciona a edição de uma política nacional de segurança cibernética, definindo "*uma instância nacional*" que será a responsável por articular um sistema nacional de segurança cibernética, com a envolvimento dos setores público e privado (BRASIL, 2018b, p. 43).

Como já explanado no Capítulo anterior, o projeto supracitado que vinha sendo elaborado teve seu escopo reduzido significativamente, uma vez que a proposta foi convertida em Decreto Presidencial, que aprovou a PNSI.

Posteriormente, a E-Ciber, publicada em meados de 2020, recomendou o estabelecimento de marco normativo específico (BRASIL, 2020a), que deveria ser capaz de direcionar o setor cibernético do país, envolvendo os Poderes de todos os entes da Federação, também abrangendo o setor privado e a sociedade. O texto da Estratégia expressamente salienta a insuficiência do arcabouço vigente, em razão da tipologia normativa adotada. Ou seja, as limitações são frutos da natureza dos decretos presidenciais, os quais se limitam à APF, não alcançando parte essencial para a discussão das questões relacionadas à segurança cibernética no país, qual seja, setor produtivo; demais Poderes e entes da Federação; e a sociedade.

Outrossim, a E-Ciber também apresenta outros elementos relacionados à discussão normativa, como por exemplo, a existência de um novo paradigma para a segurança do Estado, considerando que as vulnerabilidades de todos atores, inclusive dos cidadãos, podem ser exploradas como ameaça em um incidente que tenha grandes impactos e, como consequência, possa prejudicar a estabilidade das instituições nacionais. Os cenários são muitos.

Nenhum ator está imune aos incidentes e sua rede e seus dispositivos (computadores, roteadores, *smartphones*, *tablets* e quaisquer dispositivos inteligentes conectados à Internet) podem ser utilizados em um ataque cibernético. Essa exploração dar-se-á através do aproveitamento das vulnerabilidades desses equipamentos ou, até mesmo, do comportamento do usuário. Aqui cabe trazer à baila o ensinamento de Marcelo Malagutti de que "*todo o conceito de ferramentas de ciberataque é baseado na exploração de vulnerabilidades*" (2022a, p. 4-14).

Um exemplo muito comum para ilustrar a exploração de vulnerabilidades de dispositivos de usuários é a utilização desses dispositivos para amplificar os Ataques de Negação de Serviço, fazendo com que determinado serviço digital fique indisponível em face da quantidade de requisições recebidas. Essa é uma das grandes preocupações associadas à Internet das Coisas, com a conexão de tudo e com dispositivos de custo muito baixo, porém sem parâmetros mínimos de segurança associados[1].

Isoladamente, pode-se pensar que não seria uma preocupação estatal a exploração da rede e/ou dispositivos individuais de um cidadão. O problema reside no fato de que essa rede pode ser explorada para um ataque orquestrado contra alguma IEC, fazendo com que um setor estratégico fique fora do ar, causando caos social e, como consequência, riscos à segurança nacional. Por exemplo, um ataque coordenado ao setor financeiro impedindo as operações dos maiores bancos do país causaria grave caos e já foi utilizado em passado recente, como na Estônia em 2007[2], também podendo configurar o início de algum ataque à soberania do país, iniciado com a perturbação da ordem social. Reitera-se novamente, os cenários são muitos.

Retornando-se à E-Ciber, o próximo elemento que toca à discussão é a necessidade de compreensão holística e multissetorial do fenômeno, o qual não pode ser enfrentado de maneira limitada pela esfera estatal sem a participação do setor privado e sem considerar os indivíduos, justamente pelos motivos acima expostos. Nesse ponto, a E-Ciber cita novamente a necessidade de uma lei em sentido formal para segurança cibernética, que seria responsável pelo alinhamento da governança e conformidade nessa seara. Adicionalmente, a lei teria o condão de vincular todos os atores nacionais aos seus princípios e regras, construindo assim a confiança e segurança necessárias para a transformação digital da nossa sociedade e de todos os setores da economia (BRASIL, 2020a).

Aqui cabe lembrar que a E-Ciber foi aprovada e publicada antes da chegada da Pandemia do Covid-19 no Brasil, início de fevereiro de 2020, e que desde então, observou-se uma aceleração da transformação digital de todas as atividades da sociedade e da economia, também acompanhada de aceleração nos ataques cibernéticos. Como resultado, as preocupações com a segurança e resiliência do acesso e da fruição de todos os serviços digitais tornaram-se ainda mais relevantes.

---

[1] Como exemplo da exploração de dispositivos inteligentes para ataques de larga escala tem-se o *Malware Mirai* que infectava dispositivos como roteadores domésticos e câmeras IP fazendo com que passassem a integrar uma rede de zumbis (*botnet)* para realização de ataques de larga escala. Esse ataque foi responsável por retirar do ar o provedor de serviço de Sistema de Nomes de Domínio Dyn dos EUA, e, como consequência, serviços como Amazon, PayPal, Twitter e Netflix também ficaram indisponíveis. Para mais informações sobre o ataque, ver Antonakakis (2017).

[2] Sobre os ataques cibernéticos à Estônia ver Ottis (2008).

O texto da E-Ciber, que explora a dimensão normativa, também recomenda o aprimoramento do arcabouço legal nacional, especialmente no tocantes às políticas de segurança cibernética direcionadas ao setor produtivo. Nesse quesito reside o intuito de que a força do mercado alavanque o sucesso das ações em comparação às ações limitadas da esfera estatal e de fiscalização regulatória. Não obstante, adverte sobre a legitimidade necessária para a elaboração desses instrumentos.

Dessa forma, a recomendação é que o desenvolvimento dos arcabouços seja realizado com a maior legitimidade possível por meio da criação de mecanismos que propiciem o engajamento de vários atores não estatais, como academia e setor privado, com a finalidade de compartilhar experiências; explorar práticas internacionais; dialogar sobre padrões e melhores práticas em segurança cibernética; e apoiar o processo de tomada de decisão pela entidade responsável pela centralização da governança (BRASIL, 2020a).

A AE da E-Ciber que trata do aprimoramento do arcabouço legal de segurança cibernética exemplifica ações que podem ser adotadas para a revisão e atualização dos normativos existentes, assim como para a abordagem de novas temáticas e elaboração de novos instrumentos, destacando a medida de:

> [...] elaborar, sob coordenação do Gabinete de Segurança Institucional da Presidência da República, um anteprojeto de lei sobre segurança cibernética, com diretrizes que irão proporcionar alinhamento macroestratégico ao setor e contribuir de forma decisiva para elevar a segurança das organizações e dos cidadãos (BRASIL, 2020a).

Dessa forma, resta inconteste o reconhecimento no contexto do Arcabouço Nacional Jurídico e de Políticas Públicas, inclusive por diferentes órgãos e entidades do governo brasileiro, da necessidade da edição de uma lei formal para tratar de segurança cibernética.

Veja-se que a E-Digital foi aprovada no início de 2018 pelo então MCTIC e é fruto de Grupo de Trabalho Interministerial, contando com a participação de dezenas de órgãos e entidades da APF. Ou seja, não se trata de opinião isolada de um dos ministérios. Da mesma forma, a E-Ciber foi alvo de processo de participação conduzido pelo GSI/PR, inclusive com Consulta Pública, cuja metodologia foi destacada no próprio texto da Estratégia e apresentada no respectivo subitem do Capítulo III.

Cabe mencionar ainda que, em novembro de 2022, o Ministério da Ciência, Tecnologia e Inovações aprovou a Estratégia Brasileira para a Transformação Digital para o ciclo 2022-2026 (E-Digital 2022-2026) reprisando como ação estratégica para esse novo quadriênio a

"*edição de uma política nacional de segurança cibernética, incluindo a definição de instância nacional responsável pela articulação de um sistema nacional na matéria*".

Assim, não se pode falar em dúvida sobre a necessidade de elaboração do instrumento. No entanto, em que pese o decurso de mais de quatro anos desde a aprovação da E-Digital, e primeira manifestação formal sobre essa necessidade, até a presente data o anteprojeto sequer foi apresentado ao Congresso Nacional ou à sociedade em geral para contribuições, embora notícias sobre o seu desenvolvimento tenham circulado em mídia especializada e eventos relacionados[3]. De qualquer maneira, a corrida eleitoral presidencial de 2022 fez com que o tema naturalmente fosse empurrado para o próximo governo, o que implica em chegar em 2023 sem a necessária Lei.

Além do reconhecimento da necessidade de lei formal nessas políticas públicas brasileiras supramencionadas, cabe citar que os modelos estudados no Capítulo II corroboram essa interpretação, retomando-se agora os trabalhos da OCDE, da UIT e do GCSCC.

Nesse sentido, renova-se aqui os achados desse estudo para apoiar uma das principais proposições normativas da pesquisa, que defende a necessidade de um marco legal adequado. Iniciando com o *Guia para o Desenvolvimento de uma Estratégia Nacional de Segurança Cibernética - Engajamento estratégico em segurança cibernética* (ITU *et at*, 2021), relembra-se que o instrumento apresenta uma abordagem flexível com o objetivo de auxiliar os elaboradores de políticas públicas no desenvolvimento da visão, objetivos e prioridades de segurança cibernética do país, permitindo uma ação estratégica.

Embora inexista uma definição sobre o que constituiria uma ENSC, é possível identificar alguns elementos nucleares, que além de envolver essa visão estratégica de alto nível, também abarca visão geral de atores e suas responsabilidades; descrição de ações para proteção das IECs; e alinhamento com a agenda de transformação digital do país. Ademais, a ENSC deve incluir as ações e medidas de implementação, incluindo a alocação de recursos e identificação das respectivas métricas (ITU *et al.*, 2021c, p. 13 e 22).

Um dos pontos de destaque é a necessidade de que a ENSC estabeleça claro mecanismo de governança, o qual deve definir responsabilidades e papéis dos atores, incluindo a identificação de responsáveis pela gestão e pela implementação, bem como confirmando ou

[3] Sobre notícias em sites especializados referentes ao anteprojeto de lei abordando segurança cibernética ver: https://porta23.blogosfera.uol.com.br/2020/02/09/apos-estrategia-gsi-elabora-a-politica-nacional-de-seguranca-cibernetica/; https://teletime.com.br/18/11/2021/gsi-envia-minuta-de-politica-nacional-de-seguranca-cibernetica-a-casa-civil/ e https://www.convergenciadigital.com.br/Seguranca/Projeto-de-lei-para-seguranca-cibernetica-exige-times-setoriais-de-resposta-a-incidentes-59812.html?UserActiveTemplate=mobile. Acesso em: 26 ago. 2022.

atribuindo o mandado para as diferentes entidades; e fixando os contornos de como essas entidades irão interagir umas com as outras e com a entidade responsável pela gestão e implementação da ENSC (ITU *et al.,* 2021c, p. 22).

Em termos de processo de aprovação, o documento deve atender o rito que considera as peculiaridades de cada país, o qual poderia abarcar processo legislativo ou somente aprovação pelo Poder Executivo. No entanto, o destaque centra-se na aprovação no mais alto nível de governo, a fim de garantir o comprometimento com a sua implementação (ITU *et al.,* 2021c, p. 23-24). Essas premissas traduzem-se em princípios gerais transversais que auxiliam no desenvolvimento de uma ENSC: adoção dos instrumentos de políticas adequados e aprovação da ENSC no mais alto nível governo, com alocação dos recursos materiais financeiros e humanos para a sua implementação (ITU *et al.*, 2021c, p. 31).

Veja-se que o Guia elenca boas práticas em diversas áreas de foco, as quais reforçam essas premissas, apresentadas já no Capítulo II da pesquisa, e que no tocante à governança, exprimem a necessidade de indicar claramente os papéis e responsabilidades dos atores responsáveis pela implementação, bem como a garantia do nível máximo de apoio; estabelecimento de uma autoridade competente; garantia de cooperação intragovernamental e intersetorial; alocação de recursos adequados; e desenvolvimento de um plano de implementação (ITU *et al,* p. 34-36). Cabe ainda reiterar que a seção destinada às boas práticas na área de legislação e regulação aponta a necessidade de estabelecimento de um arcabouço jurídico doméstico para a segurança cibernética (ITU *et al,* p. 47-48).

Embora esses elementos aprovados como boas práticas não sejam prescritivos e devam ser considerados com as particularidades dos países e alinhados com as suas prioridades, constituem-se como elementos que permitem que a ENSC seja efetiva e abrangente (ITU *et al*, p. 34), cabendo a discussão sobre a pertinência da sua observância no contexto brasileiro. Um exercício interessante é a comparação da E-Ciber com as práticas identificadas no Guia, a qual permite extrair o desalinhamento do texto aprovado dessa coletânea de melhores práticas.

Em termos estruturais, a E-Ciber apresenta a visão, objetivo e ações estratégicas, que orientam e devem guiar o país nas suas ações de segurança cibernética. Ademais, a E-Ciber também traz notas sobre a metodologia empregada para sua elaboração, o diagnóstico constatado e análise de cada um dos eixos temáticos, consoante descrição constante do Capítulo III.

O primeiro ponto que merece ênfase é a natureza, ou seja, qual o tipo de instrumento foi utilizado para a aprovação da E-Ciber. No caso concreto, a E-Ciber foi aprovada por um Decreto, fundado na competência privativa do Presidente da República de dispor sobre a

organização e funcionamento da administração federal, quando não implicar aumento de despesa nem criação ou extinção de órgãos públicos[4], ou seja, trata-se de ato administrativo.

Embora tenha sido ratificada pelo Presidente da República e, portanto, pela autoridade máxima responsável pela Chefia do Poder Executivo, esse ato administrativo apresenta alguns contornos instransponíveis de limitação à APF; de impossibilidade de aumento de despesa; e de impossibilidade de criação de órgão público. Dessa forma, a primeira crítica é o limite de alcance do instrumento adotado em um tema que não pode ser tratado isoladamente na esfera federal. Não é possível pensar em endereçar os desafios crescentes de segurança cibernética apenas pensando em órgãos e entidades que compõe a APF, ainda que no seu sentido mais amplo.

Considerando que a forma de Estado brasileiro é a Federação, composta pela união indissolúvel dos Estados, Municípios e do Distrito Federal, não há como falar em visão estratégica de segurança cibernética para o país, sem uma lei que possa engajar todos os seus entes federativos e, até mesmo, os demais Poderes da União.

Mas não se trata apenas dos Poderes da União e dos entes da República Federativa do Brasil. Consoante apresentado no subitem 1.1 do Capítulo I, os desafios de segurança cibernética e suas repercussões para a segurança e proteção das IECs impõe o envolvimento e o engajamento não só do setor público, mas também o indispensável o envolvimento do setor privado. Esse, inclusive detém e é responsável pela operação de grande parte das IECs do país. Ademais, também é imprescindível a participação da comunidade técnica, academia e cidadãos, não podendo ser afastada a ideia de que segurança cibernética é uma responsabilidade compartilhada, mas sempre com a ressalva da diferença existente nos papéis e nas responsabilidades de cada um dos atores.

Nesse ponto específico, cabe trazer o ensinamento de Leonardo Vichi ao utilizar a ideia de teia formada por Estados, a quem cabe a definição das estratégias nacionalmente; setor privado, a quem cabe o desenvolvimento e implementação das políticas de segurança cibernética, especialmente nas IECs; e cidadãos, os quais são responsáveis por grande parte dos incidentes de segurança cibernética enraizados inclusive na lacuna de conscientização. Diante desse contexto, denota-se o relevante papel das Estratégias que devem equacionar essas questões (VICHI, 2021, p. 8-9).

Contrariamente ao necessário, a tipologia de ato administrativo decreto presidencial, embora ratificado pelo Chefe do Poder Executivo, o qual exerce a direção superior da

[4] Art. 84, VI, "a" da Constituição Federal com redação incluída pela Emenda Constitucional nº 32 de 11 de setembro de 2001 (BRASIL, 1988).

administração federal[5] é intrinsicamente limitado para tratar do tema, seja pela impossibilidade de atribuir papéis e responsabilidades aos órgãos e entidades que compõe os outros entes da Federação, seja pela impossibilidade de atribuir papéis e responsabilidades aos demais poderes da União e seja pela impossibilidade de criar obrigações a particulares. Constata-se, portanto, a impossibilidade de atribuição de responsabilidade aos demais e necessários atores sem uma lei no sentido formal, aprovada pelo Congresso Nacional, em respeito ao Princípio da Legalidade[6].

Embora bastante simplista, esse argumento é essencial para fins de estabelecimento de uma verdadeira atuação estratégica do país em segurança cibernética. Não é possível enfrentar os desafios e promover a segurança cibernética, e, portanto, fomentar a transformação digital da sociedade e da economia de forma fragmentada, sem todos os entes da Federação, Poderes da União e sem todos os atores. Não se promove segurança e resiliência cibernéticas isoladamente, em silos.

Na mesma linha, como o Decreto deve-se ater à organização e ao funcionamento da administração federal, não podendo assim indicar claramente os papéis e responsabilidades de todos os atores, a Estratégia limita-se à atribuir genericamente aos "*órgãos e entidades da administração pública federal, no âmbito de suas competências, as gestões que possibilitem à implementação das ações estratégicas previstas na E-Ciber*", nos termos do art. 2º do Decreto nº 10.222, de 5 de fevereiro de 2020 (BRASIL, 2020a).

Ao reler a E-Ciber, percebe-se que não há uma clara identificação dos atores envolvidos nem em nível federal, ou seja, não há mapeamento de papéis e responsabilidades de órgãos e entidades da APF, mas tão somente a previsão genérica de atuação consoante suas competências. Veja que a própria estratégia enfatiza "*ser absolutamente fundamental que cada órgão do setor público e do setor privado identifique, planeje e execute ações de sua competência*" (BRASIL, 2020a). Ou seja, a E-Ciber reconhece a responsabilidade de todos os atores, mas falha ao não identificar com clareza os papéis desses atores, ainda que limitada à APF.

Importa destacar a existência de algumas menções mais específicas ao longo das ações estratégicas, parte de diagnóstico e parte de análise dos eixos temáticos, ao serem identificadas menções às agências reguladoras e ao GSI/PR. Especificamente ao tratar da Ação Estratégica

[5] Art. 84, II, da Constituição Federal (BRASIL, 1988).

[6] Art. 5º da Constituição Federal estabelece que "[*t]odos são iguais perante a lei, sem distinção de qualquer natureza, garantindo-se aos brasileiros e aos estrangeiros residentes no País a inviolabilidade do direito à vida, à liberdade, à igualdade, à segurança e à propriedade, nos termos seguintes: [...] II - ninguém será obrigado a fazer ou deixar de fazer alguma coisa senão em virtude de lei*;" (BRASIL, 1998).

que aborda o estabelecimento de um modelo centralizado de governança no âmbito nacional, a E-Ciber defende a criação de um sistema nacional de segurança cibernética, com uma série de atribuições, e cabendo ao GSI/PR a "*coordenação da segurança cibernética em âmbito nacional, que possibilite a atuação de modo amplo, cooperativo, participativo, e alinhado com as ações de defesa cibernética, a cargo do Ministério da Defesa*" (BRASIL, 2020a).

Nesse ponto, entra-se em outro aspecto de uma melhor prática identificada no Guia (ITU *et al.*, 2021c), que trata do estabelecimento de autoridade competente de segurança cibernética, que será responsável pela execução da estratégia, retomando-se aqui uma parte relevante da E-Ciber que discorre sobre o papel do GSI/PR no eixo temático de governança:

> No caso brasileiro, ao considerar o Governo federal, destaca-se a atuação do Gabinete de Segurança Institucional da Presidência da República que, desde 2006, por meio do Departamento de Segurança da Informação, estuda e elabora diversos normativos, que consistem em Instruções Gerais, Normas Complementares, Estratégias e Política, no âmbito da Administração Pública federal, ao reunir, desde então, vasta experiência com relação a diversas áreas da segurança da informação, especialmente no que tange à segurança cibernética.
> Desse modo, **não se vislumbra a necessidade da criação de novos e dispendiosos organismos governamentais**, sendo suficiente **redimensionar a atual estrutura do Gabinete de Segurança Institucional** da Presidência da República, de forma a **lhe possibilitar a atuação em âmbito nacional**. Portanto, **urge a necessidade de uma lei que regule as ações de segurança cibernética, que especifique atribuições, que aponte mecanismos de diálogo com a sociedade e que torne possível**, ao Gabinete de Segurança Institucional da Presidência da República, com a participação de representantes de todos os entes nacionais, exercer o papel de **macro coordenador estratégico,** ao proporcionar alinhamento às ações de segurança cibernética e ao contribuir para a evolução de todo o País nesse campo, de forma convergente e estruturada. Conclui-se, ainda, ser necessário e urgente que o Governo federal priorize a aplicação de recursos na área da segurança cibernética.
> Outrossim, conforme mencionado no parágrafo anterior, devem ser considerados mecanismos que viabilizem a participação da sociedade. Dentre os instrumentos possíveis, esta Estratégia recomenda a criação de um conselho nacional de segurança cibernética, que congregue diversos atores estatais e não estatais, com o objetivo de pensar a segurança cibernética sob um prisma abrangente, inclusivo, moderno e com ênfase nas reais necessidades nacionais. (BRASIL, 2020a, Grifo nosso).

Como se deduz do texto expresso da E-Ciber supracitado, existe o claro indicativo de que seria o GSI/PR o coordenador nacional de segurança cibernética, no centro de um sistema nacional que deveria ser criado, porém que sobre o qual não é possível localizar informação alguma, ou seja, não há informações sobre implementação desse comando, salvo notícias especializadas sobre a submissão de novo anteprojeto de uma lei[7], o qual, assim como o

[7] Sobre notícias em sites especializados referentes ao anteprojeto de lei abordando segurança cibernética ver: https://porta23.blogosfera.uol.com.br/2020/02/09/apos-estrategia-gsi-elabora-a-politica-nacional-de-seguranca-cibernetica/; https://teletime.com.br/18/11/2021/gsi-envia-minuta-de-politica-nacional-de-seguranca-cibernetica-a-casa-civil/ e https://www.convergenciadigital.com.br/Seguranca/Projeto-de-lei-para-seguranca-cibernetica-exige-times-setoriais-de-resposta-a-incidentes-59812.html?UserActiveTemplate=mobile. Acesso em: 26 ago. 2022.

anteprojeto de PNSI em 2018, parece ter sido sobrestado em função do período eleitoral e das mudanças governamentais.

Assim, em relação às competências legais do GSI/PR, até 31 de dezembro de 2022, a Lei nº 13.844, de 18 de junho de 2019, que estabelecia a organização básica dos órgãos da Presidência da República e dos Ministérios, determinava as competências do GSI/PR, as quais englobavam a coordenação de atividades de segurança da informação e das comunicações no âmbito da APF; o planejamento, coordenação e supervisão das atividades de segurança da informação no âmbito da APF, incluindo a segurança cibernética; e o acompanhamento dos assuntos pertinentes às IECs (BRASIL, 2019b).

Cumpre destacar que a Medida provisória nº 1.154, de 1º de janeiro de 2023, manteve essas competências relacionadas ao planejamento, coordenação e supervisão das atividades de segurança da informação no âmbito da APF, incluindo a segurança cibernética; e ao acompanhamento dos assuntos pertinentes às IECs. No entanto, a competência relacionada à coordenação das atividades de segurança da informação e das comunicações teve sua redação alterada, deletando-se a parte que qualificava a atuação ao âmbito da APF, porém sem acrescentar a atuação nacional (BRASIL, 2023a).

Dessa forma, embora exista expressamente o indicativo do GSI/PR como coordenador nacional, falta o arcabouço legal amparando essa competência, necessidade apontada tanto pelo nosso ordenamento jurídico, quanto pela boa prática de estabelecimento do arcabouço jurídico doméstico adequado para segurança cibernética (ITU *et al.*, 2021c, p. 47-48).

Não se pode olvidar que a aprovação da E-Ciber é um avanço que precisa ser reconhecido e cujo conteúdo foi limitado em decorrência do instrumento utilizado para sua aprovação, qual seja um decreto fundado na competência privativa do Presidente da República para dispor sobre a organização e funcionamento da APF. Ou seja, a crítica ao conteúdo funda-se essencialmente na tipologia do ato, que não permite enfrentar as questões apontadas, de atribuição de papéis e responsabilidade a atores que não se limitam à APF. Na verdade, sequer se limitam à esfera federal, ao Poder Executivo e aos atores públicos, como ressaltado em diversos momentos no texto.

Para corroborar a fragmentação, salienta-se a aprovação de Estratégia Nacional de Segurança da Informação e Cibernética do Poder Judiciário (ENSEC-PJ) aprovada pelo Conselho Nacional de Justiça (CNJ) e publicada em 10 de junho de 2021[8]. Embora de iniciativa louvável do Poder Judiciário, demonstra o isolamento das ações e medidas adotadas pelos

[8] Resolução nº 396, de 7 de junho de 2021, a qual institui a Estratégia Nacional de Segurança Cibernética do Poder Judiciário (ENSEC-PJ). Disponível em: https://atos.cnj.jus.br/atos/detalhar/3975. Acesso em: 26 ago 2022.

Poderes, pelos entes federativos e pelos diversos atores, sem que se possa falar em efetiva governança centralizada, modelo defendido na E-Ciber (BRASIL, 2021a).

Outra boa prática citada refere-se à garantia de cooperação intragovernamental e intersetorial e é possível verificar a previsão de texto na E-Ciber com essa finalidade. Nessa esteira, relembra-se a previsão da criação do Sistema Nacional de Segurança Cibernética; criação de um Conselho Nacional de Segurança Cibernética; e criação de grupo de debate sobre segurança cibernética sob coordenação do GSI/PR. Esses dois últimos mecanismos seriam atribuições do Sistema, o qual seria responsável pela concretização do modelo centralizado de governança cibernética no âmbito nacional (BRASIL, 2020a). Até a data de finalização da pesquisa, não foi possível encontrar qualquer informação relacionada à constituição do Sistema.

Especialmente sobre cooperação intersetorial, essa premissa está duplamente contemplada nas AE que englobam a promoção de ambiente participativo, colaborativo, confiável e seguro, entre setores público e privado, bem como sociedade; e a ampliação da parceria, em segurança cibernética, entre setor público, setor privado, academia e sociedade. Embora relacionando uma série de medidas que poderiam ser materializadas a fim de implementar essas ações, não se pode apontar que a E-Ciber consegue garantir a cooperação nos níveis intragovernamental e intersetorial, justamente pelos fatores já esposados anteriormente.

No entanto, não se pode olvidar a existência de algumas práticas que promovem essa cooperação e, até mesmo, anteriores à E-Ciber, como o EGC, que se trata de simulação nacional promovida pelo Ministério da Defesa por meio do ComDCiber, cuja primeira edição remonta à 2018 e, portanto, anterior à E-Ciber (LIMA e SILVA, 2020).

Outra ação de implementação referente à cooperação intragovernamental e intersetorial é o Decreto nº 10.748, de 16 de julho de 2021, que instituiu a ReGIC, apresentada no subitem 3.6 do Capítulo III. Ademais, também pode ser citada a parceria estabelecida entre Anatel e a Universidade Federal de Campina Grande com a descentralização de recursos para pesquisa sobre segurança cibernética no 5G[9].

Ressalta-se que a fragmentação das iniciativas, que reflete o contexto de inexistência de uma autoridade nacional, prejudica uma visão das capacidades e lacunas brasileiras, inexistindo um repositório oficial dessas ações e iniciativas de implementação.

[9] Informações sobre o Termo de Execução Descentralizada em: https://sei.anatel.gov.br/sei/publicacoes/controlador_publicacoes.php?acao=publicacao_visualizar&id_documento=8761848&id_orgao_publicacao=0. Acesso em: 29 ago. 2022.

Adicionando mais uma camada à discussão, tem-se a questão de alocação dos recursos adequados para a implementação da E-Ciber, necessidade que novamente não pode ser atendida pelo instrumento utilizado. A alocação dos recursos precisa ser endereçada nos três instrumentos do modelo orçamentário brasileiro previstos na Constituição Federal, quais sejam, o Plano Plurianual (PPA); Lei de Diretrizes Orçamentárias (LDO) e a Lei Orçamentária Anual (LOA), nos termos do art. 165 da Constituição Federal, todos de iniciativa do Poder Executivo.

Salienta-se que o PPA deve, de maneira regionalizada, estabelecer as diretrizes, objetivos e metas da APF para as despesas relativas aos programas de duração continuada e para despesas de capital e outras delas decorrentes; e que a LDO deve compreender as metas e prioridades da APF[10]. Nessa esteira, a eventual alocação de recursos para todas as iniciativas

[10] Seção II. DOS ORÇAMENTOS. Art. 165. Leis de iniciativa do Poder Executivo estabelecerão: I - o plano plurianual; II - as diretrizes orçamentárias; III - os orçamentos anuais. § 1º A lei que instituir o plano plurianual estabelecerá, de forma regionalizada, as diretrizes, objetivos e metas da administração pública federal para as despesas de capital e outras delas decorrentes e para as relativas aos programas de duração continuada. § 2º A lei de diretrizes orçamentárias compreenderá as metas e prioridades da administração pública federal, estabelecerá as diretrizes de política fiscal e respectivas metas, em consonância com trajetória sustentável da dívida pública, orientará a elaboração da lei orçamentária anual, disporá sobre as alterações na legislação tributária e estabelecerá a política de aplicação das agências financeiras oficiais de fomento. § 3º O Poder Executivo publicará, até trinta dias após o encerramento de cada bimestre, relatório resumido da execução orçamentária. § 4º Os planos e programas nacionais, regionais e setoriais previstos nesta Constituição serão elaborados em consonância com o plano plurianual e apreciados pelo Congresso Nacional. § 5º A lei orçamentária anual compreenderá: I - o orçamento fiscal referente aos Poderes da União, seus fundos, órgãos e entidades da administração direta e indireta, inclusive fundações instituídas e mantidas pelo Poder Público; II - o orçamento de investimento das empresas em que a União, direta ou indiretamente, detenha a maioria do capital social com direito a voto; III - o orçamento da seguridade social, abrangendo todas as entidades e órgãos a ela vinculados, da administração direta ou indireta, bem como os fundos e fundações instituídos e mantidos pelo Poder Público. § 6º O projeto de lei orçamentária será acompanhado de demonstrativo regionalizado do efeito, sobre as receitas e despesas, decorrente de isenções, anistias, remissões, subsídios e benefícios de natureza financeira, tributária e creditícia. § 7º Os orçamentos previstos no § 5º, I e II, deste artigo, compatibilizados com o plano plurianual, terão entre suas funções a de reduzir desigualdades inter-regionais, segundo critério populacional. § 8º A lei orçamentária anual não conterá dispositivo estranho à previsão da receita e à fixação da despesa, não se incluindo na proibição a autorização para abertura de créditos suplementares e contratação de operações de crédito, ainda que por antecipação de receita, nos termos da lei. § 9º Cabe à lei complementar: I - dispor sobre o exercício financeiro, a vigência, os prazos, a elaboração e a organização do plano plurianual, da lei de diretrizes orçamentárias e da lei orçamentária anual; II - estabelecer normas de gestão financeira e patrimonial da administração direta e indireta bem como condições para a instituição e funcionamento de fundos. III - dispor sobre critérios para a execução equitativa, além de procedimentos que serão adotados quando houver impedimentos legais e técnicos, cumprimento de restos a pagar e limitação das programações de caráter obrigatório, para a realização do disposto nos §§ 11 e 12 do art. 166. § 10. A administração tem o dever de executar as programações orçamentárias, adotando os meios e as medidas necessários, com o propósito de garantir a efetiva entrega de bens e serviços à sociedade. § 11. O disposto no § 10 deste artigo, nos termos da lei de diretrizes orçamentárias: I - subordina-se ao cumprimento de dispositivos constitucionais e legais que estabeleçam metas fiscais ou limites de despesas e não impede o cancelamento necessário à abertura de créditos adicionais; II - não se aplica nos casos de impedimentos de ordem técnica devidamente justificados; III - aplica-se exclusivamente às despesas primárias discricionárias. § 12. Integrará a lei de diretrizes orçamentárias, para o exercício a que se refere e, pelo menos, para os 2 (dois) exercícios subsequentes, anexo com previsão de agregados fiscais e a proporção dos recursos para investimentos que serão alocados na lei orçamentária anual para a continuidade daqueles em andamento. § 13. O disposto no inciso III do § 9º e nos §§ 10, 11 e 12 deste artigo aplica-se exclusivamente aos orçamentos fiscal e da seguridade social da União. § 14. A lei orçamentária anual poderá conter previsões de despesas para exercícios seguintes, com a especificação dos investimentos plurianuais e daqueles em andamento. § 15. A União organizará e manterá registro centralizado de projetos de

relacionadas à segurança cibernética exigiria a necessária gestão para que as demandas associadas fossem contempladas no ciclo orçamentário brasileiro. Da mesma forma que outras previsões, não foi possível localizar informações consolidadas sobre o montante dotado, nem executado de orçamento em ações e medida de promoção à segurança cibernética.

Embora uma lei geral de segurança cibernética não possa endereçar as questões orçamentárias, justamente pelo sistema orçamentário brasileiro que é composto pelos três instrumentos orçamentários supracitados, pode dispor sobre a designação e/ou criação de órgão e entidades, ou seja, dispor sobre a autoridade nacional, bem como das respectivas receitas dessa autoridade, impactando assim o orçamento.

Cita-se como exemplo a Lei nº 9.472, de 16 de julho de 1997, que dispõe sobre a organização dos serviços de telecomunicações, a criação e funcionamento de um órgão regulador e outros aspectos institucionais, nos termos da Emenda Constitucional nº 8, de 1995, conhecida como Lei Geral de Telecomunicações (LGT). Essa lei tem um livro destinado a tratar do órgão regulador e das políticas setoriais, incluindo um título exclusivo para tratar das receitas, no qual traz disposições relacionadas à administração de fundo pela agência, contendo também previsões sobre a submissão anual de proposta orçamentária para inclusão na lei orçamentária anual, acrescida de planejamento plurianual.

Ademais, o art. 15 da LGT estabelece que a fixação das dotações orçamentárias da Anatel na LOA e sua programação financeira e orçamentária de execução não podem sofrer limites para empenho e movimentação (BRASIL, 1997), ou seja, não poderiam sofrer contingenciamento. Outro exemplo, é a LGPD, com alterações da Lei nº 13.853, de 8 de julho de 2019, a qual estabelece as receitas da ANPD (BRASIL, 2019a).

Interessante notar a abordagem da PND e END. A despeito de não poder tratar de dotações orçamentárias no seu texto, sustentam a necessidade de regularidade e estabilidade orçamentária-financeira para o Setor de Defesa (BRASIL, 2018d). Além disso, a proposta enviada ao Congresso Nacional de atualização da PND e END, ainda em tramitação, inclusive destaca a estabilidade para fins de aquisição de produtos de defesa e elenca como Estratégia de Defesa a regularidade orçamentária, estipulando como AED 14 a busca de "*destinação de recursos orçamentários e financeiros capazes de atender as necessidades de articulação e equipamento para as Forças Armadas, por meio da Lei Orçamentária Anual, no patamar de 2% do PIB*" (BRASIL, 2020e).

---

investimento contendo, por Estado ou Distrito Federal, pelo menos, análises de viabilidade, estimativas de custos e informações sobre a execução física e financeira. § 16. As leis de que trata este artigo devem observar, no que couber, os resultados do monitoramento e da avaliação das políticas públicas previstos no § 16 do art. 37 desta Constituição (BRASIL, 1988).

Portanto, ainda que o marco legal não possa adentrar especificamente na questão orçamentária, pelo sistema orçamentário constitucionalmente previsto, pode conter as disposições mais genéricas sobre as receitas da autoridade responsável, bem como pode, no âmbito da política e estratégia, tecer a visão estratégica que deve ser concretizada via planejamento orçamentário.

Por fim, como última boa prática elencada, tem-se a importância de desenvolvimento de um plano de implementação, com o objetivo de detalhar como os objetivos estratégicos serão atingidos, destacando o Guia que um plano efetivo detalha as entidades responsáveis por cada tarefa e objetivo, recursos necessários, tempo necessário de execução, processos e resultados esperados (ITU *et al.*, 2021c, p. 36-37).

Conforme já exposto, embora a E-Ciber liste as ações e medidas que poderiam ser adotadas para a concretização dos três objetivos estratégicos e da visão colocada, a previsão de papéis e responsabilidades é bastante genérica e não é acompanhada da previsão de recursos, nem de métricas de implementação, não se conhecendo até a presente data plano de implementação da E-Ciber. Essa posição é corroborada por Hurel que destaca que permanecem indefinidos os seus horizontes de acompanhamento e implementação (2021, p. 21).

No entanto, é possível indicar algumas ações assertivas de implementação, como a ReGIC, a qual concretiza medidas que implementam as AEs de promoção de ambiente participativo, colaborativo, confiável e seguro, entre setor público, setor privado e sociedade; e de elevação do nível de proteção das IECs Nacionais. Essas AEs mencionam, respectivamente, o fortalecimento do papel do CTIR Gov, o incentivo à constituição de ETIRs e o estímulo à notificação do CTIR Gov em incidentes cibernéticos sofridos pelas IECs (BRASIL, 2020a).

Conquanto não se conheça nenhum portal, repositório, documento ou instrumental governamental que identifique todas as organizações, papéis e iniciativas na matéria, o que é o basilar para permitir uma compreensão e coordenação dos esforços, cabe trazer à baila iniciativa do Instituto Igarapé do Portal Brasileiro da Cibersegurança[11] que faz um mapeamento do ecossistema de segurança cibernética no Brasil, identificando a pluralidade de atores e respectivos documentos, bem como ações.

Outrossim, o Instituto também publicou uma análise da E-Ciber apresentando como pontos fortes o encaminhamento para Consulta Pública; reconhecimento da atuação internacional dos países em foros especializados na temática; previsão do desenvolvimento de capacidades multissetoriais; destaque para a importância de adoção dos conceitos de *security*

[11] Portal Brasileiro de Cibersegurança. Disponível em: https://ciberseguranca.igarape.org.br/. Acesso em: 29 ago. 2022.

and privacy by design and default; e necessidade de fortalecimento dos CSIRTs (HUREL, 2021, p. 32).

Já como pontos fracos, aponta a falta de alinhamento de expectativas (formato e clareza dos objetivos); ausência de menção à sociedade civil; ausência de visão clara sobre protocolo para compartilhamento intersetorial de informações; dúvidas sobre a capacidade do GSI/PR para realizar a interlocução com a sociedade civil e para a coordenar nacionalmente o tema; indefinição do conteúdo da Lei que tratará de segurança cibernética; e ausência de plano orçamentário para desenvolvimento de planos de implementação (HUREL, 2021, p. 32).

Nota-se que dos seis pontos fracos aqui consolidados, quatro coincidem com a discussão travada nessa pesquisa e relacionam-se ao modelo tentativo de governança estabelecido e ao instrumento (e suas limitações) utilizado, visto que orbitam nesses temas a impossibilidade de alocação de recursos; a necessidade de lei formal; a necessidade de governança efetivamente nacional; a necessidade de estabelecer planos de implementação, etc. Em publicação anterior de 2018, Hurel e Lobato já defendiam a criação de uma agência nacional com atribuição de gerir a implementação de uma ENSI, também sustentando a necessidade de elaboração desse instrumento (2018, p. 16).

Como Recomendações, após o reconhecimento que a E-Ciber é um importante passo, a análise defende a publicação de relatório anual sobre a sua implementação; o estabelecimento de canais de diálogo com a sociedade civil, bem como o reconhecimento do seu papel em capacitação; o aprimoramento dos mecanismos de compartilhamento intersetorial de informações e disponibilização de diretrizes para divulgação de vulnerabilidades; o aprimoramento da interlocução do GSI/PR com academia e sociedade civil; a avaliação das capacidades do GSI; e a avaliação da necessidade de uma lei e/ou identificação do momento adequado de encaminhamento ao Congresso Nacional (HUREL, 2021, p. 33-34).

Veja-se que especificamente sobre anteprojeto de lei temático, a publicação lança um olhar de desconfiança, alertando sobre as incertezas; e a funcionalidade e impactos dos mecanismos de participação citados na E-Ciber, como os grupos de debates e o Conselho Nacional de Segurança Cibernética, assim como a contribuição da academia e sociedade civil no processo. Entretanto, o artigo reconhece a possibilidade de incentivos do marco legal à consolidação de uma cultura de segurança que abrace a sociedade e adiciona uma camada extra de preocupação com a possibilidade de confusão de conceitos associados à criminalidade e defesa cibernéticas, especialmente em um contexto de polarização e instabilidade política, resultando em divergências sobre o escopo do lei, especialmente no tocante a ações e atribuições (HUREL, 2021, p. 29-30).

Passa-se agora à avaliação da E-Ciber à luz do modelo da OCDE, que abrange tanto as Recomendações de 2015 quanto às atualizações de 2022, as quais envolvem princípios e diretrizes para as Estratégias Nacionais e foram anteriormente apresentadas no Capítulo II, subitem 2.1, novamente sob o recorte do marco legal.

No tocante aos princípios gerais, destaca-se que o princípio chave à discussão em tela é o da Responsabilidade, o qual prevê que todos os atores têm que assumir a responsabilidade pela gestão do risco de segurança digital, agindo com responsabilidade e prestando contas, com base no seu papel, contexto e na sua capacidade de agir (OECD, 2015, p. 9). Aqui se relembra que no ordenamento jurídico brasileiro a imposição de uma obrigação, ou seja, de um dever, no caso de gerir o risco de segurança digital, demanda a existência de uma lei, por força do art. 5º, II, da Constituição Federal.

Embora se reconheça a prática de imposição de deveres relacionados em regulação setorial aos detentores de IECs (sem violação ao Princípio da Legalidade, pois se funda em mandatos e competências estabelecidos por lei) [12], essa imputação é fragmentada e não abarca todos os setores da sociedade e da economia, argumento que corrobora o racional da necessidade do adequado marco legal.

Veja-se que há espaço para citar uma novidade da Recomendação do Conselho sobre Estratégias Nacionais de Segurança Digital de 2022, que traz recomendação específica para o arcabouço institucional. Essa faz referência à necessidade de clara atribuição de responsabilidade a um (ou mais) órgão(s), novo(s) ou já existente(s), para o desenvolvimento das políticas públicas e respectiva implementação, além de enfatizar a necessária coordenação interagência em diversas dimensões que possuem estreita conexão com segurança cibernética. Cita-se como exemplo de outras áreas: proteção de danos, crimes cibernéticos; governo digital, etc (OCDE, 2022b).

Adicionalmente, quanto aos princípios operacionais, os princípios relacionados ao ciclo de avaliação e tratamento de risco, bem como de medidas de segurança apropriadas ao risco demandam ação de líderes e tomadores de decisão, para que essas ações sejam implantadas

[12] Nesse sentido, ver: Regulamento de Segurança Cibernética Aplicada ao Setor de Telecomunicações, aprovada pela Resolução n.º 740, de 21 de dezembro de 2020. Disponível em: https://informacoes.anatel.gov.br/legislacao/resolucoes/2020/1497-resolucao-740; Resolução Normativa ANEEL n.º 964, de 14 de dezembro de 2021, que dispõe sobre a política de segurança cibernética a ser adotada pelos agentes do setor de energia elétrica. Disponível em: https://www.in.gov.br/en/web/dou/-/resolucao-normativa-aneel-n-964-de-14-de-dezembro-de-2021-369359262 e Resolução CMN n.º 4.893, de 26 de fevereiro de 2021, que dispõe sobre a política de segurança cibernética e sobre os requisitos para a contratação de serviços de processamento e armazenamento de dados e de computação em nuvem a serem observados pelas instituições autorizadas a funcionar pelo Banco Central do Brasil. Disponível em: https://www.ancord.org.br/wp-content/uploads/2021/03/Resolucao-CMN-n-4.893-de-26_2_2021.pdf . Acesso: 30 ago. 2022.

(OECD, 2015, p. 10). Já passando para a parte destinada às estratégias, o instrumento da OCDE enfatiza que as ENSC devem ser consistentes com os princípios e criar as condições necessárias para que todos os atores façam a gestão desses riscos. Outrossim as estratégias também devem ser direcionadas a todos os atores e adaptadas às pequenas e médias empresas e indivíduos, articulando, novamente, a responsabilidade dos atores de acordo com seus papéis, capacidade de agir e contexto de operação.

Nesse ponto retorna-se, mais uma vez, ao argumento da necessidade de uma lei em face do Princípio da Legalidade insculpido na Constituição Federal. Apesar de nenhum dos modelos preconize a imprescindibilidade de uma lei aprovada pelo Congresso Nacional, o ordenamento jurídico pátrio impõe essa exigência como condição para a concretização desses princípios e premissas consagrados e consolidados nesses instrumentos.

Não obstante todos tenham uma abordagem flexível, justamente para que possam servir como orientações universais para a elaboração de estratégias por qualquer país, as diferenças dos ordenamentos domésticos impõem a sua adaptação às conjunturas locais. Esse é o motivo pelo qual o Brasil precisa de uma lei, sob pena de continuarmos sem adequadamente endereçar pontos essenciais para o efetivo tratamento e mitigação desses riscos, os quais não param de se expandir, seja em termos civis, seja em termos militares (com a ressalva de que a última perspectiva não é objeto do trabalho).

Por fim, quanto às medidas que devem ser incluídas nas ENSC, o primeiro ponto é a liderança pelo exemplo, indicando o modelo algumas ações. Dentre as opções citadas, nota-se a adoção de um arcabouço abrangente para todas as atividades governamentais; o estabelecimento de mecanismos de coordenação entre todos os atores relevantes; e a alocação de recursos suficientes para a implementação efetiva da Estratégia (OECD, 2015, p. 12-13).

Um arcabouço abrangente, que envolva todas as atividades governamentais, ou seja abranja todos os entes da Federação (União, Estados, Municípios e Distrito Federal) e todos os Poderes, demanda lei em sentido formal. A fragmentação é extremamente prejudicial ao enfrentamento dos desafios relacionados e os diferentes níveis de maturidade, em qualquer ente ou Poder, pode, e, provavelmente, será explorada. Ou seja, a fragmentação é uma vulnerabilidade que pode ser explorada e tornar-se uma ameaça à segurança cibernética. Além disso, o segundo aspecto apontado reforça o primeiro, defendendo o estabelecimento de mecanismos de coordenação entre todos atores governamentais relevantes, os quais não se limitam aos órgãos e entidades que compõe a APF. Por fim, novamente a questão da alocação de recursos só pode ser endereçada através dos instrumentos orçamentários do nosso modelo, explicitados anteriormente.

Outras medidas pertinentes são o engajamento com outros atores e a criação de condições para que todos colaborem na gestão de riscos de segurança cibernética (OECD, 2015, p. 14-15). Políticas e planos governamentais tão somente são insuficientes para enfrentar todos desafios. É necessário o suporte da comunidade técnica, a pesquisa da academia, as percepções da sociedade civil e o engajamento do setor privado, o qual detém e opera grande parte das IECs do país, sem esquecer que todo indivíduo também tem um papel nesse ecossistema. É um paradigma bastante desafiador e que impõe a necessária coordenação, a qual não se vislumbra sem o marco legal adequado.

A despeito das recomendações da OCDE não serem vinculantes aos aderentes, não se olvida que o Brasil aderiu à Recomendação de 2015 e às quatros novas recomendações de segurança digital lançadas em 2022, sinalizando um compromisso de vontade política do país aderente para fins de implementação, diferentemente dos outros modelos estudados, fato que corrobora a prescrição do marco legal que neste capítulo é construída.

Cumpre ainda trazer as considerações do modelo o GCSCC, utilizado como base metodológica para a elaboração da E-Ciber, relacionadas à questão do marco legal. Desde o início deve-se fazer a ressalva de que embora exista uma dimensão específica para arcabouço legal e regulatório no modelo, esse arcabouço está focado na efetiva persecução da criminalidade cibernética; requisitos regulatórios de segurança cibernética; e legislação associada, como proteção de dados pessoais e proteção da criança e adolescente, por exemplo. Não endereça a questão de governança nacional de segurança cibernética, motivo pelo qual se centra na dimensão que trata de política e estratégia de segurança cibernética, a qual contempla um fator específico para a ENSC.

Recorda-se que o CMM é composto de cinco dimensões, as quais são compostas por fatores que se decompõe em aspectos, os quais são avaliados em função do estágio de maturidade descrito através de indicadores, a parte mais básica da estrutura do modelo (OXFORD, 2021, p. 7). Nesse arcabouço, o Fator ENSC, que foi apresentado no Quadro 1 do subitem 2.3 do Capítulo II, contempla os indicadores que refletem os estágios de maturidade de cada um dos seus quatros aspectos. Cabe trazer ao debate que a capacidade brasileira para o Fator ENSC foi avaliada como Estágio Formativo-Estabelecido (OXFORD, 2020b, p. 40). Ou seja, já se verifica alguns elementos que indicam o nível de maturidade estabelecido, porém não alcançando todos os indicadores desse estágio.

Retoma-se aqui os indicadores do Estágio Estabelecido para o Fator ENSC: ENSC publicada; realizada avaliação de riscos do país; ENSC apresenta papéis e necessidades dos atores relevantes; programa de implementação abrangendo todo escopo da estratégia;

mecanismos estabelecidos de monitoramento; conteúdo abrangente e associado às demais políticas nacionais; inclui conscientização, crimes cibernéticos, capacidade de resposta a incidentes, promoção de parcerias e proteção de IEC; considera o papel da ENSC no apoio a outros objetivos; plano detalhado de implementação, incluindo entidades responsáveis e recursos orçamentários; designação de órgão de coordenação com a autoridade necessária; recursos identificados e alocados; processo de revisão estabelecido; avaliação de como os debates internacionais afetam os interesses do país; participação ativa nos fóruns internacionais; e país ativamente contribui em órgãos relevantes de colaboração e desenvolvimento de políticas (OXFORD, 2021, p. 12-13).

Ao verificar os indicadores supracitados, sobressaltam as questões relacionadas aos recursos, à implementação, à designação de entidade com autoridade necessária (ou seja, com o mandato legal estabelecido) e ao monitoramento da Estratégia. Nos termos relatados por diversas vezes no presente trabalho, nenhum desses indicadores pode ser considerado atingido. Nota-se que, novamente, não existe qualquer menção à necessidade de uma lei, não existindo nenhum indicador nesse sentido, justamente pelo fato de que o modelo precisa ser genérico e flexível para que possa ser aplicável a qualquer país.

Para fins de comparação, reitera-se a citação dos indicadores do Fator ENSC para os Estágios Estratégico e Dinâmico, os últimos e mais avançados estágios de maturidade. O quarto estágio aponta para a existência de um processo de revisão e atualização implantado; a avaliação regular dos riscos e atualização da estratégia e plano de implementação; o uso do impacto da estratégia na redução do risco e dos danos é compreendido e utilizado para informar as prioridades e decisões orçamentárias; o conteúdo considera o impacto de novas tecnologias; os resultados são específicos e mensurados; a consideração de como os resultados da ENSC serão sustentados, incluindo os recursos necessários; a existência de métricas orientadas ao resultado; as evidências de que essas métricas são utilizadas para refinar os planos de ação; o desenho de métricas de fontes variadas (estatais e não estatais); a existência de supervisão independente do programa; a construção ativa pelo país de comunidades de interesse em torno de objetivos específicos de políticas; a contribuição significativa do país para órgãos operacionais regionais e internacionais; e o envolvimento ativo do país na construção de capacidades em outros países terceiros (OXFORD, 2021, p. 12-13).

Veja-se que o nível Estratégico revela a maturidade de uma ENSC que é coordenadamente concretizada e cujo processo de implementação, assim como a evolução dos riscos das tecnologias, alimentam tanto o processo de atualização e revisão da Estratégia, quanto o processo de implementação.

Não há qualquer menção à existência de um arcabouço normativo. Entretanto, para o cenário brasileiro, o instrumento adequado é pressuposto desse nível de maturidade, visto que o processo efetivo de implementação, acompanhamento e revisão da ENSC só pode ser implantado com a identificação dos papéis e responsabilidade dos atores; com a identificação de entidade responsável pelo acompanhamento da implementação; com a instalação dos mecanismos de coordenação necessários; com o estabelecimento de métricas; com a alocação dos recursos necessários; e com planos de implementação. Nessa esteira, a existência de uma lei é um passo anterior e necessário para o amadurecimento da nossa capacidade de segurança cibernética.

Apenas para ilustrar o último e mais avançado estágio de maturidade, o nível Dinâmico exige que a ENSC e o plano de implementação sejam proativamente revisados para considerar desenvolvimentos estratégicos domésticos; que o país seja uma autoridade reconhecida na comunidade internacional e apoie o desenvolvimento de estratégias nacionais e globais de segurança cibernética; que o tema esteja inserido em outras políticas nacionais; que o conteúdo considere os impactos de desenvolvimento importantes; que o conteúdo promova e encoraje cooperação bi e multilateral; que haja mecanismos implantados para mudanças abrangentes na implementação diante de mudanças significativas de conjuntura; que a implementação contribua para o desenvolvimento global de métricas; que o país seja líder na construção de consenso e ajude a moldar o debate internacional; e, por fim, que o país esteja ativamente envolvido na criação de novos mecanismos regionais e internacionais de colaboração (OXFORD, 2021, p. 12-13).

Esses Indicadores do último estágio demonstram a grande distância entre o nível máximo de maturidade do CMM e a situação atual de capacidade de segurança cibernética brasileira, devendo ser novamente ressaltado que nenhum modelo pode ser adotado sem considerar a pertinência da sua adoção e a necessária adaptação ao contexto brasileiro.

Não se busca no presente trabalho defender que o Brasil precisa de uma lei para atender ao modelo OCDE, UIT ou GCSCC, embora esse último tenha servido com subsídio metodológico para a E-Ciber e o Brasil tenha aderido às Recomendação da OCDE em segurança digital, tanto de 2015 quanto às lançadas em 2022.

Sustenta-se que o país deve, a partir dessas diretrizes internacionais e considerando as suas especificidades, encontrar o seu caminho para enfrentar os desafios de promover a segurança cibernética, e, assim, usufruir de todos os benefícios da transformação digital da sociedade e da economia. Nessa toada, deve-se ponderar as peculiaridades, inclusive do seu

ordenamento jurídico, porém sem desconsiderar as características culturais, sociais, políticas, econômicas e, até mesmo, sua dimensão continental e suas percepções de desenvolvimento.

Em linha semelhante e trazendo um olhar crítico ao desenvolvimento de capacidades de segurança cibernética, Hurel alerta que as discussões de segurança, inclusive sobre modelos que buscam revisar e/ou mensurar as capacidade de segurança cibernética, não estão isentas de dinâmicas mais amplas de competição global e fragmentação do sistema internacional. Assim, adverte que podem se tornar outro estágio de colonização, em termos de construção de modelos que não conseguem abarcar as particularidades dos países do Sul Global, os quais não se constituem como potências cibernéticas (2022, p. 80-81).

Nesse ponto, ressalta-se que especificamente para fins de estruturação do país na temática e de definição de prioridades e objetivos, a elaboração de uma ENSC é benéfica e auxilia a sua organização para o enfrentamento dos desafios nessa seara, e, dessa forma, coloca-se como um instrumento precioso para a canalização das políticas públicas necessárias. Já os indicadores, boas práticas e princípios associados pelos modelos estudados (OCDE, UIT e GCSCC) foram avaliados e considerados conforme as singularidades e contexto do nosso país, com a ressalva da delimitação da pesquisa que foca na prescrição de política pública referente ao marco legal e à autoridade nacional.

Dessa feita, a descrição dos modelos e a sua conjugação com a E-Ciber, permite apontar diversas questões que precisam ser adequadamente endereçadas. Reitera-se que não pela simples previsão e atendimento a qualquer um desses modelos apresentados, mas pela pertinência e relevância dentro do nosso contexto como país, especialmente pela nossa forma de Estado e pelo sistema jurídico pátrio. Nesse sentido, não é possível conclusão diferente que defender que o Brasil precisa de uma lei em sentido formal, ou seja, aprovada pelo Congresso Nacional.

A Lei precisa equacionar os seguintes pontos:

a) papéis e responsabilidade de todos os atores (setores público e privado, academia, sociedade civil e cidadãos);
b) promoção da adequada gestão de riscos pelos atores, considerando papéis e responsabilidades, especialmente pelos detentores e operadores de IECs;
c) as normas gerais contidas na Lei devem abarcar todos os Poderes e entes da Federação, devendo ser observadas pela União, Estados, Distrito Federal e Municípios;

d) identificação (criação ou designação de órgão ou entidade) e adequado mandato, ou seja, as competências necessárias, ao órgão ou entidade que será responsável nacionalmente pelo tema;
e) em caso de criação de nova entidade, a Lei deve abordar as receitas necessárias para a sua implantação e funcionamento, além de previsões de execução orçamentária mais genéricas, como, por exemplo, a impossibilidade de contingenciamento e a gestão da entidade para incluir suas necessidades orçamentárias na LOA e seu planejamento no PPA;
f) além de conferir o mandato para o órgão ou entidade com autoridade nacional no tema, caso necessário, deve conferir competências e responsabilidades a outros órgãos e/ou entidades que compõe a APF em temas relacionados;
g) estabelecimento do(s) mecanismo(s) de coordenação e cooperação intergovernamental e intersetorial, a fim de garantir a atuação coordenada e o necessário engajamento de todos atores; e
h) estabelecimento das competências para processos de elaboração, desenvolvimento, revisão, atualização, implementação, acompanhamento e prestação de contas relacionados à ENSC e planos associados.

Também não menos importante, o processo de elaboração e desenvolvimento desse anteprojeto de lei, de iniciativa do Poder Executivo, não pode delegar a consulta a todos atores interessados aos mecanismos de participação existentes no âmbito do processo legislativo. É necessário que esse texto chegue ao Congresso Nacional com um mínimo de amadurecimento sobre papéis e responsabilidade de atores, bem como sobre a autoridade responsável e mecanismos de coordenação e cooperação intragovernamental e intersetorial, sem os quais não será possível lograr a aprovação do projeto. O apoio dos setores e do próprio governo, bem como a sensibilização dos parlamentares sobre a importância do avanço nessa pauta, será essencial para viabilizar a sua ratificação.

Como precedente de um amplo processo de consulta realizado pelo Poder Executivo quando da elaboração de um anteprojeto de lei, cita-se o MCI, Lei nº 12.965, de 23 de abril de 2014, a qual estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil. Trata-se de tema que guarda relação estreita com a discussão em tela, uma vez que segurança cibernética é um dos temas centrais da Governança da Internet[13] e demanda a conscientização e o e engajamento multissetorial. O MCI é considerando a primeira lei que foi elaborada a partir

[13] Sobre o tema da Governança da Internet, sugere-se as obras de: Lucero (2011); Canabarro (2014); DeNardis (2014); Kurbalija (2016); e Mueller (2017).

de uma forma colaborativa entre os atores, aproveitando a Internet como plataforma para a participação, envolvendo consulta pública extensa antes do seu encaminhamento ao Poder Legislativo e continuando o engajamento durante o processo legislativo, envolvendo alguns milhares de comentários[14].

Aqui não apenas o MCI, mas a sua regulamentação, ou seja, o Decreto que regulamentou a Lei, Decreto nº 8.771, de 11 de maio de 2016, foi marcado por amplo processo de debate público que envolveu duas fases. A primeira, uma consulta mais aberta sobre os tópicos que o decreto necessitava regulamentar e, com base nos comentários e propostas, a segunda colocou a minuta de texto regulamentar para consulta. Assim como no desenvolvimento do texto do MCI, as propostas receberam alguns milhares de comentários de diversos atores[15].

Outro exemplo é a própria LGPD, resultante de extenso processo de consulta que se utilizou da mesma plataforma do MCI para realização de debate sobre o anteprojeto de lei, antes mesmo da sua submissão ao Parlamento[16]. Veja-se que tanto o MCI quanto a LGPD abrangem temas de importante intersecção com segurança cibernética e que compartilham de muitos desafios, para citar alguns, a necessidade de imposição de deveres a atores privados; a necessidade de estabelecer as competências de diversos órgãos e entidades; e a necessidade de conscientização e engajamento de diversos atores. Dessa forma, considerando o êxito da aprovação desses marcos, não há motivo para pensar que um processo diferente e sem esse amplo debate com toda a sociedade seria benéfico à finalidade pretendida, de estabelecimento de um verdadeiro marco nacional de segurança cibernética que enfrente as questões apontadas.

Inexiste dúvida de que o tema é urgente e de que o Brasil está atrasado na elaboração desse importante marco, cuja tentativa de elaboração e aprovação está documentada em instrumentos de 2018, como a E-Digital. Porém, a submissão de um anteprojeto sem o devido amadurecimento sobre obrigações, papéis, competências dos diversos órgãos e entidades, bem como sobre a designação ou criação do órgão ou entidade responsável nacionalmente certamente trará muitas dificuldades para a aprovação do projeto no âmbito do processo legislativo. Consequentemente, também adicionaria complexidade à implementação da Lei, sendo que o passado recente demonstra o sucesso dessas experiências de amplos debates em

[14] Maiores informações sobre o amplo processo de debate público, antes do início do processo legislativo, podem ser consultadas no Portal do Projeto "Pensando o Direto", uma iniciativa da Secretaria de Assuntos Legislativos do então Ministério da Justiça, disponível em: http://pensando.mj.gov.br/2014/04/23/o-que-e-o-marco-civil-da-internet/. Acesso em: 16 set. 2022.

[15] Especificamente sobre o processo de consulta desenvolvido para a elaboração do Regulamento do MCI, consultar: http://pensando.mj.gov.br/marcocivil/. Acesso em 16 set. 2022.

[16] O processo de consulta do então anteprojeto de lei sobre proteção de dados pessoais pode ser consultado em: http://pensando.mj.gov.br/dadospessoais/. Acesso em: 16 set. 2022.

temas correlatos. Nessa esteira, reforça-se que não há razão para pensar em caminho diverso a ser trilhado para a aprovação de um marco legal nacional de segurança cibernética.

Vale trazer à baila a recente publicação de novembro de 2022 do TCU que apresenta uma Lista de Alto Risco na Administração Pública Federal, alertando que o tema de segurança cibernética foi incluído na lista pela importância do desafio a ser enfrentado pela nação e que justifica atenção contínua da casa. Foram identificadas vinte e nove áreas, sendo segurança da informação e segurança cibernética uma delas. Nela é apontado que o "*arcabouço normativo vigente, em especial os decretos que orientam a atuação, não alcançam a Administração Pública como um todo, limitando-se, apenas, ao Poder Executivo federal*", fato que implica em uma carência de "*atos normativos que regulem os temas em todo o território nacional, incluindo os setores públicos e privado*" (TCU, 2022, p. 112).

Após a demonstração da imperiosa necessidade de um marco legal adequado, precedido do amplo e necessário debate público, passa-se à discussão da estrutura de governança institucional necessária.

4.2 AUTORIDADE NACIONAL

A presente seção busca discorrer sobre a necessidade de estabelecimento de uma estrutura de governança adequada para segurança cibernética, cabendo ressalvar, desde o princípio, que não se encontra dentro dos objetivos do presente trabalho o estudo dos modelos de governança existentes e a identificação do modelo ideal considerando a conjuntura brasileira. Busca-se tecer algumas contribuições sobre o tópico da governança para a instituição da respectiva Autoridade Nacional, sem adentrar especificamente em *benchmarking* de modelos.

Como visto, a E-Ciber indicou como ação estratégica o estabelecimento de um modelo centralizado de governança, com a criação de um Sistema Nacional de Segurança Cibernética, o qual teria as atribuições de promoção da coordenação nacional de diversos atores; promoção da análise conjunta dos desafios relacionados ao combate da criminalidade cibernética; auxílio no desenvolvimento de políticas públicas; criação de um Conselho Nacional de Segurança Cibernética; criação de grupos de debates sob coordenação do GSI/PR; estabelecimento de rotinas de verificações de conformidade no setor público e privado; e viabilização da convergência de esforços e iniciativas.

Outrossim, também atuaria complementarmente no tratamento de incidentes e promoção da educação e conscientização da sociedade, sendo que a E-Ciber indica que a coordenação nacional seria de responsabilidade do GSI/PR (BRASIL, 2020a). Veja-se que

mesmo com a edição de E-Ciber e demais marcos já detalhados, a insuficiência da coordenação intragovernamental e a resposta fragmentada permanece (DINIZ *et al*., 2014), como será a seguir demonstrado.

Não desconsiderando a premissa exposta na E-Ciber, de um modelo centralizado de governança nacional de segurança cibernética sob a coordenação do GSI/PR, reforça-se a necessidade do marco legal, nos termos da seção anterior, visto que não é possível implantar tal modelo com as atribuições supracitadas sem a promulgação de uma lei que confira ao GSI/PR essa competência. Como visto no Capítulo III, atualmente o GSI/PR permanece como responsável pelo planejamento, coordenação e supervisão das atividades de segurança da informação no âmbito da APF, com espeque na Medida provisória nº 1.154, de 1º de janeiro de 2023, relembrando-se que segurança cibernética é abrangida pela segurança da informação, consoante PNSI (BRASIL, 2018f).

De forma análoga, a criação do Sistema Nacional de Segurança Cibernética, com atribuições nacionais, não limitado ao nível federal também demanda uma lei, do contrário seu estabelecimento tratar-se-ia de um mecanismo sem as competências necessárias para o alcance das suas finalidades. Ou seja, a premissa básica de implementação do modelo indicado na E-Ciber é a edição de uma lei que possa concretizá-lo, um modelo de gestão centralizada com destaque para o GSI/PR como a autoridade nacionalmente responsável pelo tema e a existência de uma Sistema Nacional de Segurança Cibernética.

Especificamente sobre a centralização, Hurel ensina que não é incomum aos países identificarem um órgão de governança centralizada para segurança cibernética, porém as características do GSI/PR e a concentração de militares em seus quadros preocupa. Esse panorama corrobora a militarização do tema e a autora aponta a lacuna de diversidade para a implementação e construção da necessária coordenação, permanecendo as incertezas sobre o aporte da diversidade pelos mecanismos de participação elencados na E-Ciber e seu impacto nas deliberações. Nesse sentido, resta forçoso o estabelecimento de mecanismos de transparência, a fim de que a sociedade possa acompanhar não somente o processo de governança em si, mas também as ações de implementação (2021, p. 30).

Cabe também pontuar a existência de preocupações relacionadas à securitização da temática no contexto brasileiro (DINIZ *et al*., 2014; LOBATO; KENKEL, 2015; HUREL; LOBATO, 2015)[17]. No entanto, compartilha-se da opinião contrária (MALAGUTTI, 2022b).

[17] Interessante notar a existência de posicionamento relacionado à dessecuritização provocada pelo Marco Civil da Internet, o que implicaria em reconhecer que em algum momento o debate da construção do Marco Civil da Internet foi securitizado (VALES e SATER, 2017).

Uma hipótese para tal percepção de securitização seria decorrente da estruturação das capacidades no âmbito de defesa, com o reconhecimento do setor cibernético como um dos três estratégicos para a defesa nacional já em 2008 (BRASIL, 2008b) e, posteriormente, a estruturação do ComDCiber. Enquanto que a arquitetura institucional civil, que precisa abarcar uma série de perspectivas e áreas paradigmáticas para a segurança cibernética (por exemplo: conscientização dos usuários, educação, CSIRTS, padrões, etc.) continua relegada, sem a instituição do arcabouço jurídico necessário e a instituição responsável.

Dessa forma, a proeminência do ComDCiber em determinadas ações, como o EGC, pode conduzir à conclusão de securitização do tema. Uma hipótese alternativa e/ou complementar é a narrativa relacionada à realização dos grandes eventos no brasil (COPA FIFA 2014; Olimpíadas, 2016; etc.) e o Escândalo *Snowden*, que inclusive auxiliaram na institucionalidade da temática no âmbito militar. Na prática, verifica-se que o tema não recebe a atenção correspondente à sua relevância. Diferentemente, é a discussão da militarização do tema, a qual está diretamente associada à posição do GSI/PR, atribuições e ocupação dos seus cargos, como é explorado nessa seção 4.2 do Capítulo IV.

Apoiando a criação de uma Agência ou Autoridade Nacional de Cibersegurança, Malagutti sustenta que a entidade seria o ponto focal nacional para segurança cibernética e concentraria as iniciativas e orientação nessa seara, citando outras experiências civis que trabalham em coordenação com os órgãos correspondentes militares: Agencia Nacional de Segurança Cibernética da Itália; a Agência Nacional de Segurança dos Sistemas de Informação da França; e o Centro Nacional de Segurança Cibernética do Reino Unido (2022b, p .5-5).

Aqui, mesmo sem discutir modelos, pode-se acrescentar à discussão as competências e habilidades necessárias para que órgão e/ou entidade nacionalmente responsável tenha condições de cumprir sua missão institucional. Nessa esteira, a primeira questão que dialoga com os vários dos pontos de conclusão da necessidade de lei: o órgão e/ou entidade designada ou criada precisará coordenar diferente atores, com diferentes papéis e responsabilidades, devendo abarcar todos os Poderes e entes da Federação.

Ademais, esse órgão e/ou entidade precisará ter os recursos adequados para o cumprimento da sua missão institucional, os quais não se limitam aos recursos orçamentários, mas abarcam recursos humanos necessários para a implementação de todas as suas atribuições.

Veja-se que na Parte II da E-Ciber, que traz a análise dos eixos temáticos, particularmente o eixo de governança nacional apresenta um diagnóstico com relação ao modelo proposto, salientando que a criação de um sistema reunindo atores estatais e não estatais irá contribuir para o alinhamento estratégico e concertação das atividades, sendo atribuição do

Governo Federal o incentivo à discussão com o objetivo de fortalecimento institucional. Ademais, o próprio texto também aborda a necessidade de concepção de um órgão com capacidade e responsabilidade nacional e que conte com a participação de representantes de todos os setores da sociedade, enfatizando as competência civis, já que os assuntos associados à defesa e segurança nacionais permanecem sob a tutela do Ministério da Defesa, ou seja, mantém-se a dicotomia entre as dimensões civis e militares da segurança cibernética (BRASIL, 2020a).

Diante desse quadro, a própria E-Ciber aponta a viabilidade e eficácia de um modelo centralizado de governança de segurança cibernética indicando a sua adoção em diversos países, expressamente citando Coreia do Sul, EUA, França, Japão, Malásia, Portugal, Reino Unido e Singapura. Desse modo a análise assinala os bons resultados que a vivência desses países demonstra, com a centralização da condução do tema; e com autoridade para regulamentar e adotar ações específicas. O modelo promove a coordenação e a sinergia entre todos os atores, também contribuindo para notabilizar o caráter estratégico do tema e para consolidá-lo como assunto de Estado (BRASIL, 2020a).

Especificamente sobre a realidade brasileira e sobre o Governo Federal, o instrumento realça a atuação do GSI/PR, indicando que desde 2006 desenvolve diversas atividades relacionadas e congregaria vasta experiência em diversos campos de segurança da informação, inclusive no campo de segurança cibernética. Como ações que o GSI/PR desenvolve via então DSI, a E-Ciber cita o estudo e elaboração de normativos como instruções normativas, normas complementares, estratégias e políticas no seio da APF (BRASIL, 2020a).

Com base nesse quadro de viabilidade e eficácia da instituição de um modelo centralizado, apoiado inclusive nas experiências de vários países que lideram as capacidades em segurança cibernética[18], aliado à experiência e atuação do GSI/PR, a E-Ciber expressa a conclusão de que não é necessária a criação de novo organismo governamental, devendo-se tão somente fomentar o redimensionamento da estrutura do GSI/PR, a fim de que tenha condições de atuar em âmbito nacional (BRASIL, 2020a).

Ademais, outro elemento importante nessa discussão de modelo de governança aparece nesse trecho da E-Ciber ao expressamente mencionar a desnecessidade de "*criação de novos e dispendiosos organismos*", ou seja, surpassa-se a discussão sobre a necessidade e utilidade de

[18] Considerando os resultados da quarta edição do Índice Global de Segurança Cibernética, os países listados como exemplo de centralização de governança e de bons resultados do modelo figuram no topo do ranking, integrando posições que refletem da primeira à décima quarta posição. Considerando o ranking, os países supracitados figuram no Índice na seguinte ordem: EUA – 1º; Reino Unido – 2º; Coréia do Sul – 4º; Singapura – 4º; Malásia – 5º; Japão – 7º; França – 9º e Portugal – 14º (ITU, 2021b, p. 25).

um novo órgão e/ou entidade com o argumento do dispêndio de recursos públicos para justificar a atribuição da governança nacional ao GSI/PR.

Retoma-se que a E-Ciber contém, além da estratégia propriamente dita (visão, objetivos e AEs), uma primeira parte destinada ao diagnóstico e uma segunda parte direcionada à análise dos eixos temáticos, seção justamente na qual os trechos supracitados são encontrados. Não há no texto, nem em qualquer outro documento, consideração e avaliação sobre os benefícios e limitações dessa concepção que vislumbra o GSI/PR como macrocoordenador nacional. Nesse sentido, considerando a composição do documento, seria oportuno que fosse travada essa discussão, não existindo qualquer enfrentamento sobre desafios da atribuição da governança centralizada ao GSI/PR, salvo sob o aspecto de conferência do mandato legal, traduzido na necessidade de lei em sentido formal, aprovada pelo Congresso Nacional.

Continuando o raciocínio, cabe ainda trazer que a E-Ciber, após defender o redimensionamento da estrutura do GSI/PR, a fim de que possa atuar em nível nacional, aponta a necessidade urgente de uma lei no tema, justamente para endereçar as competências, particularizando as atribuições; indicar os mecanismos que permitirão o diálogo com a sociedade; e viabilizar, com a participação de todos os entes nacionais, que o GSI/PR exerça seu papel de macrocoordenador estratégico (BRASIL, 2020a).

Dessa feita, o GSI/PR, de maneira estruturada e convergente, promoveria o alinhamento e apoiaria a evolução de todo país na seara. Ponto não menos relevante diz respeito aos recursos, pontuando o documento sobre necessidade e urgência da priorização do tema pelo Governo Federal, para aplicação de recursos em segurança cibernética, sem adentrar em quais áreas demandariam e/ou necessitariam de priorização (BRASIL, 2020a).

Por fim, um último apontamento decorrente diretamente do texto da E-Ciber nessa questão, frisa novamente a necessidade de mecanismos de viabilização do engajamento da sociedade, citando-se como recomendação da E-Ciber a criação de um Conselho Nacional de Segurança Cibernética. Esse abarcaria todos atores, estatais e não estatais, com a finalidade de uma visão mais ampla, inclusiva e abrangente, e que possa traduzir as necessidades do país, também incentivando a constituição de grupos de debates sob a coordenação do GSI/PR, com o intuito de congregar especialistas de diferentes setores (BRASIL, 2020a).

Nos termos supracitados, a motivação para a escolha do GSI/PR como órgão coordenador nacional centra-se na experiência, especialmente do DSI, no desenvolvimento de estudos, normativos, normas complementares, estratégias e políticas no âmbito da APF, acrescida do argumento de evitar desnecessário dispêndio de recursos, o que aconteceria com a "*criação de novos e dispendiosos organismos governamentais*". No entanto, a própria E-Ciber

reconhece que a estrutura do GSI/PR é insuficiente para a missão, sendo necessário o seu redimensionamento, o que também implica em dispêndio de recursos, não havendo maiores detalhes no texto sobre como seria configurado o redimensionamento e o seu respectivo impacto orçamentário.

Transcorridos três anos da aprovação da E-Ciber, nem a Lei de Segurança Cibernética, nem qualquer outra lei ampliando as competências do GSI/PR foi aprovada. No entanto, cumpre observar que a estrutura temática do GSI/PR, sem qualquer redimensionamento até 31 de dezembro de 2022, sofreu modificações em 1° de janeiro de 2023, já no contexto no novo Governo do Presidente Luiz Inácio Lula da Silva.

Como já relatado anteriormente, o Decreto n.° 11.331, de 1° de janeiro de 2023, elevou o *status* do tema no âmbito do GSI/PR, criando uma Secretaria específica, o que implica em mais recursos, inclusive de mais cargos destinados à temática. Como a maioria dos novos cargos, inclusive de secretário e de diretor, ainda está vaga até a data de finalização da tese, não é possível tecer considerações sobre a composição dos mesmos. Muito menos sobre a adequação do redimensionamento frente à missão idealizada para o GSI/PR.

Portanto as questões que se colocam são a capacidade e a habilidade do GSI/PR em realizar essa coordenação entre todos os diferentes atores, os quais não se limitam ao setor público; e a alocação dos recursos adequados ao GSI/PR. Em relação ao primeiro ponto, Hurel salienta os desafios que circundam a atribuição da coordenação nacional ao GSI/PR, em face da permanência da fragilidade da sua relação com a sociedade civil, com apontamentos frequentes de falta de transparência e de militarização da sua agenda. Tal fragilidade representa um obstáculo significativo para o desenvolvimento de uma cultura de segurança cibernética. Alerta ainda que mecanismos formais e informais podem assistir na construção de confiança entre os atores, mas sua implementação é cercada por ceticismo (2021, p. 21), como, por exemplo, com a instituição do Conselho Nacional de Segurança Cibernética, a ser criado pelo Sistema Nacional de Segurança Cibernética.

Outrossim, a autora ainda ressalva que as incertezas abraçam esses mecanismos de participação, no tocante à funcionalidade e ao seu impacto, sendo ainda maiores as dúvidas sobre a participação da academia e da sociedade civil (2021, p. 29), recordando que a consulta pública da E-Ciber ficou aberta à participação popular por menos de trinta dias e questiona como as contribuições e comentários foram incorporados à Estratégia (2021, p. 19).

Nessa esteira, verifica-se o receio de que o órgão indicado para o papel essencial de coordenação nacional não tenha condições de dialogar com todos os atores, característica

fundamental para que se possa falar de uma governança efetiva de segurança cibernética em termos de país.

Veja-se que dentre os sete pontos fracos da E-Ciber apontados por Hurel, três referem-se à presente discussão, pois apontam: "*falta de confiança e desafiadora interlocução entre o GSI e grupos da sociedade civil*"; "*incerteza sobre a capacidade do GSI de coordenar uma gama tão abrangente de atividades*"; e "*indefinição sobre o conteúdo a ser apresentado em uma Lei de Segurança Cibernética*" (2021, p. 32) e, correspondentemente, a autora defende nas recomendações o estabelecimento de canais de diálogo, destacando a criticidade dessa interlocução e a avaliação das capacidades do GSI (2021, p. 34).

Com relação ao segundo ponto, ou seja, aos recursos, importa lembrar que GSI é órgão essencial da Presidência da República, não possuindo quadro próprio de servidores. Portanto, não realiza concurso público para o provimento dos seus cargos, utilizando outros processos para preenchimento desses cargos.

Dentro desse contexto, destaca-se a requisição de militares das Forças Armadas e pessoal civil, a qual é irrecusável e deve ser prontamente atendida, salvo hipóteses previstas em lei, nos termos do art. 22 e 23 do Decreto nº 9.668, de 2 de janeiro de 2019, que aprovou a Estrutura Regimental e o Quadro Demonstrativo dos Cargos em Comissão e das Funções de Confiança do Gabinete de Segurança Institucional da Presidência da República e altera o quantitativo de Gratificações de Exercício de Cargo em Confiança devida a Militares – RMP (BRASIL, 2019a). Esse Decreto foi revogado pelo Decreto nº 11.331, de 1º de janeiro de 2023, o qual manteve as prerrogativas de requisição (BRASIL, 2023b).

Dessa forma, não há equívoco em dizer que o provimento dos cargos se dá pela prerrogativa de requisição da Presidência da República, inexistindo uma carreira própria de servidores especializados para atuação nessa seara, o que certamente é um ponto importante a ser considerado diante da complexidade do tema e das diversas dimensões que abarca. Ademais, é inegável que os cargos do GSI/PR são tradicionalmente providos através da requisição de militares.

À título de exemplo, até 31 de dezembro de 2022, os cargos de Assessor Especial de Segurança da Informação, Diretor do Departamento de Segurança da Informação, Diretor-Adjunto eram ocupados por militares, assim como duas das três coordenações-gerais do DSI[19], o que demonstra a proeminência de militares na área responsável pela coordenação civil do

[19] Consulta realizada na página da composição do GSI/PR, disponível em: https://www.gov.br/gsi/pt-br/composicao/departamento-de-seguranca-da-informacao. Acesso em: 18 set. 2022.

tema, os quais ocupavam até o final do exercício de 2022, cinco dos seis cargos de mais alto nível relacionados à segurança cibernética.

Em relação à composição atual, não é possível proceder o mesmo e exame, uma vez que que a maioria dos cargos da nova Secretaria de Segurança de Informação e Cibernética permanece vaga e a consulta ao site do GSI/PR ainda não está disponível. Como exemplo, cita-se que o cargo de secretário (novo) e de diretor, no agora denominado Departamento de Segurança da Informação e Cibernética, ou seja, os dois cargos de mais alto nível no âmbito da APF nessa seara, ainda não foram providos[20].

Um outro aspecto que não pode ser desconsiderado é a rotatividade dos militares que impacta no provimento dos cargos e na continuidade da implementação das atividades. Portanto, considerando a militarização dos cargos associados à temática e a rotatividade inerente à carreira desses servidores, a adequação de recursos humanos do GSI/PR torna-se outro obstáculo à missão pretendida, a qual demanda interlocução crucial com todos atores, especialmente a sociedade civil, e exige recursos qualificados para tal missão, sendo a rotatividade um desafio adicional à consecução da visão estabelecida.

Como experiência recente na criação de órgãos para coordenação de temas nacionais, cabe lembrar da experiência da constituição da ANPD, a qual foi inicialmente criada como órgão da APF integrante da Presidência da República, sem aumento de despesa e, posteriormente, com o amadurecimento da sociedade e a sensibilização do governo e do Congresso Nacional, alterada para autarquia de natureza especial, dotada de autonomia técnica e decisória, nos termos do art. 55-A da LGPD, com alterações posteriores (BRASIL, 2022a).

Nessa linha, um caminho alternativo que se coloca, é a criação de órgão específico na Presidência da República, acolhendo-se como precedente a criação da ANPD, e reavaliação a curto e médio prazo sobre sua transformação em uma autarquia de natureza especial. Em que pese ainda vinculada à Presidência, ao menos inicialmente, a sua separação do GSI/PR poderia ser benéfica no tocante à desmilitarização nos seus cargos, considerando a proeminência de militares na sua ocupação. Tal providência poderia facilitar a interlocução com a sociedade civil, embora o órgão permanecesse com a prerrogativa de requisição de servidores, recurso utilizado pela ANPD para provimento de seus cargos.

A criação de uma autarquia exige lei, atribuindo personalidade jurídica, patrimônio e receita próprios para a execução de atividades da Administração Pública que demandem gestão

[20] O novo organograma resultante do Decreto n.º 11.331, de 1º de janeiro de 2023, já está disponível no site do GSI/PR em: https://www.gov.br/gsi/pt-br/assuntos/acervo/imagens/organograma-gsi-1.jpg/view. Acesso em: 04 fev. 2023. O provimento e vacância dos cargos pode ser consultada em: https://www.gov.br/gsi/pt-br/acesso-a-informacao/institucional/quem-e-quem-1. Acesso em: 04 fev. 2023.

descentralizada administrativa e financeira, nos termos do art. 5°, I, do Decreto-Lei nº 200, de 25 de fevereiro de 1967, que dispõe sobre a organização da Administração Federal, estabelece diretrizes para a Reforma Administrativa e dá outras providências (BRASIL, 1967). No caso da ANPD, seu regime especial decorre da sua autonomia técnica e decisória. Em outro exemplo, a natureza autárquica especial conferida à Anatel, decorre da sua independência administrativa, ausência de subordinação hierárquica, mandato fixo, estabilidade de seus dirigente e autonomia financeira, nos termos do art. 8º § 5º (BRASIL, 1997)[21].

Assim, a pergunta que deve ser feita é qual o tipo de estrutura organizacional é mais adequado ao contexto e à missão. As possibilidades resumem-se em órgão ou entidade. Ou seja, órgão da APF direta ou uma entidade de personalidade jurídica própria que comporia a APF indireta, sendo a última opção a escolha para as agências reguladoras nacionais e para a ANPD.

Embora não seja objeto do presente trabalho a escolha do modelo institucional, as características necessárias para a autoridade responsável pela coordenação nacional de segurança cibernética demandam a capacidade de coordenação nacional; a interlocução multissetorial; e os recursos adequados, orçamentários e humanos, fazendo com que o seu afastamento do GSI/PR pudesse trazer bons frutos ao modelo. Como elementos que corroboram a defesa desse afastamento, cita-se: militarização do provimento dos seus cargos; dificuldade de interlocução com a sociedade civil; inadequação dos recursos (reconhecida na E-Ciber); e rotatividade dos seus servidores, também decorrente da ausência de quadro próprio e da proeminência do provimento dos cargos com requisição de militares.

Ademais, não pode ser olvidado, conforme subseção 3.1 do Capítulo III, que já se encontra ativado o ComDCiber com a função de concentrar as atividades de planejamento, orientação, supervisão das atividades de defesa cibernética, cabendo assim a estruturação civil das capacidades em segurança cibernética brasileira. Portanto, seria naturalmente esperado, diante da estruturação das capacidades de defesa cibernética no contexto do Ministério da Defesa, que a dimensão civil, fosse salvaguardada e conduzida por servidores civis, sob pena de militarização dessa dimensão.

Outrossim, retoma-se também o argumento de dispêndio de recursos o que poderia levar à conclusão apressada da impossibilidade da criação de um novo órgão ou entidade. Ou seja, o debate sobre constituição de uma autoridade nacional estaria rejeitado desde seu primórdio visto que a gênese de qualquer novo órgão ou entidade importaria necessariamente em custo ao Erário.

[21] Sobre a autonomia e independência da Anatel e sobre a natureza jurídica especial das Agências Reguladoras ver Cravo (2007).

É forçoso insistir neste ponto. Não é possível cercear o debate sobre a arquitetura institucional pelo simples argumento de custo. O debate precisa ser travado sob a ótica de necessidade, adequação e eficácia do modelo de governança. Certamente a atribuição de competência a um órgão existente que não atende às necessidades e aos interesses do país é custosa ao Erário. Neste ponto relembra-se os ensinamentos de Bresser-Pereira no Capítulo I, no sentido de reforço do papel do Estado e eficiência do seu aparelho (BRESSER-PEREIRA, 1996, 1998, 2008; BRASIL, 1995).

Eventualmente, poderia ser adotado um modelo não centralizado composto por mais de um órgão ou entidade, no entanto não foi a opção identificada na E-Ciber, consoante visto no Capítulo III. Nessa foi sustentado o modelo centralizado, idealizando-se o GSI/PR como macrocoordenador nacional responsável tanto pela elaboração da E-Ciber, e de todas as políticas associadas (PNSI, PNSIC, ENSIC, PLANSIC, ReGIC, etc), quanto pela implementação, ainda que uma gama de outros órgãos e entidades tenham reconhecidamente um papel relevante a cumprir.

Retornando-se aos modelos estudados, para verificação de suas contribuições à estrutura de governança, inicia-se com o modelo da OCDE. Esse, como visto, refere-se à Recomendação de 2015 sobre Gerenciamento de Riscos de Segurança Digital para Prosperidade Econômica e Social, a qual traz uma série de princípios e diretrizes para as estratégias nacionais e que foi posteriormente desmembrada e atualizada em duas recomendações em apartado, já apresentadas na seção 2.1 do Capítulo II. As estratégias devem ser consistentes com os princípios da recomendação (conscientização, habilidades e empoderamento; responsabilidade; direitos humanos e valores fundamentais; cooperação; avaliação de risco e ciclo de tratamento; medidas de segurança; inovação; e preparação e continuidade).

Ademais, as ENSC devem ter o apoio do mais alto nível e articular uma visão clara e abrangente de todo o governo; ter como objetivo aproveitar a vantagem do ambiente digital para avançar na prosperidade econômica e social por meio da redução do risco digital; ser direcionadas a todos os atores e adequadas às pequenas e médias empresas e indivíduos; e resultar de uma abordagem coordenada intragovernamental e de um processo transparente envolvendo a todos atores (OECD, 2015, p. 9-12).

É justamente nesse nesses dois últimos pontos, que congregam o direcionamento e o engajamento de todos os atores, que reside a contribuição das Recomendações para a governança, visto que, uma vez mais, corrobora-se que o tema precisa do envolvimento de todos, sendo imprescindível que a estrutura de governança tenha condições de promover o diálogo e a participação dos mais diversos atores e, com transparência, considerar as suas

contribuições ao processo, tanto de implementação da visão estabelecida pela Estratégia Nacional, quanto de revisão e atualização da própria estratégia e instrumentos associados.

As Recomendações também endereçam as medidas que devem ser incluídas nas Estratégias Nacionais quanto à atuação do governo, os quais devem liderar por exemplo, fortalecer a cooperação internacional e assistência mútua; engajar-se com outros atores e criar as condições para que todos atores colaborem no gerenciamento do risco de segurança digital.

Embora a recomendação foque no conteúdo da Estratégia, não sendo direcionada à efetivação do processo de governança, várias ações citadas convergem para a discussão institucional já apresentada nessa subseção. Essa confluência é especialmente verificada quanto ao engajamento com outros atores e à criação das condições para que todos os atores colaborem no gerenciamento dos riscos de segurança digital. Isso demanda uma habilidade da estrutura institucional, independentemente de qual seja, de trabalho, diálogo e engajamento com os demais atores (OCDE, 2022b), necessidade que representa um grande desafio ao modelo atual centrado no GSI/PR, pelos motivos já expostos.

Cabe reiterar previsão constante da atualização das recomendações sobre as ENSC, que reforça a necessidade de um órgão com a clara atribuição na matéria (OCDE, 2022b). Nesse ponto, a Recomendação de 2022 defende que o(s) órgão(s) deve(m) ser responsável(is) pelo desenvolvimento e pela implementação, reafirmando a necessidade de garantia da coordenação necessária no âmbito do governo. Nota-se que a própria recomendação traz uma carga de flexibilidade, uma vez que destaca que pode ser: um(a) ou mais órgão(s)/entidade(s); e novo (criação de um órgão/entidade) ou já existente, sendo que nesse último caso, o órgão/entidade deve ser designado como responsável e receber as competências necessárias para sua atuação.

Ao considerar o sistema jurídico pátrio e a nossa organização da esfera estatal, a recomendação acima mais uma vez se direciona para a conclusão da imprescindibilidade de lei, assim como de uma autoridade responsável. Sendo essa última designada ou criada.

Continuando no caminho dos subsídios, o modelo da UIT, traduzido no *Guia para o Desenvolvimento de uma Estratégia Nacional de Segurança Cibernética - Engajamento estratégico em segurança cibernética* (ITU *et al.*, 2021), destaca como boa prática na área de governança o estabelecimento de uma autoridade competente dedicada responsável pela execução da Estratégia Nacional. Essa autoridade deve estar ancorada no alto nível no governo para prover direção, coordenação, ação, monitoramento e reportar sobre o progresso da estratégia.

Além disso, a autoridade deve atuar como uma entidade gestora que defina e clarifique papéis, processos, responsabilidades e tarefas necessárias à execução da estratégia, ressaltando

que, em muitos casos, essa autoridade precisa estar formalizada em uma política ou uma lei para receber o mandato necessário à sua missão, ponto extensamente discutido no subitem anterior desse Capítulo. Ademais, o Guia destaca a habilidade de envolver e dirigir diversos atores, o que também pode exigir legislação adicional, e o fato de que uma autoridade competente nacional de alto nível e bem estabelecida auxilia na coordenação e na cooperação intragovernamental (ITU, 2021, p. 35).

Por fim, retoma-se o modelo do GCSCC, base metodológica da E-Ciber. Dentro desse modelo, não existe nenhum aspecto, fator ou dimensão que especificamente enderece a questão da governança institucional nacional de segurança cibernética. Ainda assim, cabe ressaltar que no Fator ENSC, o Aspecto de Implementação e Revisão, um dos indicadores do Estágio Estabelecido é justamente a designação de um órgão de coordenação. Esse, precisa deter autoridade suficiente para exigir dos demais órgãos e entidades responsáveis as ações de implementação, além de abordar os recursos necessários de implementação. Outro elemento presente nesse aspecto, e considerado para fins de definição de maturidade, é o engajamento de diversos atores (não limitado a atores governamentais) na implementação da ENSC (OXFORD, 2021, p. 13).

Nessa esteira, embora limitadas as menções à governança institucional nacional no modelo do GCSCC, são apontadas as questões referentes à interlocução com outros atores não governamentais, aos recursos e à capacidade de coordenação da autoridade, especialmente pela demanda de envolver diversos órgãos e entidades que possuem competência em alguma das facetas desse fenômeno. Assim sendo, todos os modelos analisados apoiam e suportam as conclusões já apontadas da limitação do GSI/PR em tornar-se efetivamente a autoridade nacional nessa seara.

Além dos modelos, pontua-se novamente o delineamento da recente publicação de novembro de 2022 do TCU, constante da Lista de Alto Risco na Administração Pública Federal, que nesse tema afirma que a "*macroestrutura nacional responsável pela governança e gestão de Segurança da Informação e de Segurança Cibernética, apesar de atuante, não é adequada*". A publicação também reitera que o órgão responsável, GSI/PR, não alcança a APF como um todo, limitando-se ao Poder Executivo Federal. Ademais, ressalta a necessidade de uma estrutura, órgão ou entidade, com autoridade ampla, salientando a importância estratégica do tema para o país (TCU, 2022, p. 112).

Ao travar o debate sobre a política brasileira em segurança cibernética, Lobato também conclui de forma análoga que é desejável que o país desenvolva uma política mais coesa e que

supere a fragmentação da sua arquitetura institucional como fundamento de coerência das suas iniciativas (LOBATO, 2017, p. 27).

Por todo e exposto e da mesma forma que na subseção anterior, que endereçou a necessidade de um marco legal para o tema, sintetiza-se que o modelo de governança, partindo-se do pressuposto de adoção de um modelo centralizado indicado na E-Ciber, demanda uma Autoridade Nacional de Segurança Cibernética.

Assim, a instituição dessa Autoridade Nacional deve considerar os sete seguintes e imprescindíveis pontos:

a) autoridade deve ter mandato nacional previsto em lei;
b) o órgão ou entidade, criada ou designada, precisa ter as competências necessárias para o desempenho das suas funções;
c) a governança estabelecida precisa buscar a coordenação de todos os Poderes e entes da Federação;
d) o órgão ou entidade precisa deter a capacidade e habilidade de interlocução e engajamento com diferentes atores de diferentes setores da economia e sociedade;
e) a autoridade precisa dos recursos adequados para o desempenho das suas atividades, os quais não se limitam à dotação orçamentária. Não podem ser esquecidas as limitações existentes no modelo atualmente indicado em face das características peculiares do GSI/PR, especialmente da militarização do provimento dos seus cargos e da inerente rotatividade desses servidores; *vi*) a avaliação e escolha do modelo institucional não deve ser limitada à discussão do dispêndio e custo ao Erário do órgão ou entidade, sendo pertinente a discussão das características necessárias à relevância e ao efetivo desempenho das suas atividades; e
f) é necessário ser avaliada a pertinência da desmilitarização do órgão ou entidade, considerando que a autoridade precisa tratar das dimensões civis do fenômeno, ou seja, não endereçará os aspectos relacionados à defesa nacional e à segurança nacional, os quais são de competência do Ministério da Defesa e, mais especificamente, do ComDCiber, sem prejuízo da necessária e importante interlocução entre as duas esferas.

Nessa perspectiva, as premissas supracitadas não são o ponto de chegada da arquitetura institucional, mas representam o ponto de partida que deve ser considerado no aprofundamento das discussões sobre a governança adequada à realidade e contexto brasileiros, não podendo partir-se da importação de modelos sem a devida reflexão. Da mesma forma, também não pode ser afastada a discussão sobre a pertinência de criação de um novo órgão ou entidade somente

sob o argumento do custo ao Erário, sem considerar a complexidade dos desafios impostos e a importância do tema.

4.3 CONCLUSÕES PARCIAIS

O presente capítulo procurou apresentar a imprescindibilidade de existência de um Marco Legal na matéria, bem como da instituição de uma Autoridade Nacional de Segurança Cibernética. Essa condição decorre do confronto das contribuições dos modelos da Organização para a Cooperação e Desenvolvimento Econômico, da União Internacional de Telecomunicações e do Centro Global de Capacidade de Segurança Cibernética da *Oxford Martin School* da Universidade de Oxford, explanados no Capítulo II, com o Arcabouço Nacional Jurídico e de Políticas Públicas descrito no Capítulo III.

Dessa forma, em apertada síntese, o Capítulo centrou-se em duas questões fulcrais para as políticas públicas brasileiras em segurança cibernética: Marco legal e Autoridade Nacional de Segurança Cibernética, tópicos sobre os quais foram desenvolvidas as prescrições como contribuição específica da pesquisa. Ressaltou-se que essas duas proposições normativas permitirão que o Brasil, em um esforço de toda a nação, possa construir uma Estratégia Nacional de Segurança Cibernética (ENSC), formal e material, e assim, promover efetivamente uma cultura de segurança cibernética e, por consequência, viabilizar a Transformação Digital e o Desenvolvimento do país.

Marco Legal — quanto ao primeiro tópico, esse Capítulo corroborou a inarredável necessidade de Lei em matéria de segurança cibernética a ser aprovada pelo Congresso Nacional e apontou oito pontos de atenção que devem fazer parte do conteúdo mínimo desse novo Marco Legal. Como se viu, os pontos abarcaram, em resumo:

a) papéis e responsabilidade de todos atores, não se limitando à esfera estatal;
b) adequada e proporcional gestão de riscos por esses atores, considerando seus papéis e responsabilidades;
c) abrangência nacional incluindo todos Poderes e entes da Federação; *iv*) criação ou designação e adequado mandato para o órgão ou entidade responsável nacionalmente pelo tema;
d) atribuição das competências e responsabilidades aos demais órgãos e entidades que compõem a Administração Pública Federal;
e) estabelecimento de coordenação e cooperação intergovernamental e intersetorial;

f) definição de competências para todo o ciclo de vida associado à ENSC, ou seja, desde a sua elaboração até a prestação de contas da sua implementação, bem como de planos associados; e
g) em caso de criação de nova entidade, a Lei precisa endereçar as receitas necessárias e conter previsões sobre a execução orçamentária.

Com o endereçamento desses pontos, esperou-se sanar as existentes lacunas do Arcabouço Nacional Jurídico e de Políticas Públicas vigente, permitindo assim os fundamentos para o desenvolvimento de uma ação coordenada e abrangente do Estado Brasileiro na promoção de segurança cibernética. Esse esforço alavanca a Transformação Digital e fomenta a proteção das Infraestruturas Críticas, o que, como externalidade positiva, contribui para a segurança nacional e a defesa nacional.

Faz-se necessário esclarecer que a elaboração e aprovação da legislação necessária não é um ponto final, mas o início da caminhada e todos os desafios de implementação permanecem. No entanto, as premissas fundamentais estarão estabelecidas, permitindo o foco nas ações de implementação, as quais, atualmente, são inviabilizadas justamente pela inexistência dessa Lei, como se procurou demonstrar ao longo do texto.

Autoridade Nacional — no que tange à arquitetura institucional nacional, a despeito de não ter sido realizado estudo comparativo de outros modelos organizacionais adotados por diversos países, visto que ultrapassaria a delimitação do escopo da presente pesquisa, concluiu-se pela necessidade de uma Autoridade Nacional de Segurança Cibernética. Ademais, elaborou-se contribuições para a discussão sobre o perfil institucional necessário para que autoridade possa atuar em âmbito nacional.

Essas contribuições basearam-se nos três modelos estudados e no Arcabouço Nacional Jurídico e de Políticas Públicas existente, inclusive ponderando experiências recentes do contexto brasileiro. Essa conjuntura permitiu tecer apontamentos sobre competências e características necessárias que a autoridade precisa deter. Esses delineamentos permanecem válidos independentemente da autoridade ser resultado da criação de um novo órgão ou entidade, ou da designação de um órgão ou entidade já existente, partindo-se da premissa de centralização da coordenação, a qual foi manifestada expressamente na Estratégia Nacional de Segurança Cibernética (E-Ciber).

Cumpre agora elencar os elementos norteadores que definem o perfil da Autoridade Nacional de Segurança Cibernética. Sustentou-se sete quesitos:

a) mandato nacional previsto em lei;
b) competências necessárias para o desempenho das suas funções;

c) viabilização da coordenação nacional com abrangência de todos os Poderes e entes da Federação;
d) capacidade e habilidade de interlocução com todos atores e setores;
e) recursos adequados, com destaque especial aos recursos humanos e a forma de provimento dos seus cargos;
f) escolha do perfil institucional (órgão ou entidade; novo ou existente) não somente atrelada ao custo ao Erário; e
g) avaliação da desmilitarização, considerando as competências do órgão ou entidade de endereçar a perspectiva civil dos desafios relacionados à segurança cibernética.

Interessante relembrar um exemplo institucional recente, a criação da Autoridade Nacional de Proteção de Dados, a qual nasceu como novo órgão da Presidência da República, sem aumento de despesa em 2019 e, em 2022, foi transformada em autarquia de natureza especial, ou seja, uma nova entidade, transpondo o paradigma do dispêndio de recursos. Nessa esteira, caso o argumento do aumento de despesa não pudesse ser afastado desde o primórdio, poderia ser utilizada abordagem semelhante, permitindo o amadurecimento das discussões e da arquitetura institucional.

De outra banda, foi forçosa a conclusão de que o perfil de governança atual com o indicativo do Gabinete de Segurança Institucional da Presidência da República (GSI/PR) como macrocoordenador nacional carece de competências, capacidades e recursos necessários. Essa deficiência é decorrente de características inerentes ao provimento dos seus cargos, trazendo dificuldades adicionais para a estabilidade e continuidade do desenvolvimento e manutenção dos esforços em segurança cibernética.

Ademais, também se advertiu que a militarização do provimento dos cargos do GSI/PR acrescenta outra camada de preocupação, considerando que a autoridade terá como atribuição a dimensão civil do problema e a perspectiva militar já possui órgão específico, qual seja o Comando de Defesa Cibernética (ComDCiber).

Por todo o exposto, a discussão travada neste Capítulo IV conduziu para a inevitabilidade de uma Lei em Segurança Cibernética, assim como para a indispensabilidade de uma Autoridade Nacional de Segurança Cibernética, com um perfil institucional adequado. Somando-se a essas duas premissas, elaborou-se uma prescrição de princípios para o Marco Legal e para Autoridade Nacional, com o objetivo de contribuir para o desenvolvimento das capacidades e da implementação das políticas públicas em segurança cibernética, finalizando assim o presente esforço.

5 CONCLUSÕES

Em retrospectiva, percebe-se que a pesquisa foi alicerçada em três acúmulos. Conquanto distintos, vislumbra-se uma significativa confluência entre eles na elaboração do trabalho. São eles: Marco Teórico; Modelos de Estratégias Nacionais de Segurança Cibernética (ENSC); e Arcabouço Nacional Jurídico e de Políticas Públicas.

Cabe, pois, uma brevíssima digressão de modo a situar esses acúmulos na construção do problema e da hipótese de pesquisa.

No primeiro acúmulo, o Marco Teórico da pesquisa operou a sistematização da literatura pertinente, a fim de inserir o tópico de segurança cibernética no contexto da Quarta Revolução Industrial e como elemento basilar da Transformação Digital. E, consequentemente, da oportunidade de Desenvolvimento dos países.

Procurou-se demonstrar que a segurança cibernética é o fundamento para que qualquer país possa se beneficiar de toda potencialidade oferecida pelas tecnologias disruptivas — que, como referido, introduzem inovações que conduzem a novas aplicações e novos mercados. Essas tecnologias, como toda inovação, carregam consigo uma dupla face: ao par das oportunidades, os desafios.

De fato, não é possível eliminar completamente todos os riscos associados à crescente e massiva utilização das Tecnologias de Informação e Comunicação. Portanto, faz-se necessário o adequado gerenciamento e mitigação desses riscos. É precisamente essa conjuntura que explica e justifica a predominância da temática nas agendas das organizações internacionais, inclusive sob o aspecto securitário.

Diante desse quadro, no curso da tese, sustentou-se o desenvolvimento de ENSCs como uma das respostas domésticas a esses desafios. Tais respostas apoiam-se em modelos construídos pela comunidade internacional.

O segundo acúmulo traduziu-se no estudo dos modelos de ENSCs. Nesse sentindo, descreveu-se três iniciativas internacionais que auxiliam países na construção desse instrumento estratégico, denominando-as de modelos.

Assim, foram designadas como tal: *i*) a Recomendação de 2015 da Organização para a Cooperação e Desenvolvimento Econômico (OCDE) sobre Gerenciamento de Riscos de Segurança Digital para Prosperidade Econômica e Social; *ii*) o Guia para o Desenvolvimento de uma Estratégia Nacional de Segurança Cibernética elaborado pela União Internacional de Telecomunicação e parceiros; e *iii*) o Modelo de Maturidade de Capacidade de Segurança

Cibernética do Centro Global de Capacidade de Segurança Cibernética da *Oxford Martin School* da Universidade de Oxford.

Acerca do primeiro modelo, ainda se destaca dois pontos. O primeiro refere-se à recente atualização e desmembramento dessa Recomendação de 2015 em duas: Recomendação do Conselho sobre Gerenciamento de Riscos de Segurança Digital; e Recomendação do Conselho sobre Estratégias Nacionais de Segurança Digital, as quais integram o novo Arcabouço de Segurança Digital da organização, lançado em dezembro de 2022, já aderidas pelo Brasil.

O segundo ponto retoma que, embora as recomendações não se constituam como instrumentos vinculantes, a adesão pelo Brasil às recomendações da OCDE implica em um compromisso político do país de empreendimento de esforços de implementação. Condição cuja importância é reforçada ao considerar que o país se encontra em processo de adesão à organização.

Com a análise sistemática dos três modelos, concluiu-se que, a despeito das suas distinções, predomina a convergência. Desse modo, foram referidas diferenças, notadamente quanto à abrangência e ao detalhamento. Também restou explicitado que os modelos não podem, e não devem, ser utilizados como uma prescrição incondicional a ser perseguida, ignorando-se circunstâncias de tempo e espaço. Afinal, não se pode desconsiderar o contexto particular de cada país quando da sua avaliação e utilização.

Dessa forma, apontou-se que esses três modelos podem auxiliar os países no desenvolvimento das suas capacidades. Posto que seu emprego crítico e criador viabiliza o aporte de importantes subsídios para elaboração e implementação de uma ENSC. E, portanto, reconheceu-se a relevância de conhecer, estudar e entender cada um desses modelos. Reiterou-se que os modelos devem ser conformados à realidade de cada nação, sem se olvidar do compromisso brasileiro manifestado na aderência às recomendações da OCDE.

Aqui cumpre reiterar o alinhamento da tese à advertência de Bresser-Pereira, ao alertar que não se deve acolher instituições e reformas exportadas. Ao contrário, podem e devem ser importadas, o que implica necessariamente na sua adaptação (2004). De forma análoga, faz-se a defesa da importação de modelos no presente trabalho, servindo como ponto de partida, não de chegada, da construção de esforços nacionais.

O último acúmulo refere-se à análise do Arcabouço Nacional Jurídico e de Políticas Públicas. Nesse enfoque, também se partiu de uma visão mais abrangente para chegar à Estratégia Nacional de Segurança Cibernética (E-Ciber) e, posteriormente, apresentou-se os demais instrumentos e políticas relacionados.

Aqui se insiste na conclusão parcial: o Arcabouço Nacional Jurídico e de Políticas Públicas brasileiro padece de timidez, limitação e insuficiência. A timidez advém da forma como o tema é tratado diante de todos os riscos que necessariamente precisam ser geridos e a magnitude do desafio que se descortina. A limitação resulta da abrangência restrita à Administração Pública Federal e, portanto, não engloba os demais Poderes, nem entes da Federação. Muito menos os atores não estatais. Por fim, a insuficiência manifesta-se na incapacidade de expressar resposta eficiente.

Embora tímido, limitado e insuficiente, o Arcabouço é vasto e complexo, sendo elaborado o "Quadro 3: Síntese do Arcabouço Nacional Jurídico e de Políticas Públicas" ao final Capítulo III para facilitar a compreensão do mapeamento e da análise que foi operacionalizada naquele Capítulo.

Do somatório dos três acúmulos, extraíram-se dois produtos: a hipótese da pesquisa; e o conteúdo normativo da tese. Isto foi objeto do Capítulo IV — Análise e Prescrição de Política Pública.

A hipótese foi revelada na constatação de que conquanto exista um instrumento formal denominado Estratégia Nacional de Segurança Cibernética (E-Ciber), essa não se constitui materialmente enquanto tal, respondendo ao problema de pesquisa que questionou a existência material de uma ENSC no Brasil. Nesse ponto, aclara-se a utilização da dicotomia formal *versus* material, para apresentar a diferença entre o cumprimento de uma formalidade, procedimento e rito (aspecto formal), em contraste com o conteúdo e a substância de determinado ato (aspecto material).

O Conteúdo normativo concretizou-se nas prescrições de políticas públicas: Marco Legal e Autoridade Nacional de Segurança Cibernética. Atesta-se que elas não recaíram na ENSC em si, mas em conteúdo ético do processo necessário para produzi-la. Como se buscou evidenciar, o desenvolvimento de uma ENSC não é um esforço individual, seja de um cidadão ou instituição, mas uma construção coletiva de uma nação. Dessarte, a prescrição retrocede passos, com o intuito prover as condições necessárias para a sua formulação. É essa percepção que se buscou traduzir com o título do trabalho.

A proposição normativa procurou se ater ao Princípio da Legalidade, sustentando a aprovação de um Marco Legal e de instituição de uma Autoridade Nacional de Segurança Cibernética, delimitando um conteúdo mínimo que cada uma dessas prescrições deveria abarcar, as quais consubstanciam os desafios da temática e do contexto brasileiro.

No tocante à primeira prescrição, de estabelecimento do Marco Legal de Segurança Cibernética, resgata-se que o conteúdo ético associado envolve minimamente o endereçamento de oito pontos:

a) papéis e responsabilidade de todos atores, não se limitando à esfera estatal;
b) adequada e proporcional gestão de riscos por esses atores, considerando seus papéis e responsabilidades;
c) abrangência nacional incluindo todos Poderes e entes da Federação;
d) criação ou designação e adequado mandato para o órgão ou entidade responsável nacionalmente pelo tema;
e) atribuição das competências e responsabilidades aos demais órgãos e entidades que compõem a Administração Pública Federal;
f) estabelecimento de coordenação e cooperação intergovernamental e intersetorial;
g) definição de competências para todo o ciclo de vida associado à ENSC; e
h) em caso de criação de nova entidade, a Lei precisa endereçar as receitas necessárias e conter previsões sobre a execução orçamentária.

Já com relação à segunda prescrição, de instituição da Autoridade Nacional de Segurança Cibernética, rememora-se que o conteúdo ético atenta para sete quesitos:

a) mandato nacional previsto em lei;
b) competências necessárias para o desempenho das suas funções;
c) viabilização da coordenação nacional, englobando todos os Poderes e entes da Federação;
d) capacidade e habilidade de interlocução com todos atores e setores;
e) recursos adequados, com destaque especial aos recursos humanos e à forma de provimento dos seus cargos;
f) escolha do perfil institucional (órgão ou entidade; novo ou existente) não limitada pelo argumento de custo ao Erário; e
g) avaliação da desmilitarização, considerando as competências do órgão ou entidade de endereçar a perspectiva civil dos desafios relacionados à segurança cibernética.

Com relação ao último quesito, de avaliação da desmilitarização, alerta-se para o fato de que a capacidade institucional vislumbrada pela E-Ciber, com o Gabinete de Segurança Institucional da Presidência da República (GSI/PR) como macrocoordenador nacional, padece da carência de competências, capacidades e recursos necessários. Adicionalmente, a militarização inerente ao provimento dos cargos do órgão desencadeia preocupações, considerando a dimensão civil do fenômeno que precisa ser endereçada. Esse cenário não

favorece a estabilidade e a continuidade do desenvolvimento e manutenção dos esforços em segurança cibernética.

Em nenhum momento considerou-se quaisquer das proposições acabadas. Como o próprio título expressou, trata-se de construção a ser empreendida por todo o país. Essas prescrições despontam como sustentáculo latente desse processo.

Dessa forma, a contribuição genuína do trabalho pode ser vislumbrada sobre três perspectivas: consolidar e compreender os três principais modelos utilizados internacionalmente para a elaboração de Estratégias Nacionais de Segurança Cibernética; consolidar e descrever o arcabouço brasileiro vigente no tema, incluindo também um histórico dos marcos; e, finalmente, apoiando-se nesses dois elementos pressupostos, prover a base para confrontar a duas questões essenciais: Marco Legal e Autoridade Nacional de Segurança Cibernética.

Como fundamento da relevância social do trabalho, aponta-se que, além importância de compreender o arcabouço doméstico existente de enfrentamento dos problemas associados à segurança cibernética e os modelos que apoiam esses desenvolvimentos, adicionalmente, o trabalho reveste-se de pertinência temporal.

Veja-se que a E-Ciber encerrará sua validade no final do exercício de 2023, ano de defesa da tese, possibilitando assim que a pesquisa que foi realizada sirva como insumo ao processo de revisão da atual estratégia e edição de nova, com vigência a partir de 2024, bem como das outras políticas relacionadas e necessárias, as quais se traduzem nas duas prescrições já enunciadas: Marco Legal e Autoridade Nacional de Segurança Cibernética.

Cabe lembrar que se trabalhou com o horizonte de vigência da E-Ciber atualmente existente, mas com a cautela de que o atual governo empossado no início de 2023 pode decidir diferentemente, considerando que essa política pública foi emanada no governo anterior e se projeta no tempo para o mandato atual. De toda sorte, as contribuições permanecem válidas, seja pela análise dos modelos, seja por possibilitarem ao leitor navegar pelo Arcabouço Nacional Jurídico e de Políticas Públicas existente.

Nesse ponto, ressalva-se a escassa bibliografia que aborda o desenvolvimento de arcabouços estratégicos e organizacionais em segurança cibernética sob a perspectiva civil. Em termos de bibliografia nacional na temática, a restrição fica ainda mais destacada, existindo um número muito limitado de referências, fato que corrobora a relevância da pesquisa. No entanto, salienta-se que a sua maior contribuição reside na prescrição de política pública em dois aspectos: marco legal e autoridade nacional, os precisam ser invariavelmente confrontados pelo país, consoante se procurou demonstrar no presente esforço.

A magnitude dessa construção abre todo um leque de estudo, que pode constituir um programa de pesquisa. Interessa sublinhar que tal valoração se dá não pelo aporte da tese, mas pelo tamanho do desafio.

Aqui se compartilha possibilidades de pesquisas futuras, como estudo de modelo institucional para a Autoridade Nacional de Segurança Cibernética; *benchmarking* internacional de arquitetura institucionais; e acompanhamento da implementação do Arcabouço Nacional Jurídico e de Políticas Públicas.

Importa ressaltar que o Brasil deve buscar um caminho que atenda aos seus interesses, suas necessidades e suas particularidades. Ademais, experiências bem-sucedidas como o desenvolvimento do Marco Civil da Internet (MCI), bem como a aprovação da Lei Geral de Proteção de Dados (LGPD) e a instituição da Autoridade Nacional de Proteção de Dados (ANPD), demonstram que as prescrições normativas propostas, embora não acabadas, são passos iniciais que podem ser desenvolvidos, contribuindo sobremaneira para a construção das capacidades brasileiras em segurança cibernética.

Veja-se que a experiência do desenvolvimento do MCI, bem como sua respectiva regulamentação, e da LGPD demonstram a viabilidade e importância de um processo de construção nacional de marcos legais. Ao passo que a experiência da instituição da ANPD, inicialmente como órgão e, posteriormente, como entidade com personalidade jurídica própria, demonstra o amadurecimento da sociedade na temática e a bem-sucedida transposição à rejeição de criação de novas entidades estatais. Tais experiências iluminam as prescrições normativas aqui defendidas.

A construção de capacidades não se constitui um fim em si mesma, mas busca garantir que o país possa se beneficiar da Transformação Digital e promover o seu Desenvolvimento e a sua inserção internacional, para o bem-estar de toda a população brasileira.

REFERÊNCIAS

ANTONAKAKIS, Manos; APRIL, Tim; *et al.* Understanding the mirai botnet. *In*: *26th USENIX security symposium (USENIX Security 17)*. 2017. p. 1093-1110. Disponível em: https://www.usenix.org/system/files/conference/usenixsecurity17/sec17-antonakakis.pdf. Acesso em: 19 out. 2022.

AYRES PINTO, Danielle Jacon; GRASSI, Jéssica Maria. Guerra cibernética, ameaças às infraestruturas críticas e a defesa cibernética do Brasil. *Revista Brasileira de Estudos de Defesa*, Brasil, v. 7, p. 103-131, 2020. Disponível em: https://rbed.abedef.org/rbed/article/view/75178/42133. Acesso em: 29 dez. 2022.

AYRES PINTO, Danielle Jacon; PAGLIARI, Graciela de Conti; GRASSI, Jéssica Maria. Apresentação. *In*: AYRES PINTO, Danielle Jacon; PAGLIARI, Graciela de Conti; GRASSI, Jéssica Maria (org.). *A geopolítica das estratégias em defesa cibernética*: como EUA, China, Rússia e Israel protegem seu ciberespaço. Rio de Janeiro: Alpheratz, 2021. p. 11-14.

BARRY, Charles; ZIMET, Elihu. Military Service Cyber Overview. *In*: WENTZ, Larry; BARRY, Charles; STARR, Stuart. *Military Perspectives on Cyberpower.* Washington: Center for Technology and National Security Policy at the National Defense University, 2009. p. 1-27.

BOWER, Joseph L; CHRISTENSEN, Clayton M. Disruptive Technologies: Catching the Wave. *Harvard Business Review*, Boston, Jan./Feb. p. 43-53, 1995.

BRANTLY, Aaron F.; PUYVELDE, Damien Van. *Cybersecurity*: PoliTICS, Governance and Conflict in Cyberspace. Cambridge: Polity Press, 2019.

BRASIL. *Lei nº 12.965, de 23 de abril de 2014*. Estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil. Brasília, 2014a. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm. Acesso em: 16 set. 2022.

BRASIL. Câmara da Reforma do Estado. *Plano Diretor da Reforma do Aparelho do Estado*. 1995. Disponível em: http://www.biblioteca.presidencia.gov.br/publicacoes-oficiais/catalogo/fhc/plano-diretor-da-reforma-do-aparelho-do-estado-1995.pdf. Acesso em: 30 dez. 2022.

BRASIL. Congresso Nacional. *Mensagem (CN) n° 9, de 2020*. Encaminha, para apreciação, os textos da proposta da Política Nacional de Defesa, da Estratégia Nacional de Defesa e o Livro Branco de Defesa Nacional. Brasília, 2020e. Disponível em: https://legis.senado.leg.br/diarios/ver/104470?sequencia=8. Acesso em: 12 jan. 2021.

BRASIL. Conselho Nacional de Justiça. *Resolução nº 396, de 7 de junho de 2021*. Institui a Estratégia Nacional de Segurança Cibernética do Poder Judiciário (ENSEC-PJ). Brasília, 2021a. Disponível em: https://atos.cnj.jus.br/atos/detalhar/3975. Acesso em: 26 ago. 2022.

BRASIL. *Constituição da República Federativa do Brasil de 1988*. 1988. Disponível em: http://www.planalto.gov.br/ccivil_03/constituicao/constituicao.htm. Acesso em: 12 jan. 2021.

BRASIL. *Decreto Legislativo nº 179, de 14 de dezembro de 2018*. Aprova a Política Nacional de Defesa, a Estratégia Nacional de Defesa e o Livro Branco de Defesa Nacional, encaminhados ao Congresso Nacional pela Mensagem (CN) nº 2 de 2017 (Mensagem nº 616, de 18 de novembro de 2016, na origem). Brasília, 2018e. Disponível em: https://www2.camara.leg.br/legin/fed/decleg/2018/decretolegislativo-179-14-dezembro-2018-787452-anexo-pl.pdf. Acesso em: 12 fev. 2021.

BRASIL. *Decreto Legislativo nº 373, de 25 de setembro de 2013*. Aprova a Política Nacional de Defesa, a Estratégia Nacional de Defesa e o Livro Branco de Defesa Nacional, encaminhados ao Congresso Nacional pela Mensagem nº 83, de 2012 (Mensagem nº 323, de 17 de julho de 2012, na origem). Brasília, 2013a. Disponível em: https://www2.camara.leg.br/legin/fed/decleg/2013/decretolegislativo-373-25-setembro-2013-777085-publicacaooriginal-141221-pl.html. Acesso em: 04 nov. 2022.

BRASIL. *Decreto n° 10.748, de 16 de julho de 2021*. Institui a Rede Federal de Gestão de Incidentes Cibernéticos. Brasília, 2021b. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2019-2022/2021/decreto/D10748.htm. Acesso em: 26 ago. 2022.

BRASIL. *Decreto n° 11.200, de 15 de setembro de 2022*. Aprova o Plano Nacional de Segurança de Infraestruturas Críticas. Brasília, 2022a. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2019-2022/2022/decreto/D11200.htm. Acesso em: 20 out. 2022.

BRASIL. *Decreto nº 10.222, de 5 de fevereiro de 2020*. Aprova a Estratégia Nacional de Segurança Cibernética. Brasília, 2020a. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2019-2022/2020/decreto/ D10222.htm. Acesso em: 15 fev. 2020.

BRASIL. *Decreto nº 10.227, de 5 de fevereiro de 2020*. Promulga os textos dos Instrumentos de Emenda à Constituição e à Convenção da União Internacional de Telecomunicações, contidos nos Atos Finais das Conferências de Plenipotenciários de Antalya e Guadalajara. Brasília, 2020b. Disponível em: https://www.planalto.gov.br/ccivil_03/_Ato2019-2022/2020/Decreto/D10227.htm. Acesso em: 07 ago. 2022.

BRASIL. *Decreto nº 10.363, de 21 de maio de 2020*. Altera o Decreto nº 9.668, de 2 de janeiro de 2019, que aprova a Estrutura Regimental e o Quadro Demonstrativo dos Cargos em Comissão e das Funções de Confiança do Gabinete de Segurança Institucional da Presidência da República, e remaneja e transforma cargos em comissão. Brasília, 2020c. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2019-2022/2020/decreto/D10363.htm. Acesso em: 17 nov. 2022.

BRASIL. *Decreto nº 10.569, de 9 de dezembro de 2020*. Aprova a Estratégia Nacional de Segurança de Infraestruturas Críticas. Brasília, 2020f. Disponível em:

http://www.planalto.gov.br/ccivil_03/_ato2019-2022/2020/decreto/D10569.htm. Acesso em: 10 dez. 2020.

BRASIL. *Decreto nº 3.505, de 13 de junho de 2000*. Institui a Política de Segurança da Informação nos órgãos e entidades da Administração Pública Federal. Brasília, 2000a. Disponível em: http://www.planalto.gov.br/ccivil_03/decreto/d3505.htm. Acesso em: 01 nov. 2022.

BRASIL. *Decreto nº 4.801, de 6 de agosto de 2003*. Cria a Câmara de Relações Exteriores e Defesa Nacional, do Conselho de Governo. Brasília, 2003b. Disponível em: http://www.planalto.gov.br/ccivil_03/decreto/2003/d4801.htm. Acesso em: 01 nov. 2022.

BRASIL. *Decreto nº 4.829, de 3 de setembro de 2003*. Dispõe sobre a criação do Comitê Gestor da Internet no Brasil – CGI.br, sobre o modelo de governança da Internet no Brasil, e dá outras providências. Brasília, 2003c. Disponível em: http://www.planalto.gov.br/ccivil_03/decreto/2003/d4829.htm. Acesso em: 08 jan. 2023

BRASIL. *Decreto nº 5.772, de 8 de maio de 2006*. Aprova a Estrutura Regimental e o Quadro Demonstrativo dos Cargos em Comissão e das Gratificações de Exercício em Cargo de Confiança do Gabinete de Segurança Institucional da Presidência da República, e dá outras providências. Brasília, 2006. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2004-2006/2006/decreto/d5772.htm. Acesso em: 01 nov. 2022.

BRASIL. *Decreto nº 6.703, de 18 de dezembro de 2008*. Aprova a Estratégia Nacional de Defesa, e dá outras providências. Brasília, 2008b. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2007-2010/2008/decreto/d6703.htm. Acesso em: 02 nov. 2022.

BRASIL. *Decreto nº 8.135, de 4 de novembro de 2013*. Dispõe sobre as comunicações de dados da administração pública federal direta, autárquica e fundacional, e sobre a dispensa de licitação nas contratações que possam comprometer a segurança nacional. Brasília, 2013b. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2013/decreto/d8135.htm. Acesso em: 05 nov. 2022.

BRASIL. *Decreto nº 8.771, de 11 de maio de 2016*. Regulamenta a Lei nº 12.965, de 23 de abril de 2014, para tratar das hipóteses admitidas de discriminação de pacotes de dados na internet e de degradação de tráfego, indicar procedimentos para guarda e proteção de dados por provedores de conexão e de aplicações, apontar medidas de transparência na requisição de dados cadastrais pela administração pública e estabelecer parâmetros para fiscalização e apuração de infrações. Brasília, 2016a. Disponível em: http://www.planalto.gov.br/ccivil_03/_Ato2015-2018/2016/Decreto/D8771.htm. Acesso em: 16 set. 2022.

BRASIL. *Decreto nº 9.319, de 21 de março de 2018*. Institui o Sistema Nacional para a Transformação Digital e estabelece a estrutura de governança para a implantação da Estratégia Brasileira para a Transformação Digital. Brasília, 2018. Brasília, 2018a. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato 2015-2018/2018/decreto/D9319.htm. Acesso em: 26 out. 2020.

BRASIL. *Decreto nº 9.573, de 22 de novembro de 2018*. Aprova a Política Nacional de Segurança de Infraestruturas Críticas. Brasília, 2018d. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/decreto/D9573.htm. Acesso em: 18 out. 2020.

BRASIL. *Decreto nº 9.637, de 26 de dezembro de 2018*. Institui a Política Nacional de Segurança da Informação. Brasília, 2018f. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/decreto/D9637 .htm. Acesso em: 05 jan. 2019.

BRASIL. *Decreto nº 9.668, de 2 de janeiro de 2019*. Aprova a Estrutura Regimental e o Quadro Demonstrativo dos Cargos em Comissão e das Funções de Confiança do Gabinete de Segurança Institucional da Presidência da República e altera o quantitativo de Gratificações de Exercício de Cargo em Confiança devida a Militares – RMP. Brasília, 2019a. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2019-2022/2019/decreto/d9668.htm. Acesso em: 18 set. 2022.

BRASIL. *Decreto n° 11.331, de 1° de janeiro de 2023*. Aprova a Estrutura Regimental e o Quadro Demonstrativo dos Cargos em Comissão, das Funções de Confiança e das Gratificações do Gabinete de Segurança Institucional da Presidência da República e remaneja cargos em comissão, funções de confiança e gratificações. Brasília, 2023b. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2023-2026/2023/decreto/D11331.htm. Acesso em: 04 fev. 2023.

BRASIL. *Decreto-Lei nº 200, de 25 de fevereiro de 1967*. Dispõe sobre a organização da Administração Federal, estabelece diretrizes para a Reforma Administrativa e dá outras providências. Brasília, 1967. Disponível em: http://www.planalto.gov.br/ccivil_03/decreto-lei/del0200.htm#view. Acesso em: 21 set. 2022.

BRASIL. Gabinete de Segurança Institucional. *Instrução Normativa nº 1, de 27 de maio de 2020*. Dispõe sobre a Estrutura de Gestão da Segurança da Informação nos órgãos e nas entidades da administração pública federal. Brasília, 2020d. Disponível em: https://www.in.gov.br/en/web/dou/-/instrucao-normativa-n-1-de-27-de-maio-de-2020-258915215. Acesso em: 02 nov. 2022.

BRASIL. Gabinete de Segurança Institucional. *Portaria nº 91, de 26 de julho de 2017*. Aprova o Regimento Interno do Gabinete de Segurança Institucional da Presidência da República. Brasília, 2017. Disponível em: https://pesquisa.in.ºgov.br/imprensa/jsp/visualiza/index.jsp?data=27/07/2017&jornal=1&pagina=5&totalArquivos=144. Acesso em: 17 nov. 2022.

BRASIL. *Lei Complementar nº 97, de 9 de junho de 1999*. Dispõe sobre as normas gerais para a organização, o preparo e o emprego das Forças Armadas. Brasília, 1999. Disponível em: http://www.planalto.gov.br/ccivil_03/leis/lcp/lcp97.htm. Acesso em: 06 jan. 2021.

BRASIL. *Lei nº 10.683, de 28 de maio de 2003*. Dispõe sobre a dispõe sobre a organização da Presidência da República e dos Ministérios, e dá outras providências.

Brasília, 2003a. Disponível em: http://www.planalto.gov.br/ccivil_03/leis/2003/l10.683.htm. Acesso em: 01 nov. 2022.

BRASIL. *Lei nº 12.735, de 30 de novembro de 2012*. Altera o Decreto-Lei nº 2.848, de 7 de dezembro de 1940 - Código Penal, o Decreto-Lei nº 1.001, de 21 de outubro de 1969 - Código Penal Militar, e a Lei nº 7.716, de 5 de janeiro de 1989, para tipificar condutas realizadas mediante uso de sistema eletrônico, digital ou similares, que sejam praticadas contra sistemas informatizados e similares; e dá outras providências. Brasília, 2012a. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2012/lei/l12735.htm. Acesso em: 04 nov. 2022.

BRASIL. *Lei nº 12.737, de 30 de novembro de 2012*. Dispõe sobre a tipificação criminal de delitos informáticos; altera o Decreto-Lei nº 2.848, de 7 de dezembro de 1940 - Código Penal; e dá outras providências. Brasília, 2012b. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2012/lei/l12737.htm. Acesso em: 04/11/2022.

BRASIL. *Lei nº 13.266, de 5 de abril de 2016*, que extingue e transforma cargos públicos; altera a Lei nº 10.683, de 28 de maio de 2003, que dispõe sobre a organização da Presidência da República e dos Ministérios, e a Lei nº 11.457, de 16 de março de 2007; e revoga dispositivos da Lei nº 10.683, de 28 de maio de 2003. Brasília, 2016b. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2016/Lei/L13266.htm. Acesso em: 16 nov. 2022.

BRASIL. *Lei nº 13.341, de 29 de setembro de 2016*. Altera as Leis nº 10.683, de 28 de maio de 2003, que dispõe sobre a organização da Presidência da República e dos Ministérios, e 11.890, de 24 de dezembro de 2008, e revoga a Medida Provisória nº 717, de 16 de março de 2016. Brasília, 2016c. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2016/lei/l13341.htm. Acesso em: 16 nov. 2022.

BRASIL. *Lei nº 13.709, de 14 de agosto de 2018*. Lei Geral de Proteção de Dados (LGPD). Brasília, 2018c. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm. Acesso em: 18 set. 2022.

BRASIL. *Lei nº 13.844, de 18 de junho de 2019*. Lei que estabelece a organização básica dos órgãos da Presidência da República e dos Ministérios. Brasília, 2019b. Disponível em: https://www.planalto.gov.br/ccivil_03/_Ato2019-2022/2019/Lei/L13844.htm. Acesso em: 06 ago. 2022.

BRASIL. *Lei nº 13.853, de 8 de julho de 2019*. Altera a Lei nº 13.709, de 14 de agosto de 2018, para dispor sobre a proteção de dados pessoais e para criar a Autoridade Nacional de Proteção de Dados; e dá outras providências. Brasília, 2019c. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2019-2022/2019/lei/l13853.htm. Acesso em: 31 dez. 2022.

BRASIL. *Lei nº 14.460, de 25 de outubro de 2022*. Transforma a Autoridade Nacional de Proteção de Dados (ANPD) em autarquia de natureza especial e transforma cargos comissionados; altera as Leis nº 13.709, de 14 de agosto de 2018 (Lei Geral de Proteção de Dados Pessoais), e 13.844, de 18 de junho de 2019; e revoga dispositivos da Lei nº

13.853, de 8 de julho de 2019. Brasília, 2022b. Disponível em: https://www.planalto.gov.br/ccivil_03/_Ato2019-2022/2022/Lei/L14460.htm#art7. Acesso em: 31 dez. 2022.

BRASIL. *Lei nº 9.472, de 16 de julho de 1997*. Dispõe sobre a dispõe sobre a organização dos serviços de telecomunicações, a criação e funcionamento de um órgão regulador e outros aspectos institucionais, nos termos da Emenda Constitucional nº 8, de 1995. Brasília, 1997. Disponível em: http://www.planalto.gov.br/ccivil_03/leis/l9472.htm. Acesso em: 02 set. 2022.

BRASIL. *Medida provisória nº 1.154, de 1º de janeiro de 2023*. Estabelece a organização básica dos órgãos da Presidência da República e dos Ministérios. Brasília, 2023a. Ed. Especial. Disponível em: http://www.planalto.gov.br/ccivil_03/_Ato2023-2026/2023/Mpv/mpv1154.htm. Acesso em: 05 fev. 2023.

BRASIL. Ministério da Ciência e Tecnologia. *Sociedade da Informação no Brasil:* livro verde. Brasília, 2000b. 231 p.

BRASIL. Ministério da Ciência, Tecnologia e Inovações. *Estratégia Brasileira para a Transformação Digital (E-Digital)*. Ciclo 2022-2026. Aprovada pela Portaria MCTI nº 6.543, de 16 de novembro de 2022. Brasília, 2022c. Disponível em: https://www.gov.br/mcti/pt-br/acompanhe-o-mcti/transformacaodigital/arquivosestrategiadigital/e-digital_ciclo_2022-2026.pd. Acesso em: 18 nov. 2022.

BRASIL. Ministério da Ciência, Tecnologia, Inovações e Comunicações. *Estratégia Brasileira para a Transformação Digital (E-Digital)*, aprovada pela Portaria MCTIC nº 1.556, de 21 de março de 2018. Brasília, 2018b. Disponível: https://antigo.mctic.gov.br/mctic/export/sites/institucional/arquivos/estrategiadigital.pdf. Acesso em: 13 jan. 2021.

BRASIL. Ministério da Defesa. *Glossário das Forças Armadas*. 5. ed. Brasília, 2015b. Disponível em: https://bdex.eb.mil.br/jspui/bitstream/123456789/141/1/MD35_G01.pdf. Acesso em: 13 jan. 2021.

BRASIL. Ministério da Defesa. *Portaria Normativa nº 2.777, de 27 de outubro de 2014*. Dispõe sobre a diretriz de implantação de medidas visando à potencialização da Defesa Cibernética Nacional e dá outras providências. Brasília, 2014d. Disponível em: https://pesquisa.in.gov.br/imprensa/jsp/visualiza/index.jsp?data=28/10/2014&jornal=1&pagina=7&totalArquivos=56. Acesso em: 06 nov. 2022.

BRASIL. Ministério da Defesa. *Portaria Normativa nº 3.010, de 18 de novembro de 2014*. Aprova a Doutrina Militar de Defesa Cibernética. Brasília, 2014e. Disponível em: https://www.gov.br/defesa/pt-br/arquivos/legislacao/emcfa/publicacoes/doutrina/md31a_ma_08a_defesaa_ciberneticaa_1a_2014.pdf. Acesso em: 06 nov. 2022.

BRASIL. Ministério da Defesa. *Portaria Normativa nº 3.389, de 21 de dezembro de 2012*. Dispõe sobre a Política Cibernética de Defesa. Brasília, 2012. Disponível em: https://www.gov.br/defesa/pt-

br/arquivos/doutrina_militar/MD31P02PoliticaCiberneticadeDefesa1Ed2012.pdf. Acesso em: 04 nov. 2022.

BRASIL. *Portaria Interministerial MP/MC/MD nº 141, de 2 de maio de 2014*. Dispõe que as comunicações de dados da Administração Pública Federal direta, autárquica e fundacional deverão ser realizadas por redes de telecomunicações e serviços de tecnologia da informação fornecidos por órgãos ou entidades da Administração Pública Federal, incluindo empresas públicas e sociedades de economia mista da União e suas subsidiárias, observado o disposto nesta Portaria. Brasília, 2014c. Disponível em: https://www.legisweb.com.br/legislacao/?id=269793. Acesso em: 06 nov. 2022.

BRASIL. Presidência da República. Gabinete de Segurança Institucional. *Instrução Normativa nº 1, de 13 de junho de 2008*. Disciplina a Gestão de Segurança da Informação e Comunicações na Administração Pública Federal, direta e indireta, e dá outras providências. Brasília, 2008a. Disponível em: https://pesquisa.in.gov.br/imprensa/jsp/visualiza/index.jsp?data=18/06/2008&jornal=1&pagina=6&totalArquivos=120. Acesso em: 02 nov. 2022.

BRASIL. Presidência da República. Gabinete de Segurança Institucional. *Portaria nº 45, de 8 de setembro de 2009*. Institui, no âmbito da Câmara de Relações Exteriores e Defesa Nacional (CREDEN), o Grupo Técnico de Segurança Cibernética e dá outras providências. Brasília, 2009. Disponível em: https://pesquisa.in.gov.br/imprensa/jsp/visualiza/index.jsp?data=09/09/2009&jornal=1&pagina=2&totalArquivos=80. Acesso em: 02 nov. 2022.

BRASIL. Presidência da República. Gabinete de Segurança Institucional. Departamento de Segurança da Informação e Comunicações. *Livro Verde*: segurança cibernética no Brasil. Brasília, 2010. Disponível em: http://dsic.planalto.gov.br/legislacao/1_Livro_Verde_SEG_CIBER.pdf/view. Acesso em: 07/10/2020.

BRASIL. Presidência da República. Gabinete de Segurança Institucional. *Estratégia de segurança da informação e comunicações e de segurança cibernética da administração pública federal 2015-2018*: versão 1.0. Homologada pela Portaria do Conselho de Defesa Nacional n.° 14, de 11 de maio de 2015. Brasília, 2015a. Disponível em: https://www.gov.br/gsi/pt-br/arquivos/4_estrategia_de_sic.pdf. Acesso em: 30 out. 2022.

BRASIL. Presidência da República. Gabinete de Segurança Institucional. Departamento de Segurança da Informação. *Glossário de Segurança da Informação*. Brasília, 2019d. Disponível em: http://dsic.planalto.gov.br/arquivos/documentos-pdf/glossario_completo.pdf. Acesso em: 30 set. 2020.

BRASIL. Senado Federal. *CPI da Espionagem*. Relatório Final. Brasília, 2014b. Disponível em: https://www12.senado.leg.br/noticias/arquivos/2014/04/04/integra-do-relatorio-de-ferraco. Acesso em: 06 nov. 2022.

BRESSER-PEREIRA, Luiz Carlos. *Crise Econômica e Reforma do Estado no Brasil*. São Paulo: Editora 34, 1996.

BRESSER-PEREIRA, Luiz Carlos. Uma reforma gerencial da administração pública no Brasil. *Revista do Serviço Público*, Brasília, v. 49, n. 1, p. 5-42, 1998. Disponível em: https://bresserpereira.org.br/papers/1997/97.Reforma_gerencial-RSP.pdf. Acesso em: 30 dez. 2022.

BRESSER-PEREIRA, Luiz Carlos; GRAU, Nuria Cunill. Entre o Estado e o mercado: o público não-estatal. *In*: Bresser-Pereira, Luiz Carlos; GRAU, Nuria Cunill (org.). *O Público Não-Estatal na Reforma do Estado*. Rio de Janeiro: Editora FGV, 1999. p 15-48. Disponível em: https://bresserpereira.org.br/papers/1998/84PublicoNaoEstataRefEst.p.pg.pdf. Acesso em: 30 dez. 2022.

BRESSER-PEREIRA, Luiz Carlos. Instituições, bom Estado, e reforma da gestão pública. *In*: BIDERMAN, Ciro; ARVATE, Paulo (org.). *Economia do Setor Público no Brasil*. São Paulo: Campus Elsevier, 2004. p. 3-15. Disponível em: https://bresserpereira.org.br/papers/2004/556-Insts-BomEstado-Reforma95-98.pdf. Acesso em: 30 dez. 2022.

BRESSER-PEREIRA, Luiz Carlos. O modelo estrutural de gerência pública. *Revista de Administração Pública*, Rio de Janeiro, v. 42, n. 2, p. 391-410, 2008. Disponível em: https://bresserpereira.org.br/papers/2007/07.06.ModeloEstruturaldeGer%C3%AAnciaP%C3%BAblica.RAP.25fev.2008.pdf. Acesso em: 30 dez. 2022.

BRUSTOLIN, Vitelio. Comparative Analysis of Regulations for Cybersecurity and Cyber Defense in the United States and Brazil. *Revista Brasileira de Estudos de Defesa*, Brasil, v. 6, n. 2, p. 93–123, jul./dez. 2019. Disponível em: https://rbed.abedef.org/rbed/article/view/75149. Acesso em: 14 jan. 2023.

CANABARRO, Diego Rafael; BORNE, Thiago Ferreira. The Brazilian reactions to the Snowden Affairs: implications for the study of International Relations in an interconnected world. *Conjuntura Austral*, Porto Alegre, v. 6, p. 50-74, 2015. Disponível em: https://seer.ufrgs.br/index.php/ConjunturaAustral/article/view/54617/34317. Acesso: 26 ago. 2022.

CENTER FOR STRATEGIC AND INTERNATIONAL STUDIES - CSIS. *Net Losses: Estimating the Global Cost of Cybercrime. Economic Impact of Cybercrime II*. 2014. Disponível em: https://csis-website-prod.s3.amazonaws.com/s3fs-public/legacy_files/files/attachments/140609_rp_economic_impact_cybercrime_report.pdf. Acesso em: 20 jul. 2017.

CEPIK, Marco; CANABARRO, Diego Rafael; FERREIRA, Thiago Borne. Cyberwar: Clausewitzian Encounters. *Space & Defense*, Lincoln, v. 8, p. 19-33, 2015. Disponível em: https://professor.ufrgs.br/marcocepik/files/cepik__canabarro__borne_-_2015_-_cyberwar.pdf. Acesso em: 28 jun. 2022.

CLARKE, Richard Alan; KNAKE, Robert K. *Cyber war: the next threat to National Security and what to do about it.* Old Saybrook: Tantor Media, 2014.

COMITÊ GESTOR DA INTERNET NO BRASIL - CGI.br. Pesquisa sobre o Uso das Tecnologias da Informação e da Comunicação no Brasil – TIC DOMICÍLIOS e TIC EMPRESAS. São Paulo, 2005. Disponível em: https://cetic.br/media/docs/publicacoes/2/tic-2005.pdf. Acesso em: 01 nov. 2022.

COMITÊ GESTOR DA INTERNET NO BRASIL - CGI.br. Documentos da Cúpula Mundial sobre a Sociedade da Informação. *Cadernos CGI.br Referências*, São Paulo, v. 1, 2014. Disponível em: https://www.cgi.br/media/docs/publicacoes/1/CadernosCGIbr_DocumentosCMSI.pdf. Acesso em 07 out. 2020.

CRAVO, Vanessa Copetti. A Autonomia e Independência da Anatel no Contexto Juspolítico Brasileiro. *Cadernos do Programa de Pós-Graduação em Direito – PPGDir/UFRGS*, v. 6, n. 7/8, p. 151-193, 2007. Porto Alegre: PPGDir/UFRGS, 2007.

CRAVO, Vanessa Copetti. *Crimes Cibernéticos e as Principais Iniciativas Regionais e Internacionais*. 2011. Dissertação (Mestrado em Direito) – Faculdade de Direito, Universidade Federal do Rio Grande do Sul, Porto Alegre, 2011. Disponível em: https://lume.ufrgs.br/bitstream/handle/10183/238688/000827488.pdf?sequence=1. Acesso em: 07 ago. 2022.

DINIZ, Gustavo; MUGGAH, Robert Muggah; GLENNY, Misha Glenny. Deconstructing Cyber Security in Brazil: Threats and Responses. Igarapé Institute, *Strategic Paper*, Rio de Janeiro, n. 11, Dec. 2014. Disponível em: https://igarape.org.br/wp-content/uploads/2014/11/Strategic-Paper-11-Cyber2.pdf. Acesso em: 27 dez. 2022.

DREYER, Paul *et al. Estimating the Global Cost of Cyber Risk:* Methodology and Examples. RAND Corporation, 2018. Disponível em: https://www.rand.org/pubs/research_ reports/RR2299 .html. Acesso em: 01 out. 2020.

DUARTE, Érico Esteves. Impactos de Novas Tecnologias em Política de Defesa: Lições e Limites do Modelo Norte-Americano. *Boletim de Economia e Política Internacional*, Brasília, v. 1, p. 71-82, 2011. Disponível em: https://repositorio.ipea.gov.br/bitstream/11058/4032/1/BEPI_n08_ impacto.pdf. Acesso em: 18 nov. 2022.

DUARTE, Érico Esteves. A Conduta da Guerra na Era Digital e Implicações para o Brasil: Uma Análise de Conceitos, Políticas e Práticas de Defesa. Texto para Discussão (IPEA), Brasília, v. 1760, p. 1-93, 2012. Disponível em: https://repositorio.ipea.gov.br/bitstream/11058/1088/1/TD_1760.pdf. Acesso em 30 jul. 2022.

EUROPEAN UNION AGENCY FOR NETWORK AND INFORMATION SECURITY - ENISA. *Definition of Cybersecurity: Gaps and overlaps in standardization.* v. 1.0 Dec. 2015. Disponível em: https://www.enisa.europa.eu/publications/definition-of-cybersecurity. Acesso em: 26 out. 2022.

EUROPEAN UNION AGENCY FOR NETWORK AND INFORMATION SECURITY - ENISA. *ENISA Overview of cybersecurity and related terminology*. 2017. Disponível

em: https://www.enisa.europa.eu/publications/enisa-position-papers-and-opinions/enisa-overview-of-cybersecurity-and-related-terminology. Acesso em: 26 out. 2022.

EUROPEAN UNION AGENCY FOR NETWORK AND INFORMATION SECURITY - ENISA. Incident Response. *Glossary*. [201?]. Disponível em: https://www.enisa.europa.eu/topics/incident-response/glossary/phishing-spear-phishing?v2=1. Acesso em: 09 jan. 2022.

FURTADO, CELSO. *A Pré-Revolução Brasileira*. Rio de Janeiro: Fundo de Cultura, 1962.

GERRING, John. Mere Description. *British Journal of Political Science*, Cambridge, v. 42, n. 4, p. 721-746, May 2012.

GIORDANO, Vitória Rangel; BOSSO, João Paulo Cavazzani. A Estruturação da Defesa e da Segurança Cibernética a partir do Mapeamento Documental dos Estados Unidos da América. *In*: AYRES PINTO, Danielle Jacon; PAGLIARI, Graciela de Conti; GRASSI, Jéssica Maria (org.). *A Geopolítica das Estratégias em Defesa Cibernética: como EUA, China, Rússia e Israel protegem seu ciberespaço*. Rio de Janeiro: Editora Alpheratz, 2021. p. 15-46.

HUREL, Louise Marie. Cibersegurança no Brasil: uma análise da estratégia nacional. *Instituto Igarapé, Artigo Estratégico*, Rio de Janeiro, n. 54, p. 1-44, abr. 2021. Disponível em: https://igarape.org.br/wp-content/uploads/2021/04/AE-54_Seguranca-cibernetica-no-Brasil.pdf. Acesso em: 29 set. 2022.

HUREL, Louise Marie. Interrogating the Cybersecurity Development Agenda: A Critical Reflection. *The International Spectator*, Rome, v. 52, n. 3, p. 66-84, 2022. Disponível em: https://www.tandfonline.com/doi/full/10.1080/03932729.2022.2095824. Acesso em 29 ago. 2022.

HUREL, Louise Marie; LOBATO, Luisa Cruz. *Uma Estratégia para a Governança da Segurança Cibernética no Brasil*. *Instituto Igarapé, Nota Estratégico,* n. 30, set. 2018. Disponível em: https://igarape.org.br/wp-content/uploads/2018/09/Uma-estrate%CC%81gia-para-a-governanc%CC%A7a-da-seguranc%CC%A7a-ciberne%CC%81tica-no-Brasil.pdf. Acesso em: 29 ago. 2022.

INTERNATIONAL TELECOMMUNICATION UNION - ITU. *Final Acts of the Plenipotentiary Conference (Minneapolis, 1998). Genebra,* 1999. Disponível em: https://search.itu.int/history/HistoryDigitalCollectionDocLibrary/4.16.43.en.100.pdf. Acesso em: 07 ago. 2022.

INTERNATIONAL TELECOMMUNICATION UNION - ITU. *ITU Building the Information Society.* Genebra: ITU, 2007. Disponível em: https://www.itu.int/dms_pub/itu-s/opb/gen/s-gen-bis-2007-pdf-e.pdf. Acesso em: 07 ago. 2022.

INTERNATIONAL TELECOMMUNICATION UNION - ITU. Global Cybersecurity Agenda. *Report of the Chairman of the High-Level Experts Group (HLEG)*. Genebra,

2008. Disponível em: https://www.itu.int/en/action/cybersecurity/Documents/gca-chairman-report.pdf. Acesso em: 15 abr. 2020.

INTERNATIONAL TELECOMMUNICATION UNION - ITU. Telecommunication Standardization Sector of ITU. *Recommendation ITU-T X.1205. Overview of cybersecurity*. Genebra, 2009a. Disponível em: https://www.itu.int/rec/t-rec-x.1205-200804-i. Acesso em: 26 out. 2022.

INTERNATIONAL TELECOMMUNICATION UNION - ITU. *Cybersecurity for all. Global Cybersecurity Agenda. A Framework for International Cooperation.* Genebra: ITU, 2009b.

INTERNATIONAL TELECOMMUNICATION UNION - ITU. *Global Cybersecurity Index and Cyberwellness Profiles*. Genebra, 2015. Disponível em: https://www.itu.int/pub/D-STR-SECU-2015. Acesso em: 09 out. 2020.

INTERNATIONAL TELECOMMUNICATION UNION - ITU. *Global Cybersecurity Index (GCI).* Genebra, 2017. Disponível em: https://www.itu.int/dms_pub/itu-d/opb/str/D-STR-GCI.01-2017-R1-PDF-E.pdf. Acesso em: 08 set. 2022.

INTERNATIONAL TELECOMMUNICATION UNION – ITU. *Guide to developing a national cybersecurity strategy - Strategic engagement in cybersecurity.* Genebra, 2018a. Disponível em: https://www.itu.int/pub/d-str-cyb_guide.01-2018. Acesso em: 01 mar. 2019.

INTERNATIONAL TELECOMMUNICATION UNION - ITU. *Global Cybersecurity Index 2018*. Genebra, 2019a. Disponível em: https://www.itu.int/ dms_pub/itu-d/opb/str/d-str-gci.01-2018-pdf-e.pdf. Acesso em: 12 fev. 2020.

INTERNATIONAL TELECOMMUNICATION UNION - ITU. *Collection of the basic texts of the International Telecommunication Union adopted by the Plenipotentiary Conference*. *Edition* 2019. Genebra, 2019b. Disponível em: http://handle.itu.int/11.1004/020.1000/5.22.61.en.100. Acesso em: 07 ago 2022.

INTERNATIONAL TELECOMMUNICATION UNION - ITU. *Global Cybersecurity Index 2020 – Frequently Asked Questions*. Genebra, 2021a. Disponível em: https://www.itu.int/en/ITU-D/Cybersecurity/Documents/GCIv4/GCI-FAQ.pdf. Acesso em: 09 ago. 2022.

INTERNATIONAL TELECOMMUNICATION UNION - ITU. *Global Cybersecurity Index 2020*. Genebra, 2021b. Disponível em: https://www.itu.int/dms_pub/itu-d/opb/str/D-STR-GCI.01-2021-PDF-E.pdf. Acesso em: 2 maio 2022.

INTERNATIONAL TELECOMMUNICATION UNION (ITU) *et al*. *Guide to Developing a National Cybersecurity Strategy 2nd* Edition – Strategic Engagement in Cybersecurity. Genebra, 2021. Disponível em: https://ncsguide.org/wp-content/uploads/2021/11/2021-NCS-Guide.pdf. Acesso em: 21 maio 2022.

INTERNATIONAL TELECOMMUNICATION UNION - ITU. *World Telecommunication Development Conference 2022 (WTDC-22). Provisional Final Report*. Genebra, 2022a. Disponível em: https://www.itu.int/dms_pub/itu-d/md/18/wtdc21/c/D18-WTDC21-C-0103!R1!PDF-E.pdf. Acesso em: 11 ago. 2022.

INTERNATIONAL TELECOMMUNICATION UNION - ITU. *Final Act of the Plenipotentiary Conference (Bucharest, 2022)*. Genebra, 2022b. Disponível em: https://www.itu.int/dms_pub/itu-s/opb/conf/S-CONF-ACTF-2022-PDF-E.pdf . Acesso em: 06 jan. 2022.

KUERBIS, Brenden; BADIEI, Farzaneth. Mapping the cybersecurity institutional landscape. *Digital Policy, Regulation and Governance*, Bingley, v. 19.6, p. 466-492, 2017. Disponível em: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3891296. Acesso em: 15 set. 2021.

KURBALIJA, Jovan. *An Introduction to Internet Governance*. 7th ed. Malta: DiploFoundation, 2016. Disponível em: https://www.diplomacy.edu/resources/books/introduction-internet-governance. Acesso em: 24 out. 2019.

LIBICKI, Martin C. Cyberspace Is Not a Warfighting Domain. I*/S: A Journal of Law and Policy*, Columbus, v. 8, n. 2, p. 325-340, 2012. Disponível em: https://kb.osu.edu/bitstream/handle/1811/73111/1/ISJLP_V8N2_321.pdf. Acesso em: 28 ago. 2022.

LIMA E SILVA, Walbery Nogueira de. Atuação colaborativa da Defesa Cibernética na proteção de infraestruturas críticas de interesse para a Defesa Nacional. *Data & Hertz*, Brasília, n. 1, p. 52-59, 2020. Disponível em: http://www.ebrevistas.eb.mil.br/datahertz/article/view/6796. Acesso em: 10 ago 2022.

LINDSTROM, Gustav; LUIIJF**,** Eric. Political aims and policy methods. *In*: KLIMBURG, Alexander (ed.). *National Cyber Security Framework Manual*. Tallinn: NATO CCD COE, 2012. p. 44-65. Disponível em: https://www.academia.edu/25202109/Political_ Aims_and_Policy_Methods?email_work_card=title. Acesso em: 15 out. 2020.

LOBATO, Luísa Cruz. La política brasileña de ciberseguridad como estrategia de liderazgo regional. *URVIO - Revista Latinoamericana de Estudios de Seguridad*, Quito, n. 20, p. 16-30, jun. 2017. Disponível em: https://revistas.flacsoandes.edu.ec/urvio/issue/view/150. Acesso em: 27 dez. 2022.

LOBATO, Luísa Cruz; KENKEL, Kai Michael. Discourses of Cyberspace Securitization in Brazil and in the United States. *Revista Brasileira de Política Internacional,* Brasília, v. *58*, n. 2, p. 23–43, 2015. Disponível em: https://doi.org/10.1590/0034-7329201500202. Acesso em: 29 dez.2022.

LUCERO, Everton. *Governança de Internet:* aspectos da formação de um regime global e oportunidades para a ação diplomática. Brasília: Fundação Alexandre Gusmão, 2011. Disponível em: http://funag.gov.br/biblioteca/download/822-Governanca_da_Internet.pdf . Acesso em: 20 set. 2017.

LUIIJF, H. A. M. et al. Ten national cyber security strategies: a comparison. *In*: *International Workshop on Critical Information Infrastructures Security*. Springer, Berlin, Heidelberg, 2011.

MALAGUTTI, Marcelo. *Software Power*: um olhar brasileiro. Brasília: Instituto Vegetius, 2022a.

MALAGUTTI. *Ciberdefesa e Cibersegurança*: um olhar brasileiro. Brasília: Instituto Vegetius, 2022b.

MARTINS, José Miguel Quedi. *Digitalização e guerra local*: como fatores do equilíbrio internacional. 2008. Tese (Doutorado em Ciência Política) – Instituto de Filosofia e Ciências Humanas, Universidade Federal do Rio Grande do Sul, Porto Alegre, 2008.

MUELLER, Milton. Is Cybersecurity Eating Internet Governance? Causes and Consequences of Alternative Framings. *Digital Policy, Regulation and Governance*, Bingley, v. 19.6, p. 415-428, 2017.

NATASIU, Cătălin-ionuț. Cyber Security Strategies in the Internet Era. *Scientific Research and Education in the Air Force*, Brasov, p. 619-624, 2016. Disponível em: https://ns.afahc.ro/ro/afases/2016/SOCIO/NASTASIU.pdf. Acesso em: 27 dez. 2022.

ORGANIZATION FOR ECONOMIC CO-OPERATION AND DEVELOPMENT - OECD. *OECD Guidelines for the Security of Information Systems.* Paris, 1992. Disponível em: https://www.oecd.org/digital/ieconomy/oecdguidelinesforthesecurityofinformationsystems1992.htm. Acesso em: 13 ago 2022.

ORGANIZATION FOR ECONOMIC CO-OPERATION AND DEVELOPMENT - OECD. *Recommendation of the Council concerning Guidelines for Cryptography Policy*. Paris, 1997. Disponível em: https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0289. Acesso em: 27 dez. 2022.

ORGANIZATION FOR ECONOMIC CO-OPERATION AND DEVELOPMENT - OECD. *OECD Guidelines for the Security of Information Systems and Networks:* Towards a Culture of Security. Paris, 2002. Disponível em: https://www.oecd.org/sti/ieconomy/15582260.pdf. Acesso em: 13 ago. 2022**.**

ORGANIZATION FOR ECONOMIC CO-OPERATION AND DEVELOPMENT - OECD. *Working Party on Information Security and Privacy*. Paris, 2005. Disponível em: https://www.oecd.org/digital/ieconomy/36871394.pdf. Acesso em: 13 ago. 2022.

ORGANIZATION FOR ECONOMIC CO-OPERATION AND DEVELOPMENT - OECD. *Committee on Information, Communications and Computer Policy (ICCP)*. Paris, 2010. Disponível em: https://www.oecd.org/digital/ieconomy/37328586.pdf. Acesso em: 13 ago. 2022.

ORGANIZATION FOR ECONOMIC CO-OPERATION AND DEVELOPMENT - OECD. Cybersecurity Policy Making at a Turning Point: Analysing a New Generation of National Cybersecurity Strategies for the Internet Economy. *OECD Digital Economy*

Papers, Paris, n. 211, 2012. Disponível em: https://www.oecd-ilibrary.org/docserver/5k8zq92vdgtln.ºpdf?expires=1659430670&id=id&accname=guest&checksum=92E90AC4DD2D4D4DCC4C8E0B69F58A6A. Acesso em: 02 ago. 2022.

ORGANIZATION FOR ECONOMIC CO-OPERATION AND DEVELOPMENT - OECD. *Digital Security Risk Management for Economic and Social Prosperity:* OECD Recommendation and Companion Document. Paris, 2015. Disponível em: https://www.oecd.org/sti/ieconomy/digital-security-risk-management.pdf. Acesso em: 01 set. 2020.

ORGANIZATION FOR ECONOMIC CO-OPERATION AND DEVELOPMENT - OECD. *Going Digital:* Shaping Policies, Improving Lives. Paris: OECD, 2019a. Disponível em: https://doi.org/10.1787/9789264312012-en. Acesso em: 15 maio 2022.

ORGANIZATION FOR ECONOMIC CO-OPERATION AND DEVELOPMENT - OECD. *Recommendation of the Council on Digital Security of Critical Activities.* Paris, 2019b. Disponível em: https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0456. Acesso em: 27 dez. 2022.

ORGANIZATION FOR ECONOMIC CO-OPERATION AND DEVELOPMENT - OECD. *Going Digital in Brazil*. OECD Reviews of Digital Transformation. Paris: OECD, 2020a. Disponível em: http://www.oecd.org/digital/oecd-reviews-of-digital-transformation-going-digital-in-brazil-e9bf7f8a-en.htm. Acesso em: 27 out. 2020.

ORGANIZATION FOR ECONOMIC CO-OPERATION AND DEVELOPMENT - OECD. *Active with Brazil.* Paris: OECD, 2020b. Disponível em: https://issuu.com/oecd.publishing/docs/active_with_brazil_2020__en_web-1a_. Acesso em: 01 ago. 2022.

ORGANIZATION FOR ECONOMIC CO-OPERATION AND DEVELOPMENT - OECD. *The OECD at 60*. Paris, 2020c. Disponível em: https://read.oecd-ilibrary.org/view/?ref=1059_1059103-whi5k2wv7w&title=OECD-at-60. Acesso em: 12 ago. 2022.

ORGANIZATION FOR ECONOMIC CO-OPERATION AND DEVELOPMENT - OECD. *Recommendation of the Council on Digital Security Risk Management*. Paris, 2022a. Disponível em: https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0479. Acesso em: 27 dez. 2022.

ORGANIZATION FOR ECONOMIC CO-OPERATION AND DEVELOPMENT - OECD. *Recommendation of the Council on National Digital Security Strategies.* Paris, 2022b. Disponível em: https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0480. Acesso em: 27 dez. 2022.

ORGANIZATION FOR ECONOMIC CO-OPERATION AND DEVELOPMENT - OECD. *Recommendation of the Council on the Digital Security of Products and Services*. Paris, 2022c. Disponível em: https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0481. Acesso em: 27 dez. 2022.

ORGANIZATION FOR ECONOMIC CO-OPERATION AND DEVELOPMENT - OECD. *Recommendation of the Council on the Treatment of Digital Security Vulnerabilities.* Paris, 2022d. Disponível em: https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0482. Acesso em: 27 dez 2022.

ORGANIZATION FOR ECONOMIC CO-OPERATION AND DEVELOPMENT - OECD. *OECD Policy Framework on Digital Security*. Paris: OECD, 2022e. Disponível em: https://read.oecd-ilibrary.org/science-and-technology/oecd-policy-framework-on-digital-security_a69df866-en#page1. Acesso em: 27 dez. 2022.

OTTIS, Rain. Analysis of the 2007 cyber attacks against Estonia from the information warfare perspective. *In*: EUROPEAN CONFERENCE ON INFORMATION WARFARE, 7., Reading, MA, 2008. *Proceedings* […]. Reading, MA: Academic Publishing, 2008. Disponível em: https://ccdcoe.org/uploads/2018/10/Ottis2008_AnalysisOf2007FromTheInformationWarfarePerspective.pdf. Acesso em 08 jul. 2022.

PEREZ, Carlota; SOETE, Luc. 21 Catching up in technology: entry barriers and windows of opportunity. *In*: DOSI, G et al. eds. *Technical Change and Economic Theory.* Francis Pinter: London, 1988, p. 458-479. Disponível em: https://carlotaperez.org/wp-content/downloads/publications/development-s-g/Perez-Soete%20TCh&EcTh_1988_on%20catching%20up1.pdf. Acesso em: 15 maio 2022.

PEREZ, Carlota. Technological revolutions and techno-economic paradigms. *Cambridge Journal of Economics,* Cambridge, 34.1, p. 185-202, 2010. Disponível em: http://technologygovernance.eu/files/main/2009070708552121.pdf. Acesso em: 15 maio 2022.

RADU, Roxana. Negotiating meanings for security in the cyberspace. *Digital Policy, Regulation and Governance*, Bingley, v. 15.6, p. 32-41, 2013.

RID, Thomas. *Rise of the Machines: a cybernetic history*. London: W. W. Norton, 2016.

SABILLON, Regner; CAVALLER, Victor; CANO, Jeimy. National cyber security strategies: global trends in cyberspace, *International Journal of Computer Science and Software Engineering*, Dubai, v. 5, n. 5, p. 67-81, 2016. Disponível em: http://ijcsse.org/published/volume5/ issue5/p1-V5I5.pdf. Acesso: 05 out. 2020.

SHAFQAT, Narmeen; MASOOD, Ashraf. Comparative analysis of various national cyber security strategies. *International Journal of Computer Science and Information Security*, Pittsburgh, v. 14, n. 1, p. 129-136, 2016.

SCHWAB, Klaus. The Fourth Industrial Revolution: What it Means, How to Respond. *Japan Spotlight*, Tokyo, p. 3-5, Jul./Aug. 2016. Disponível em: https://www.jef.or.jp/journal/pdf/208th_Cover_01.pdf . Acesso em: 15 maio 2022.

SCHWAB, Klaus; DAVIS, Nicholas. *Aplicando a Quarta Revolução Industrial*. São Paulo: Edipro, 2018.

SHACKELFORD, Scott J.; KASTELIC, Andraz. Toward a State-Centric Cyber Peace? Analyzing the Role of National Cybersecurity Strategies in Enhancing Global Cybersecurity. *New York University Journal of Legislation and Public Policy*, New York, v. 18, p. 895-984, 2016. Disponível em: http://dx.doi.org/10.2139/ssrn.2531733. Acesso em: 27 dez. 2022.

THORSTENSEN, Vera; NOGUEIRA, Thiago Rodrigues São Marcos (coord.). *O Brasil a Caminho da OCDE:* explorando novos desafios. São Paulo: VT Assessoria Consultoria e Treinamento, 2020.

TRIBUNAL DE CONTAS DA UNIÃO (Brasil). Lista de Alto Risco da Administração Pública Federal. Brasília, 2022. Disponível em: https://portal.tcu.gov.br/data/files/1E/07/C0/FC/925628102DFE0FF7F18818A8/lista_de_alto_risco_da_administracao_publica.pdf. Acesso em: 23 nov. 2022.

TVARONAVIČIENĖ, Manuela; PLĖTA, Tomas; CASA, Silvia Della; *et al*. Cyber security management of critical energy infrastructure in national cybersecurity strategies: cases of USA, UK, France, Estonia and Lithuania. *Insights into Regional Development*, Vilnius, v. 2 (4), p. 802-813, 2020. Disponível em: https://hal.archives-ouvertes.fr/hal-03298796. Acesso em: 27 dez. 2022.

UNITED NATIONS GENERAL ASSEMBLY - UNGA. Resolution 45/94, *Guidelines for the regulation of computerized personal data files.* New York, Dec. 1990. Disponível: https://documents-dds-y.un.org/doc/RESOLUTION/GEN/NR0/564/84/IMG/NR056484.pdf?OpenElement. Acesso em: 14 jan. 2023.

UNITED NATIONS GENERAL ASSEMBLY - UNGA. Resolution 53/70, *Developments in the Field of Information and Telecommunications in the Context of International Security.* New York, Dec. 1998. Disponível em: https://undocs.org/en/A/RES/53/70. Acesso em: 11 nov. 2019.

UNITED NATIONS GENERAL ASSEMBLY - UNGA. Resolution 54/49, *Developments in the Field of Information and Telecommunications in the Context of International Security.* New York, Dec. 1999. Disponível em: https://undocs.org/en/A/RES/54/49. Acesso em: 14 jan. 2023.

UNITED NATIONS GENERAL ASSEMBLY - UNGA. Resolution 55/28, *Developments in the Field of Information and Telecommunications in the Context of International Security.* New York, Dec. 2000. Disponível em: https://undocs.org/en/A/RES/55/28. Acesso em: 14 jan. 2023.

UNITED NATIONS GENERAL ASSEMBLY - UNGA. Resolution 55/63, *Combating the criminal misuse of information technologies.* New York, Jan. 2001a. Disponível: https://undocs.org/en/A/RES/55/63. Acesso em: 14 jan. 2023.

UNITED NATIONS GENERAL ASSEMBLY - UNGA. Resolution 56/19, Developments in the Field of Information and Telecommunications in the Context of International Security. New York, Nov. 2001b. Disponível em: https://undocs.org/en/A/RES /56/19. Acesso em: 11 nov. 2019.

UNITED NATIONS GENERAL ASSEMBLY - UNGA. Resolution 56/121, *Combating the criminal misuse of information technologies*. New York, Jan. 2002a. Disponível: https://undocs.org/en/A/RES/56/121. Acesso em: 14 jan. 2023.

UNITED NATIONS GENERAL ASSEMBLY - UNGA. Resolution 56/183, *World Summit on the Information Society*. New York, Jan. 2002b. Disponível em: https://undocs.org/en/A/RES/56/183. Acesso em: 07 ago. 2022.

UNITED NATIONS GENERAL ASSEMBLY - UNGA. Resolution 57/53, *Developments in the Field of Information and Telecommunications in the Context of International Security*. New York, Dec. 2002c. Disponível em: https://undocs.org/en/A/RES/57/53. Acesso em: 14 jan. 2023.

UNITED NATIONS GENERAL ASSEMBLY - UNGA. Resolution 57/239, *Creation of a global culture of cybersecurity*. New York, Dec. 2002d. Disponível em: https://undocs.org/en/A/RES/57/239. Acesso em: 13 ago. 2022.

UNITED NATIONS GENERAL ASSEMBLY - UNGA. Resolution 58/32, *Developments in the Field of Information and Telecommunications in the Context of International Security*. New York, Dec. 2003a. Disponível em: https://undocs.org/en/A/RES/58/32. Acesso em: 14 jan. 2023.

UNITED NATIONS GENERAL ASSEMBLY - UNGA. Resolution 58/199, *Creation of a global culture of cybersecurity and the protection of critical information infrastructures*. New York, Dec. 2003b. Disponível em: https://undocs.org/en/A/RES/58/199. Acesso em: 13 ago. 2022.

UNITED NATIONS GENERAL ASSEMBLY - UNGA. Resolution 59/61, *Developments in the Field of Information and Telecommunications in the Context of International Security*. New York, Dec. 2004. Disponível em: https://undocs.org/en/A/RES/59/61. Acesso em: 14 jan. 2023.

UNITED NATIONS GENERAL ASSEMBLY - UNGA. Resolution 60/45, *Developments in the Field of Information and Telecommunications in the Context of International Security*. New York, Dec. 2005. Disponível em: https://undocs.org/en/A/RES/60/45. Acesso em: 11 nov. 2019.

UNITED NATIONS GENERAL ASSEMBLY - UNGA. Resolution 61/54, *Developments in the Field of Information and Telecommunications in the Context of International Security*. New York, Dec. 2006. Disponível em: https://undocs.org/en/A/RES/61/54. Acesso em: 14 jan. 2023.

UNITED NATIONS GENERAL ASSEMBLY - UNGA. Resolution 62/17, *Developments in the Field of Information and Telecommunications in the Context of International Security*. New York, Jan. 2008. Disponível em: https://undocs.org/en/A/RES/62/17. Acesso em: 14 jan. 2023.

UNITED NATIONS GENERAL ASSEMBLY - UNGA. Resolution 63/37, *Developments in the Field of Information and Telecommunications in the Context of*

International Security. New York, Jan. 2009. Disponível em: https://undocs.org/en/A/RES/63/37. Acesso em: 14 jan. 2023.

UNITED NATIONS GENERAL ASSEMBLY - UNGA. Resolution 64/25, *Developments in the Field of Information and Telecommunications in the Context of International Security*. New York, Jan. 2010a. Disponível em: https://undocs.org/en/A/RES/64/25. Acesso em: 14 jan. 2023.

UNITED NATIONS GENERAL ASSEMBLY - UNGA. Resolution 64/211, *Creation of a global culture of cybersecurity and taking stock of national efforts to protect critical information infrastructures.* New York, Mar. 2010b. Disponível em: https://undocs.org/en/A/RES/64/211. Acesso em: 13 ago. 2022.

UNITED NATIONS GENERAL ASSEMBLY - UNGA. Resolution 65/41, *Developments in the Field of Information and Telecommunications in the Context of International Security.* New York, Dec. 2010c. Disponível em: https://undocs.org/en/A/RES /65/41. Acesso em: 11 nov. 2019.

UNITED NATIONS GENERAL ASSEMBLY - UNGA. Resolution 66/24, *Developments in the Field of Information and Telecommunications in the Context of International Security.* New York, Dec. 2011. Disponível em: https://undocs.org/en/%20A/ RES/66/24. Acesso em: 11 nov. 2019.

UNITED NATIONS GENERAL ASSEMBLY - UNGA. Resolution 67/27, *Developments in the Field of Information and Telecommunications in the Context of International Security.* New York, Dec. 2012. Disponível em: https://undocs.org/en/A/RES/64/25. Acesso em: 14 jan. 2023.

UNITED NATIONS GENERAL ASSEMBLY - UNGA. Resolution 68/167, *The right to privacy in the digital age.* New York, Jan. 2014a. Disponível em: https://undocs.org/en/A/RES /68/243. Acesso em: 11 nov. 2019.

UNITED NATIONS GENERAL ASSEMBLY - UNGA. Resolution 68/243, *Developments in the Field of Information and Telecommunications in the Context of International Security.* New York, Jan. 2014b. Disponível em: https://undocs.org/en/A/RES /68/243. Acesso em: 11 nov. 2019.

UNITED NATIONS GENERAL ASSEMBLY - UNGA. Resolution 69/28, *Developments in the Field of Information and Telecommunications in the Context of International Security.* New York, Dec. 2014c. Disponível em: https://undocs.org/en/A/RES/69/28. Acesso em: 14 jan. 2023.

UNITED NATIONS GENERAL ASSEMBLY - UNGA. Resolution 69/166, *The right to privacy in the digital age.* New York, Feb. 2015a. Disponível em: https://undocs.org/en/A/RES /69/166. Acesso em: 14 jan. 2023.

UNITED NATIONS GENERAL ASSEMBLY - UNGA. Resolution 70/237, *Developments in the Field of Information and Telecommunications in the Context of International Security.* New York, Dec. 2015b. Disponível em: https://undocs.org/en/A/RES /70/237. Acesso em: 11 nov. 2019.

UNITED NATIONS GENERAL ASSEMBLY - UNGA. Resolution 71/28, *Developments in the Field of Information and Telecommunications in the Context of International Security.* New York, Dec. 2016. Disponível em: https://undocs.org/en/A/RES/71/28. Acesso em: 14 jan. 2023.

UNITED NATIONS GENERAL ASSEMBLY - UNGA. Resolution 71/199, *The right to privacy in the digital age.* New York, Jan. 2017. Disponível em: https://undocs.org/en/A/RES /71/199. Acesso em: 14 jan. 2023.

UNITED NATIONS GENERAL ASSEMBLY - UNGA. Resolution 73/27, *Developments in the Field of Information and Telecommunications in the Context of International Security*. New York, Dec. 2018. Disponível em: https://undocs.org/en/A/RES /73/27. Acesso em: 11 nov. 2019.

UNITED NATIONS GENERAL ASSEMBLY - UNGA. Resolution 73/179, *The right to privacy in the digital age*. New York, Jan. 2019a. Disponível em: https://undocs.org/en/A/RES /73/179. Acesso em: 14 jan. 2023.

UNITED NATIONS GENERAL ASSEMBLY - UNGA. Resolution 73/187, *Countering the use of information and communications technologies for criminal purposes*. New York, Jan. 2019b. Disponível em: https://undocs.org/en/A/RES /73/187. Acesso em: 11 nov. 2019.

UNITED NATIONS GENERAL ASSEMBLY - UNGA. Resolution 73/266, *Advancing responsible State behaviour in cyberspace in the context of international security*. New York, Jan. 2019c. Disponível em: https://undocs.org/en/A/RES /73/266. Acesso em: 11 nov. 2019.

UNITED NATIONS GENERAL ASSEMBLY - UNGA. Resolution 74/29, *Developments in the Field of Information and Telecommunications in the Context of International Security*. New York, Dec. 2019d. Disponível em: https://undocs.org/en/A/RES/74/29. Acesso em: 14 jan. 2023.

UNITED NATIONS GENERAL ASSEMBLY - UNGA. Resolution 75/32, *Advancing responsible State behaviour in cyberspace in the context of international security.* New York, Dec. 2020a. Disponível em: https://undocs.org/en/A/RES /75/32. Acesso em: 14 jan. 2023.

UNITED NATIONS GENERAL ASSEMBLY - UNGA. Resolution 75/176, *The right to privacy in the digital age.* New York, Dec. 2020b. Disponível em: https://undocs.org/en/A/RES /75/176. Acesso em: 14 jan. 2023.

UNITED NATIONS GENERAL ASSEMBLY - UNGA. Resolution 75/240, *Developments in the Field of Information and Telecommunications in the Context of International Security.* New York, Jan., 2021a. Disponível em: https://undocs.org/en/A/RES/75/240. Acesso em: 14 jan. 2023.

UNITED NATIONS GENERAL ASSEMBLY - UNGA. Resolution 76/19, *Developments in the Field of Information and Telecommunications in the Context of*

International Security. New York, Dec. 2021b. Disponível em: https://undocs.org/en/A/RES/76/19. Acesso em: 14 jan. 2023.

UNITED NATIONS GENERAL ASSEMBLY - UNGA. Resolution 77/36, *Developments in the Field of Information and Telecommunications in the Context of International Security.* New York, Dez. 2022a. Disponível em: https://undocs.org/en/A/RES/77/36. Acesso em: 14 jan. 2023.

UNITED NATIONS GENERAL ASSEMBLY - UNGA. Resolution 77/37, *Programme of action to advance responsible State behaviour in the use of information and communications technologies in the context of international security.* New York, Dec. 2022b. Disponível em: https://undocs.org/en/A/RES /77/37. Acesso em: 14 jan. 2023.

UNITED NATIONS GENERAL ASSEMBLY - UNGA. Resolution 77/211, *The right to privacy in the digital age.* New York, Jan. 2023. Disponível em: https://undocs.org/en/A/RES /77/211. Acesso em: 14 jan. 2023.

UNIVERSITY OF OXFORD (OXFORD). Global Cyber Security Capacity Centre. *Cybersecurity Capacity Maturity Model for Nation*s (CMM). Rev. Ed. Oxford, 2016. Disponível em: https://cybilportal.org/wp-content/uploads/2020/05/cmm-revised-edition_09022017_1.pdf . Acesso em: 10 set. 2020.

UNIVERSITY OF OXFORD *et al. Cybersecurity Capacity Review: Federative Republic of Brazil*. Oxford, 2020a. Disponível em: http://www.oas.org/en/sms/cicte/docs/eng-cybersecurity-capacity-review-brazil.pdf. Acesso em: 30 set. 2020.

UNIVERSITY OF OXFORD *et al. Revisão da Capacidade de Cibersegurança: República Federativa do Brasil.* Oxford, 2020b. Disponível em: https://www.oas.org/pt/ssm/cicte/docs/PORT-Revisao-da-Capacidade-de-Ciberseguranca.pdf. Acesso em: 04 ago. 2022.

UNIVERSITY OF OXFORD. Global Cyber Security Capacity Centre. *Cybersecurity* Capacity *Maturity Model for Nation*s (CMM). Oxford, 2021. Disponível em: https://gcscc.ox.ac.uk/files/cmm2021editiondocpdf. Acesso em: 04 ago. 2022.

VALES, Tiago; SATER, Joe Abdul. Is There a Way to Desecuritise Cyberspace? How Brazil's Legal Framework for the Internet Could Have Done That. *Encuentro Latinoamericano,* Montreal, v. 4, n. 2, p. 77-92, 2017. Disponível em: https://iapss.org/core/storage/2021/11/ELA_4_2.pdf . Acesso em: 29 dez. 2022.

VAN EVERA, Stephen. *Guide to Methods for Students of Political Science*. Ithaca: Cornell University Press, 1997.

VICHI, Leonardo. Prefácio. *In*: AYRES PINTO, Danielle Jacon; PAGLIARI, Graciela de Conti; GRASSI, Jéssica Maria (org.). *A geopolítica das estratégias em defesa cibernética*: como EUA, China, Rússia e Israel protegem seu ciberespaço. Rio de Janeiro: Alpheratz, 2021. p. 7-10.

WIMMER, Miriam. Interfaces entre Proteção de Dados Pessoais e Segurança da Informação: um debate sobre a Relação entre Direito e Tecnologia. *In*: DONEDA,

Danilo; MENDES, Laura Schertel Mendes; CUEVA, Ricardo Villas Bôas (org.). *Lei Geral de Proteção de Dados Pessoais*: a caminho da efetividade: contribuições para a implementação da LGPD. São Paulo: Revista dos Tribunais, 2020, p. 127-144.

WORLD ECONOMIC FORUM. *The Global Risks Report*. 17 ed. Geneva, 2022. Disponível em: https://www3.weforum.org/docs/WEF_The_Global_Risks_Report_2022.pdf. Acesso em: 21 maio 2022.

APÊNDICE A - APRESENTAÇÃO

A presente pesquisa foi fruto de uma necessidade e uma aspiração. Em primeiro lugar uma necessidade de melhor compreensão de como o Brasil estava e continua a navegar nas águas da governança nacional de segurança cibernética, no seu sentido mais amplo, e quais modelos existentes e utilizados pela comunidade internacional poderiam auxiliar o país nesse processo. Sem desconsiderar as suas peculiaridades, inclusive do seu ordenamento jurídico e suas características culturais, sociais, políticas, econômicas e, até mesmo, sua dimensão continental, e suas percepções de desenvolvimento, essa discussão pode contribuir para que o Brasil possa trilhar o seu caminho de construção das capacidades necessárias para fazer frente aos desafios de promover a segurança cibernética, e, assim, maximizar os benefícios da transformação digital da sociedade e da economia para todos brasileiros.

Em segundo lugar, uma aspiração, um desejo de com base nesse entendimento, a pesquisa pudesse efetivamente traduzir-se em prescrição de política pública, especialmente, assistindo o país na elaboração do marco legal adequado e do estabelecimento de uma Autoridade Nacional, os quais ainda restam pendentes, em que pese movimentos de avanço e retrocesso relatados durante o trabalho.

Aliando necessidade e aspiração, encontra-se a trajetória profissional há quase duas décadas para a Agência Nacional de Telecomunicações (Anatel), que detém importante papel nessa seara, como reguladora da infraestrutura que permite a conectividade e, portanto, papel fundamental na promoção de segurança cibernética não só para o setor, mas para o país. Ademais, a Anatel possui a particular competência legal de representar o Brasil nos órgãos internacionais de telecomunicações, sob coordenação do Poder Executivo, participando ativamente das atividades da União Internacional de Telecomunicações (UIT), da Organização para a Cooperação e Desenvolvimento Econômico (OCDE) e da Organização dos Estados Americanos, inclusive nas questões relacionadas à segurança cibernética.

Dessa forma, uma das suas principais atividades profissionais é o engajamento desde 2009 nessas organizações, compondo as delegações brasileiras nesses fóruns, inclusive nas últimas duas Conferências de Plenipotenciários da UIT (realizadas em 2018 em Dubai, nos Emirados Árabes; e em 2022 em Bucareste, na Romênia), nas quatro últimas Conferências Mundiais de Desenvolvimento de Telecomunicações, e diversas reuniões do Grupo de Trabalho sobre Segurança na Economia Digital da OCDE.

Nessa linha, atualmente trabalha-se na coordenação da resposta do Brasil ao Índice Global de Segurança Cibernética e preside-se o Grupo de Experts do índice. Ademais, já se

liderou grupos de aprimoramento desse questionário; contribuiu-se para o processo de revisão e atualização das recomendações da OCDE na matéria; e também foi realizada colaboração, de forma individual, na Consulta Pública da Estratégia Nacional de Segurança Cibernética (E-Ciber), sendo várias das suas contribuições incorporadas ao texto final, embora a contribuição sobre a necessidade de um agência na matéria não tenha sido acatada.

Recentemente, também foi assumida a liderança da Questão de Estudos de Segurança Cibernética no âmbito do Setor de Desenvolvimento da UIT, conjuntamente com representante dos EUA, a fim de enfrentar questões de interesse do país, como segurança cibernética no 5G; esquema de certificação em segurança cibernética; conscientização; dentre outros. Cumpre ressaltar que o conteúdo desse estudo foi estabelecido por proposta brasileira levada à Conferência de Mundial de Desenvolvimento das Telecomunicações, realizada em Kigali, na Ruanda em 2022.

Ainda no âmbito da Anatel, a servidora é uma das responsáveis pelo andamento operacional e logístico do Grupo Técnico de Segurança Cibernética e Gestão de Riscos de Infraestrutura Crítica (GT-Ciber). Esse grupo foi criado pelo Regulamento de Segurança Cibernética Aplicada ao Setor de Telecomunicações, aprovado pela Resolução nº 740, de 21 de dezembro de 2020, contribuindo-se na sua elaboração e, atualmente, dedicando-se para sua implementação. A finalidade da instituição do grupo é estruturar a governança da segurança cibernética no setor, reconhecendo justamente a transversalidade do tema e a necessidade do multissetorialismo.

Por todo exposto, destaca-se a familiarização com esses modelos da comunidade internacional; a vivência da realidade fragmentada da nossa governança institucional nacional; a experiência de representação brasileira nesses fóruns; e busca pela internalização de melhores práticas, dedicando-se cotidianamente para promover a segurança das redes brasileiras.