Luca Belli
Breno Pauli Medeiros
Natália Couto
Erica Bakonyi
Walter Britto Gaspar
Daniel Dore Lage

Governança e regulação da cibersegurança no Brasil

Proteção da infraestrutura crítica, segurança da informação e construção da soberania digital

Prefácio de Marcos Antonio Amaro dos Santos, Ministro de Estado Chefe do Gabinete de Segurança Institucional da Presidência da República

Lumen Juris Direito

Governança e regulação da cibersegurança no Brasil

Lumen Juris Editora

www.lumenjuris.com.br

Filiais

Sede: Rio de Janeiro
Rua Newton Prado, nº 43
CEP: 20930-445
São Cristóvão
Rio de Janeiro – RJ
Tel. (21) 2580-7178

Maceió
(Divulgação)
Cristiano Alfama Mabilia
cristiano@lumenjuris.com.br
Maceió – AL
Tel. (82) 9-9661-0421

Luca Belli
Breno Pauli Medeiros
Natália Couto
Erica Bakonyi
Walter Britto Gaspar
Daniel Dore Lage

Governança e regulação da cibersegurança no Brasil

Proteção da infraestrutura crítica, segurança da informação e construção da soberania digital

Prefácio de Marcos Antonio Amaro dos Santos, Ministro de Estado Chefe do Gabinete de Segurança Institucional da Presidência da República

Editora Lumen Juris
Rio de Janeiro
2026

Categoria: Direito Digital

Editor: João Luiz da Silva Almeida
Produção editorial: Angel Cabeza
Designer editorial: Rebecca Ramos e Thassiel Melo
Diagramação: Renata Chagas
Gerente administrativo-financeiro: Carla Sampaio
Financeiro: Juliano de Oliveira
Assistente financeiro: Jefferson Badaró
Gerente comercial e logística: Arlei Rocha
Comercial e relacionamento: Cristiano Mabilia
Eventos: Arianna Pacheco

Impresso no Brasil | *Printed in Brazil*

Dados Internacionais de Catalogação na Publicação (CIP)

G721

Governança e regulação da cibersegurança no Brasil : proteção da infraestrutura crítica, segurança da informação e construção da soberania digital : de acordo com a Estratégia Nacional de Cibersegurança, decreto nº 12.573/2025 / Luca Belli... [et. al] ; prefácio de Marcos Antonio Amaro dos Santos. – 1. ed. – Rio de Janeiro : Lumen Juris, 2025.

296 p. ; 23 cm.

Inclui bibliografia.
ISBN 978-85-519-3792-1

1. Redes de computadores - Medidas de segurança. 2. Segurança da informação. 3. Crime por computador - Legislação. 4. Governança da internet. 5. Regulação. I. Belli, Luca (autor). II. Medeiros, Breno Pauli (autor). III. Couto, Natália (autor). IV. Bakonyi, Erica (autor). V. Gaspar, Walter Brito (autor). VI. Lage, Daniel Dore (autor). VII. Santos, Marcos Antonio amaro dos (prefaciador). VIII. Título.

CDD 343.09981

Ficha catalográfica elaborada por Ellen Tuzi CRB-7: 6927

Editora Lumen Juris
Rua Newton Prado, 43, São Cristóvão, Rio de Janeiro/RJ
CEP: 20930-445
Telefone: (21) 2580-7178 | atendimento@lumenjuris.com.br

Prefácio

É com grande satisfação que apresento ao público a obra Governança e regulação da cibersegurança no Brasil. Em um mundo dinâmico e extremamente interconectado, a proteção do ciberespaço deixou de ser tema exclusivo de especialistas para afirmar-se como tema de Política Pública, Segurança Nacional, Soberania e Cidadania.

O país destaca-se pela velocidade de sua transformação digital. Infraestruturas críticas, serviços essenciais, atividades econômicas e a vivência diária encontram-se, cada vez mais, condicionados às tecnologias digitais. Essa realidade amplia, de modo significativo, a necessidade de proteger os ciberativos nacionais, mitigar vulnerabilidades e assegurar a continuidade de serviços estratégicos.

Assim, o livro expressa a necessária colaboração entre Estado, setor produtivo, academia, sociedade civil e Forças Armadas, ressaltando a importância de uma abordagem multidisciplinar e integrada. Mais que um compêndio teórico, apresenta-se como guia prático e acessível, útil tanto para especialistas – gestores públicos, profissionais de segurança e acadêmicos – quanto para a população em geral, cada vez mais exposta aos riscos do ambiente digital.

A obra expõe, de forma abrangente e didática, aspectos técnicos, jurídicos, administrativos e estratégicos da cibersegurança, harmonizando profundidade analítica com simplicidade expositiva. Ela examina as bases conceituais e institucionais do tema, ao mesmo tempo em que detalha os mecanismos regulatórios que estruturam a resposta nacional às ameaças digitais. Ao fazê-lo, oferece contribuição valiosa para consolidar um arcabouço sistêmico de proteção cibernética em sintonia com as melhores práticas internacionais.

Destaco que este trabalho dialoga diretamente com a Estratégia Nacional de Cibersegurança, instituída pelo Decreto nº 12.573, de 4 de agosto de 2025. Essa Estratégia é organizada em quatro eixos fundamentais: (i) proteção do cidadão e da sociedade; (ii) resiliência dos serviços essenciais e das infraestruturas críticas; (iii) cooperação entre instituições públicas e privadas; e (iv) soberania nacional e governança. Trata-se, portanto, de uma obra que reforça a visão estratégica do Estado, traduzindo-a em conhecimento prático e pedagógico.

Outro mérito relevante desse trabalho é sua visão multidisciplinar. A cibersegurança não se resume a um desafio tecnológico, envolve também segurança, direito, administração pública, economia, defesa, educação e relações internacionais. Essa abordagem integrada é indispensável para robustecer a resiliência digital do país e alicerçar o caminho para uma verdadeira soberania digital.

O livro oferece, ainda, significativas reflexões sobre a educação e a literacia digital como fundamentos para a segurança cibernética. A difusão de práticas de ciber-higiene, a capacitação de profissionais e a conscientização da sociedade constituem condições indispensáveis para reduzir riscos e sedimentar uma cultura nacional de segurança digital.

Por todas essas razões, considero que este livro tornar-se-á referência essencial para gestores, reguladores, profissionais de tecnologia, militares, acadêmicos e todos aqueles que, de diferentes formas, contribuem para a segurança do ciberespaço brasileiro. Sua relevância pedagógica e estratégica é inegável e certamente se refletirá na formulação de políticas públicas, em cursos de capacitação, em ações de conscientização e em práticas cotidianas de instituições e cidadãos.

Em suma, o livro Governança e regulação da cibersegurança no Brasil sistematiza os fundamentos da segurança digital e se apresenta como instrumento estratégico de capacitação de múltiplos atores. Com isso, fortalece a posição do país rumo a uma cibersegurança robusta, em consonância com as necessidades brasileiras e com as melhores práticas internacionais.

Ao apresentá-lo, cumprimento seus autores Luca Belli, Breno Pauli Medeiros, Natália Couto, Erica Bakonyi, Walter Britto Gaspar e Daniel Dore Lage e reitero a convicção de que a construção de uma cibersegurança sólida e soberana requer a união de esforços entre Estado e sociedade, coordenação permanente e atualização contínua diante dos desafios do mundo digital. Que esta obra inspire e oriente tais ações, servindo de alicerce para um Brasil mais seguro, resiliente e preparado para o futuro.

Brasília, 24 de setembro de 2025.

Marcos Antonio Amaro dos Santos

Ministro de Estado Chefe do Gabinete de
Segurança Institucional da Presidência da República.

Sobre os Autores

Luca Belli, PhD, é professor da Escola de Direito do Rio de Janeiro da Fundação Getulio Vargas (FGV Direito Rio), onde coordena o Centro de Tecnologia e Sociedade (CTS) e o projeto CyberBRICS; doutor (PhD) em direito público pela Université Paris Panthéon-Assas; autor de mais de 80 publicações sobre governança e regulação de tecnologias. Luca é editor do *International Data Privacy Law Journal* da Oxford University Press, e Diretor da conferência *Computers Privacy and Data Protection in Latin America* (CPDP LatAm). Em julho de 2025, foi nomeado membro do Conselho Nacional sobre Transformação Digital, estabelecido pela Presidência da República, e, em fevereiro de 2024, foi nomeado membro do Comitê Nacional de Cibersegurança da Presidência da República.

Breno Pauli Medeiros é pesquisador do projeto CyberBRICS, no Centro de Tecnologia e Sociedade da Escola de Direito do Rio de Janeiro da Fundação Getulio Vargas (FGV Direito Rio); pesquisador de Pós-Doutorado na Escola de Comando e Estado-Maior do Exército (ECEME), no projeto PRO-DEFESA V: Inteligência Artificial e Tecnologias Quânticas; especialista em *Cyber Policy Development* pelo William J. Perry Center for Hemispheric Defense Studies. Atuou como *Visiting Research Associate* na King's College London entre 2022 e 2023.

Natália Couto é doutoranda e mestre em Direito da Regulação pela Escola de Direito do Rio de Janeiro da Fundação Getúlio Vargas (FGV Direito Rio); pesquisadora e coordenadora de projetos no Centro de Tecnologia e Sociedade da FGV Direito Rio no projeto CyberBRICS – cibersegurança; é professora convidada do LL.M em Direito: Regulação da Inteligência Artificial e Tecnologias Digitais na FGV Direito Rio; e especialista em direito público e privado pela Escola da Magistratura do Estado do Rio de Janeiro (EMERJ).

Erica Bakonyi é doutoranda em Direito da Regulação, na FGV Direito Rio; mestre em Direito pela Universidade de Coimbra; possui MBA em Gestão da Segurança da Informação (Infnet) e especialização em Licitações e Contratos Administrativos (Uniseb); membro do Conselho Municipal de Proteção de Dados Pessoais e da Privacidade (CMPDPP) da cidade do Rio de Janeiro; pesquisadora na Centro de Tecnologia e Sociedade da FGV Direito Rio, no projeto CyberBRICS. Advogada e Consultora na área de Proteção de Dados; atuação como DPO-as-a-service; ministra cursos nas áreas de proteção de dados pessoais, segurança da informação e inteligência artificial; e foi *Visiting Fellow* na ANU Australian College of Law 2025.

Walter Britto Gaspar é advogado; pesquisador; designer gráfico; doutorando em políticas públicas na UFRJ; especializado em sistemas de inovação, direitos digitais e proteção de dados. Sua pesquisa de doutorado foca no sistema brasileiro de inovação em tecnologias quânticas. Atua como pesquisador e coordenador de projetos no Centro de Tecnologia e Sociedade da FGV Direito Rio, nos projetos Data Regulations e CyberBRICS; é professor de Ética na Manipulação de Dados na Escola de Matemática Aplicada da Fundação Getulio Vargas; e membro do Conselho Municipal de Proteção de Dados Pessoais e da Privacidade (CMPDPP), Rio de Janeiro.

Daniel Dore Lage é pesquisador do Centro de Tecnologia e Sociedade da FGV Direito Rio); mestre em Direito da Regulação (FGV Direito Rio); pós-graduando em Crimes Cibernéticos, Cibersegurança e Inteligência (Instituto Greco); pós-graduado em Direito Digital (CERS), Direito Público (PUC-Minas), Ciências Penais (UFJF) e em Direito Urbanístico e Ambiental (PUC-Minas); graduado em Direito (UFJF); consultor em proteção de dados pessoais e privacidade; e *Fellow of Information Privacy*, CIPP/E e CIPT (IAPP).

Sumário

Lista de ilustrações

Lista de quadros

Introdução

O leitor desse livro já deve estar amplamente acostumado às inúmeras notícias de incidentes de segurança, cibercrimes, incidentes cibernéticos; ou talvez ter sido até vítima de tais acontecimentos que se tornaram, tristemente, ocorrências frequentes. O atual processo de transformação digital, intensificado pela pandemia de Covid-19, impulsionou uma digitalização sem precedentes de sistemas, infraestruturas e serviços públicos e privados, gerando benefícios significativos, mas também desafios inéditos. Este estudo se concentra nos desafios da cibersegurança que nossa sociedade, economia e democracia precisam enfrentar para se tornar mais resilientes e alcançar a soberania digital.[1]

Neste sentido, este volume analisa as diferentes dimensões da governança e da regulação da cibersegurança, começando pela exploração das bases conceituais da própria noção de cibersegurança, para analisar subsequentemente quais são suas dimensões e identificar os elementos estratégicos, regulatórios e institucionais necessários para afirmar uma cibersegurança efetiva. Tal análise nos permite traçar um diagnóstico da situação paradoxal da cibersegurança no Brasil.

O Brasil é um raro exemplo de país que sobe consideravelmente nos rankings internacionais de cibersegurança, sendo atualmente o segundo mais ciberseguro das Américas,[2] enquanto, ao mesmo tempo, vê aumento exponencial no volume de ciberataques sofridos.[3] Assim como no expe-

1 Para uma análise deste conceito e sua conexão com a cibersegurança, ver a seção 1.7.

2 Em 2021, o Brasil subiu 53 posições, passando do 71º para o 18º lugar, no Global Cybersecurity Index, *ranking* sobre segurança produzido pela União Internacional de Telecomunicações, agência do setor de tecnologia da ONU. Ainda em 2018, o Brasil era classificado como o 6º país nas Américas, em 2021 como 3º e, na edição mais recente do *ranking*, publicada em 2025, o segundo país mais comprometido com a Agenda Global de Cibersegurança da UIT que define objetivos no tocante às medidas legais; medidas técnicas e procedimentais; estruturas organizacionais (governança); capacitação e conscientização; e cooperação internacional. Todas as edições do ranking se encontram disponíveis no site dedicado ao ITU. Global Cybersecurity Index. Disponível em: https://www.itu.int/en/ITU-D/Cybersecurity/Pages/global-cybersecurity-index.aspx.

3 Segundo a empresa Fortinet (2025), o Brasil foi alvo de 356 bilhões de tentativas de ciberataques em 2024.

rimento hipotético proposto pelo físico austríaco Erwin Schrödinger em 1935, a cibersegurança no Brasil parece estar, ao mesmo tempo, avançando e retrocedendo – em um estado paradoxal de sobreposição, simultaneamente segura e vulnerável, como o famoso gato de Schrödinger, vivo e morto ao mesmo tempo.

Assim, apesar dos evidentes avanços, a situação da cibersegurança no país permanece ainda crítica. Este trabalho argumenta que a atual situação da cibersegurança no Brasil deriva da falta de uma abordagem sistêmica direcionada à análise do funcionamento das tecnologias digitais e de qual tipo de governança, política industrial, capacitação e regulação são necessárias para conseguir enxergar os riscos existentes e mitigá-los de maneira eficiente e efetiva (Belli *et al.,* 2023b). Nos parece evidente que, não obstante seus benefícios inegáveis, o nosso processo de transformação digital também trouxe uma série de desafios, que estamos somente aprendendo a enfrentar e que, neste contexto, a cibersegurança ganha um papel-chave para o desenvolvimento sustentável do país.

Particularmente, os últimos 20 anos testemunharam o aumento da escala e sofisticação das ciberameaças (Koupaei, 2023; Li; Liu, 2021) que incluem violação de privacidade, ciberataques, amplo número de cibercrimes, o crescente uso ofensivo de inteligência artificial (Belli, 2024a) e até campanhas de desinformação voltadas a interferir em processos democráticos (Belli *et al*., 2023b). Dessa forma, incidentes cibernéticos com grande visibilidade mediática não somente levaram ao grande público a percepção dos riscos cibernéticos e de suas consequências concretas, como a paralisia decorrente do *ransomware* Wannacry em 2017 ou o incidente da Crowdstrike, em 2024, como também consolidou nos tomadores de decisão a necessidade de enfrentar e/ou eventualmente mitigar estas ameaças.

Porém, no momento desta publicação, uma Lei Geral de Cibersegurança e uma Agência Nacional de Cibersegurança – elementos que já destacamos como essenciais para conseguir proporcionar soluções orgânicas à falta de cibersegurança no Brasil (Belli *et al*., 2023b) – ainda não foram adotadas, apesar das evidências que ilustram de maneira contundente a necessidade de tais elementos. Assim, ao longo dos últimos anos, o Brasil testemunhou um número crescente de incidentes cibernéticos, que continua aumentando exponencialmente (Fortinet, 2025; Kaspersky, 2025).

A título de exemplo, elencam-se ataques ao Poder Judiciário que inviabilizaram o acesso ao sistema judicial por semanas (Vital, 2020), incidentes cibernéticos que envolveram a paralisação do serviço de informações do Ministério da Saúde (ConectSUS), impedindo a população de acessar informações do seu histórico vacinal e comprometendo dados pessoais sensíveis de cidadãos (Vargas; Rodrigues, 2021), e ataques sofridos por inúmeras administrações estaduais e municipais, representados de maneira eloquente pelo ciberataque os sistemas da Prefeitura do Rio de Janeiro, que obrigou a interrupção de serviços públicos tais como emissão de nota fiscal eletrônica, e outros serviços essenciais por várias semanas (Schendes, 2022).

Somam-se a estes incidentes ocorrências mais recentes como a invasão e o vazamento de informações de sistemas públicos, incluindo os sistemas do Ministério Público, Senado Federal, Exército Brasileiro, e centenas de outros ataques e falhas relatados cotidianamente pela imprensa (G1, 2024). Como destacaremos neste trabalho, a necessidade de um pensamento sistêmico deriva não somente da multiplicidade e complexidade dos elementos que compõem as tecnologias digitais, mas também da interconexão entre tais tecnologias que, frequentemente, são compartilhadas ou usadas por um amplo leque de organizações. Neste sentido, por exemplo, o incidente que desabilitou o Sistema Eletrônico de Informações (SEI), usado para a elaboração, edição e tramitação de documentos do Governo Federal, afetou também o Ministério da Gestão e Inovação (MGI) e se alastrou para outros oito ministérios, além da Casa da Moeda e do Conselho de Controle de Atividades Financeiras (COAF) (Boechat, 2024). Outro exemplo que se destaca foi o incidente envolvendo uma empresa responsável por mediar transferências bancárias no Sistema Financeiro Nacional (SFN) que configurou, até então, o maior ataque financeiro da história do Brasil (BBC News Brasil, 2025).

Muitos destes eventos, assim como outros ao redor do globo, combinam técnicas variadas para explorar vulnerabilidades provocadas por falhas técnicas de sistemas, redes ou decorrentes de ações humanas, sejam elas intencionais ou não (Belli *et al.*, 2023b).[4] Comumente, os atores que

4 Embora os incidentes cibernéticos possam ter uma miríade de causas e perpetradores, um ciberataque abrange diversas fases e estratégias, frequentemente adaptadas ao objetivo do agressor e ao perfil da vítima. Em geral, o ataque inicia-se com a fase de reconhecimento, na qual o invasor coleta informações sobre os sistemas-alvo, buscando identificar vulnerabilidades

exploram essas vulnerabilidades englobam desde atacantes com motivação própria até grupos organizados que podem ser apoiados por Estados ou contratados por entidades privadas (ENISA, 2022b). Contribuindo para a complexidade deste cenário, tornou-se notório o papel que tecnologias, como a Inteligência Artificial (IA), vêm desempenhando em ataques cibernéticos, potencializando os componentes técnicos e sociais inerentes a estas ameaças (Geluvaraj; Satwik; Kumar, 2018; Malatji; Tolah, 2024).

Esta realidade exige estratégias sofisticadas de mitigação de riscos, defesa e resiliência, para conter o impacto potencial de um incidente cibernético. O conjunto dessas estratégias e medidas é tratado como segurança cibernética. Como discutiremos ao longo deste volume, a imensa maioria dos riscos cibernéticos poderia ser evitada – ou ao menos mitigada – com a adoção de medidas básicas de ciber-higiene. Contudo, estas práticas ainda são pouco comuns entre a população, em grande parte devido à baixa literacia digital (Microsoft, 2024; Verizon, 2025).

Em vista deste contexto, o presente trabalho almeja oferecer uma contextualização necessária para entender, primeiramente, a interconexão dos demais elementos que compõem uma abordagem sistêmica à cibersegurança e, em seguida, um retrato do panorama brasileiro da cibersegurança. Consoante essa aspiração, o trabalho pretende avançar respondendo à seguinte pergunta de pesquisa: Quais são os conceitos, objetos e atores envolvidos na cibersegurança, e quais estratégias e regulações já existem ou devem ser desenvolvidas ou fortalecidas para a proteção de ativos digitais, promovendo uma cibersegurança centrada nas pessoas?

A estrutura deste trabalho

Para tanto, este trabalho parte da análise do próprio conceito de cibersegurança para entender quais são as ações necessárias para traduzir

específicas. Em seguida, ocorre a fase de exploração, onde técnicas como *phishing*, injeção de *malware* ou exploração de falhas conhecidas são utilizadas para ganhar acesso não autorizado. Após a invasão, o atacante busca estabelecer presença contínua na rede, por meio de *backdoors* ou outros métodos de persistência, garantindo a capacidade de retorno e controle. Durante essa fase, ele pode realizar movimentos laterais na rede, expandindo seu acesso e escalando privilégios para obter controle mais profundo e abrangente. Na fase final, o ciberataque culmina com a execução do objetivo principal, que pode envolver a extração de dados sensíveis, sabotagem de sistemas, extorsão financeira ou espionagem.

tal conceito em prática e como estas ações devem ser integradas numa visão estratégica e articuladas por meio de um mecanismo de governança efetivo. Neste sentido, o trabalho dá continuidade a produções anteriores precedentes (Belli, 2021a; Belli *et al.*, 2023b; Goldoni; Rodrigues; Medeiros, 2024), com intuito de oferecer um diagnóstico da atual situação da cibersegurança brasileira e debater quais opções poderiam ser mais palatáveis para melhorar o cenário atual, caracterizado por uma percepção difundida de fragmentação regulatória e "ciber-insegurança" (Cloudflare, 2024; ENISA, 2024b; Inter American Development Bank; Organization of American States, 2020).

Diante desses desafios e em conformidade com os objetivos propostos, o presente trabalho está estruturado em três partes, seguidas de um glossário e complementado por anexos explicativos. A primeira parte se inicia com a identificação do conceito de cibersegurança na literatura, destacando os elementos essenciais que o compõem. Este esforço começa pela análise expositiva da teoria da securitização, que descreve o estabelecimento de objetos de referência a serem securitizados por atores responsáveis. Neste sentido, o entendimento natural é de que a cibersegurança tem por objeto de referência o ciberespaço. Isto é, a coleção das tecnologias digitais que usamos cotidianamente para nossas atividades pessoais, sociais e econômicas.

Contudo, como a seção irá demonstrar, a complexidade, amplitude e permeabilidade do que pode ser definido como ciberespaço contribui para um cenário no qual múltiplos atores responsáveis iniciam processos de securitização sobre diferentes componentes dos sistemas digitais que se tornaram essenciais para o funcionamento de nossa sociedade, economia e até da nossa democracia. Estes processos de securitização, por vezes, perpassam diferentes jurisdições, serviços, tecnologias e propriedades, resultando em uma securitização fragmentada.

Amparada por este ponto de partida conceitual, a primeira parte deste trabalho segue então para a construção histórica da forma como o Brasil desenvolveu seu processo de securitização mediante a percepção político-institucional sobre a cibersegurança. Sob a ótica da securitização, o tema passou a ser tratado em duas esferas distintas: a ciberdefesa, vinculada à égide militar, e a cibersegurança, relacionada à política institucional civil. Observa-se, portanto, que os objetos de referência variam conforme a

abordagem adotada: sob uma perspectiva militar, o foco recai sobre o "ciberespaço" como domínio estratégico e operacional; já em uma visão mais ampla de segurança cibernética, incluem-se os chamados "ativos digitais", que compõem o ciberespaço, e as pessoas usuárias de tecnologias digitais.

A depender dos parâmetros do processo de securitização, os atores responsáveis pela promoção da segurança também variam ou se sobrepõem, conferindo maior complexidade à governança do setor. Esse caso se torna evidente no exemplo das infraestruturas críticas, analisadas na seção 1.3, que representam uma interseção entre cibersegurança e ciberdefesa, configurando um objeto de securitização híbrida. Esse estudo permite compreender como diferentes processos de securitização se sobrepõem na proteção de ativos essenciais ao funcionamento não somente econômico, mas também democrático do país, como destacaremos na seção 1.4.

Em seguida, na seção 1.5, o estudo oferece uma taxonomia de ataques e ameaças cibernéticas, para que o leitor consiga entender concretamente quais riscos afetam os ativos digitais, e também frisa a necessidade de se adotar uma abordagem centrada no indivíduo com o objetivo de se construir uma cibersegurança que possa maximizar direitos individuais e coletivos. Neste sentido, a seção 1.6 destaca a relevância de se considerar a cibersegurança como uma ferramenta de proteção e maximização, ao invés de um limitador dos direitos e objetivos constitucionais.

Esta abordagem de cibersegurança centrada nas pessoas prioriza os indivíduos e seus direitos fundamentais, ao contrário do modelo tradicional focado na segurança nacional. Defende que políticas digitais respeitem direitos humanos, com o Estado apoiando instituições que protejam o bem-estar individual, promovendo supervisão cidadã e garantindo liberdade, privacidade e dignidade no ciberespaço. Uma abordagem centrada no papel ativo das pessoas e em sua capacidade de contribuir com sua postura ativa, criativa e inovativa ao desenvolvimento da autonomia tecnológica nacional serve como um pilar da soberania digital, por sua vez, abordada na seção 1.7.

Esta primeira parte se conclui com a seção 1.7 dedicada à soberania digital, voltada não somente a esclarecer este conceito para o leitor, mas também a evidenciar a íntima conexão entre cibersegurança e soberania digital (Belli, 2021a; Belli *et al.*, 2023b; Belli; Goldoni; Karina, 2023; Goldoni; Rodrigues; Medeiros, 2024). Esta conexão será ilustrada de maneira

ainda mais contundente nas Seções 2.5 e 2.6, dedicadas, respectivamente, à literacia digital e à política industrial, destacando que a construção da cibersegurança não deve ser enxergada como custo, mas como uma oportunidade para promover o desenvolvimento social e econômico do país.

A segunda parte deste volume oferece uma fotografia do cenário regulatório da cibersegurança no Brasil, incluindo iniciativas que precisam ser desenvolvidas e/ou amadurecidas para promover a cibersegurança. Esta parte adota uma abordagem cartesiana, decompondo a cibersegurança em seus diferentes componentes: governança; regulação setorial; segurança da informação; combate ao cibercrime; literacia digital; política industrial; e relação com as chamadas tecnologias disruptivas, e em específico a IA.

Especialmente, esta parte almeja destacar a necessidade de se adotar uma abordagem sistêmica para desenvolver estratégias e planos de implementação capazes de concretizar a segurança e a defesa dos objetos de referência, conseguindo ao mesmo tempo entender e mitigar riscos e reafirmar a autodeterminação e a autonomia tecnológica. Dada a complexidade do tema, considera-se, neste trabalho, igualmente essencial a adoção de mecanismos ágeis e eficientes de governança com foco na coordenação e cooperação entre atores, seja para proporcionar uma maior sinergia entre eles, e/ou para facilitar a interação público-privada.

Haja vista a evidente pluralidade de atores de natureza muito diferente que participam desse ecossistema e necessitam ser implicados para alcançar respostas efetivas, nos parece essencial que tal multiplicidade de atores seja implicada em um mecanismo capaz de proporcionar uma comunicação, coordenação e cooperação na perspectiva de incrementar a qualidade da elaboração e implementação da regulação em cibersegurança (Belli, 2015; Belli *et al.*, 2023b).

Nesse sentido, diante do cenário dinâmico que caracteriza a cibersegurança e das crescentes ameaças, o fortalecimento da governança e da regulação da cibersegurança torna-se ainda mais urgente, exigindo uma abordagem integrada entre diferentes setores para mitigar riscos emergentes e garantir maior resiliência digital. Em vista deste desafio, a terceira parte deste documento oferece um prognóstico estratégico para a soberania digital do Brasil, no qual a cibersegurança e a literacia digital devem ser pilares fundamentais. Esta última seção levará o leitor até a conclusão deste trabalho, destacando a importância de ações estruturadas e integra-

das, como formação e treinamento, desenvolvimento de competências e capacidades, além de políticas de conscientização voltadas para a cibersegurança, que devem ser alavancadas como eixos centrais de uma política nacional capaz de alcançar cibersegurança e soberania digital.

Ao final, a conclusão aponta elementos que devem ser considerados como pilares de uma nova estratégia de cibersegurança, não somente no contexto brasileiro, mas em qualquer país interessado em fortalecer a segurança de seus ativos digitais e estimular a cooperação entre os atores responsáveis por manter tal cibersegurança. Particularmente, a conclusão inclui a sugestão de algumas abordagens concretas que poderiam ser exploradas para favorecer uma comunicação intrasetorial e a coordenação e cooperação multissetorial. Por fim, o presente trabalho é complementado por um glossário de cibersegurança que visa evidenciar e explicar os diferentes elementos e conceitos utilizados neste estudo.

A conexão deste trabalho com a nova Estratégia Nacional de Cibersegurança

A nova Estratégia Nacional de Cibersegurança (E-Ciber) (GSI, 2025a), instituída pelo Decreto nº 12.573, de 4 de agosto de 2025, atualiza o arcabouço normativo voltado à consolidação da segurança digital brasileira. A E-Ciber 2025 é estruturada em quatro eixos fundamentais que refletem a necessidade de uma abordagem sistêmica (Belli *et al*., 2023b) articulando: *i)* a proteção e a conscientização de cidadãos e sociedade; *ii)* a segurança e resiliência das infraestruturas críticas e dos serviços essenciais; *iii)* a cooperação multissetorial; e *iv)* a soberania nacional.

A E-Ciber representa a segunda edição do instrumento estratégico brasileiro voltado à matéria, sucedendo a versão inaugural, publicada em 2020 e vigente até 2023 (GSI, 2020).[5] A atualização da abordagem brasileira reflete uma evolução conceitual e doutrinária na concepção da cibersegurança, como destacaremos na primeira seção. Adicionalmente, a nova E-Ciber

5 O presente trabalho também abarca a nova edição da Política Nacional de Segurança da Informação, publicada concomitantemente a E-Ciber, pelo Decreto nº 12.572, de 4 de agosto de 2025 (Brasil, 2025).

também traz avanços não somente normativos e organizacionais, como destacaremos na segunda seção deste trabalho. Inserida no marco da Política Nacional de Cibersegurança, a E-Ciber resulta de proposição formulada pelo Comitê Nacional de Cibersegurança, colegiado composto por vinte e cinco instituições, abrangendo órgãos da Administração Pública Federal, representantes de entidades da sociedade civil do meio acadêmico e científico, bem como do setor empresarial, todos com atuação direta ou indireta no campo da segurança cibernética.

O primeiro eixo, voltado à proteção e à conscientização da sociedade, compreende ações educativas e preventivas que visam à construção de uma cultura de segurança digital, com especial atenção à literacia digital e à inclusão de grupos vulneráveis no ambiente virtual. Tal dimensão se coaduna, no presente livro, com a seção 2.5, que examina a literacia digital como instrumento essencial para transformar as pessoas, tipicamente consideradas como o "elo fraco" da cibersegurança, em "elo forte". Essa mudança de paradigma é instrumental não somente para efetivar direitos e garantias fundamentais, mas também para permitir à sociedade brasileira entender os benefícios das tecnologias digitais, sem ser mera consumidora passiva de tais tecnologias, mas conseguindo contribuir ativamente para a segurança digital, se tornando até produtora de soluções de cibersegurança. Neste sentido, o primeiro eixo dialoga também com a soberania digital, que será destacada nas seções 1.7 e 2.5 deste volume.

O segundo eixo, dedicado à segurança e à resiliência dos serviços essenciais e das infraestruturas críticas, propõe o fortalecimento de mecanismos de proteção de setores estratégicos, como energia, telecomunicações, saúde e transporte, por meio da adoção de padrões técnicos, certificações e planos de contingência. Esse conteúdo dialoga diretamente com a seção 2.3, que aborda a segurança da informação, analisando suas dimensões técnicas, normativas e organizacionais.

O terceiro eixo da E-Ciber, centrado na cooperação e na integração entre órgãos e entidades públicas e privadas, encontra correspondência na seção 2.1, relativa à governança. A ênfase recai sobre a criação e o fortalecimento de estruturas colaborativas e multissetoriais de cibersegurança, o compartilhamento de informações sobre incidentes e a construção de protocolos que favoreçam a resposta coordenada a ameaças no ciberespaço, tanto no plano interno quanto no plano internacional.

Por fim, o quarto eixo, que trata da soberania nacional e da governança, orienta-se pela preservação dos interesses estratégicos do país no domínio digital, pela redução da dependência tecnológica externa e pelo fomento à indústria nacional de cibersegurança. Tal eixo se relaciona intimamente com o discurso sobre soberania digital (Belli *et al.*, 2023b; Belli; Jiang, 2024), como será argumentado nas seções 1.7, 2.6 e 3, dedicadas, respectivamente, à relação entre cibersegurança e soberania digital, às dimensões da política industrial, e a necessidade de se estimular o desenvolvimento de soluções nacionais em cibersegurança para incrementar a autonomia tecnológica do país.

No conjunto, observa-se que a nova visão estruturante oferecida pela E-Ciber não apenas converge com as temáticas aqui tratadas, mas também fornecem uma arquitetura lógica e normativa que sustenta o tratamento orgânico da cibersegurança nas dimensões conceituais, normativas, técnicas, institucionais e estratégicas, tal como se desenvolverá ao longo deste trabalho.

1 Cibersegurança: raízes conceituais, políticas e práticas

Para compreender a complexidade do conceito de cibersegurança, torna-se necessária uma breve digressão sobre como a definição de segurança forneceu as bases para o desenvolvimento da noção de cibersegurança. Quando se fala em segurança, uma das vertentes mais difundidas para explicar o seu significado é fundamentada na teoria da securitização da Escola de Copenhague (Hansen; Nissenbaum, 2009; Lobato; Kenkel, 2015).

O ponto central desta teoria foi descrever um processo intersubjetivo pelo qual o conceito de segurança se desloca do domínio político-militar tradicional para uma abordagem mais ampla, abrangendo fenômenos que transcendem a esfera estatal (Buzan *et al.*, 1997). Com isso, possibilitou-se tratar a segurança em muitos setores – econômico ou social, por exemplo – e por diversos atores de natureza diferente, que agem como partes interessadas ou *stakeholders*.

Segundo a teoria da Escola de Copenhague, a segurança não é tratada sob um viés único, mas construída discursivamente em torno de áreas específicas, motivo pelo qual se utiliza o termo "securitização" para caracterizar essa abordagem (Buzan *et al.*, 1997; Fichtner, 2018a; Hansen; Nissenbaum, 2009; Lobato; Kenkel, 2015). Nessa perspectiva, a segurança é um ato de fala que securitiza um ou mais objetos de referência, isto é, objetos que precisam de proteção e, por consequência, necessitam de medidas urgentes a fim de reduzir a situação de risco em que se encontram (Buzan *et al.*, 1997).

Apesar de não estar inicialmente incluída como área securitizada pela Escola de Copenhague, Hansen e Nissenbaum (2009) identificaram a segurança cibernética como um setor específico dentro do terreno mais amplo dos estudos sobre segurança. O discurso securitizador que sustenta a cibersegurança pode ser entendido como um processo em que objetos – sejam digitais, físicos e/ou humanos – tornam-se alvos de ameaças que se manifestam no ciberespaço por meio das demais tecnologias digitais que o compõem. À medida que essa percepção de ameaça se consolida, o discurso securitizador é formalizado em documentos e estratégias nacionais,

provocando transformações no arcabouço político-administrativo dos Estados (Dunn Cavelty; Wenger, 2020; Hansen; Nissenbaum, 2009). Estas mudanças terão maior ou menor urgência, conforme a própria percepção do risco e, consequentemente, irão movimentar esforços de securitização respectivos e proporcionais.

No cenário atual, a percepção de ameaças emana não somente de fontes tradicionais, como forças militares adversárias ou desastres naturais, mas passa a envolver a exploração de vulnerabilidades de sistemas digitais por um amplo leque de finalidades maliciosas por cibercriminosos, *hackers*, terroristas e grupos políticos extremistas. A título de exemplo, pode-se imaginar uma situação em que a infraestrutura crítica e os serviços essenciais de um país sejam alvos de uma ação organizada, em que atores podem utilizar de seu conhecimento técnico para alterar o funcionamento dos componentes digitais que regulam fornecimento de serviços essenciais como infraestrutura hídrica e energética, ou paralisando sistemas de transporte ou interferindo no funcionamento de sistemas de hospitais e sistemas financeiros.

Como frisamos na introdução, esta percepção acerca da pluralidade das ameaças oriundas do ciberespaço é corroborada por evidências de ataques recorrentes, elevando a questão da segurança cibernética de uma preocupação técnica a um tema político-institucional que envolve segurança nacional. Esse raciocínio é consolidado em diretivas e estratégias nacionais que ancoram o discurso securitizador. No Ocidente, por exemplo, Hansen e Nissenbaum (2009) argumentam que o ciberespaço teve seu processo de securitização estabelecido, mediante desenvolvimentos político-institucionais como a criação da *Commission on Critical Infrastructure Protection* em 1996, o lançamento de uma estratégia nacional dos EUA na forma da *National Strategy to Secure Cyberspace de 2003* e a criação do *Cooperative Cyber Defence Centre of Excellence* da OTAN em 2008 (Hansen; Nissenbaum, 2009).

A estes desenvolvimentos ocidentais soma-se a elaboração de vários documentos estratégicos, como a publicação, na China, da *International Strategy of Cooperation on Cyberspace* em 2017 (Ministry of Foreign Affairs of the PRC, 2017) e, na Rússia, da *Foreign Policy Concept of the Russian Federation* em 2016 (The Ministry of Foreign Affairs of the Russian Federation, 2016), em que ambos os países tratam de iniciativas para a proteção do ciberespaço em vista a novas ameaças, fundamentando o discurso securitário também sob uma perspectiva oriental.

No âmbito brasileiro, o discurso e a urgência sobre a necessidade de promover a segurança cibernética podem ser observados nas diversas políticas públicas concretizadas em instrumentos normativos e estratégias, iniciados, em grande parte, nas Forças Armadas Brasileiras e, posteriormente, alargados para o campo da política pública civil.

Para entender o caso brasileiro e esta evolução da esfera militar à civil, podem ser mencionadas, ilustrativamente, a primeira Política de Segurança da Informação, estabelecida em 2000 (Decreto 3.505/2000, Presidência da República, 2000) e posteriormente atualizada em 2018 (Decreto nº 9.637/2018, Presidência da República, 2018), em conjunto com a Estratégia Nacional de Cibersegurança (E-Ciber) de 2020 (Decreto nº 10.222/20; Brasil, 2020b), que foi atualizada em 2025 com a promulgação do Decreto nº 12.573/2025 (GSI, 2025a), por determinação da Política Nacional de Cibersegurança instituída pelo Decreto nº 11.856/2023 (Presidência da República, 2023).

Esses documentos revelam que a cibersegurança no Brasil surgiu, inicialmente, como um tema essencialmente militar, com pouca participação civil. Como será demonstrado à frente, esse quadro foi revertido: a cibersegurança passou a ser predominantemente uma pauta civil, ainda que com a necessária participação das Forças Armadas no campo específico da ciberdefesa.

Somam-se aos decretos supramencionados uma série de documentos tocantes direta ou indiretamente a processos securitários no ciberespaço, tal como estratégias nacionais direcionadas à Defesa (Brasil, 2008, 2012, 2020a; CGEE; MCTI, 2022), às normas setoriais (ANATEL, 2020, 2024; ANEEL, 2021; BCB, 2021), legislações específicas para crimes cibernéticos e a adoção de acordos internacionais como a Convenção de Budapeste sobre Cibercrime (Council of Europe, 2001), além de declarações e posicionamentos de lideranças e representantes políticos (Amorim, 2013).

Conforme destacado na introdução deste trabalho, a amplitude do desafio imposto pela cibersegurança abarca o próprio estabelecimento de um conceito de cibersegurança e os elementos que o compõem. As diversas interpretações desses elementos podem tornar as abordagens sobre o tema ainda mais intrincadas, dificultando a definição de objetivos claros e a delimitação precisa das responsabilidades entre os diferentes atores envolvidos. Por isso, a próxima seção se propõe a explorar o conceito de cibersegurança e analisar criticamente os seus elementos.

1.1 O conceito de cibersegurança

O conceito de cibersegurança não é unívoco na literatura acadêmica. Como um conceito disputado, a cibersegurança abarca diversas definições que envolvem diferentes objetos, escopos, lentes de análise, referenciais teóricos e objetos a serem securitizados (Cavelty, 2013; Dunn Cavelty; Wenger, 2020; Fichtner, 2018a; Wolff, 2016). Em parte, essa pluralidade de definições reflete a volatilidade e transversalidade do conceito, que evoluiu de uma preocupação técnica voltada aos sistemas de informação para uma temática estratégica de alto nível, amplamente discutida em fóruns internacionais e incorporada em documentos estratégicos, como Políticas Nacionais de Segurança e Defesa (Dunn Cavelty; Wenger, 2020; Hansen; Nissenbaum, 2009; Veale; Brown, 2020).

A única definição que alcançou certo consenso global foi elaborada pelo Setor de Normatização das Telecomunicações da União Internacional de Telecomunicações (ITU-T) da ONU cristalizando, portanto, o consenso dos 193 estados-membros, inclusive o Brasil. Essa definição caracteriza a cibersegurança como:

> A cibersegurança é o conjunto de ferramentas, políticas, conceitos de segurança, diretrizes, abordagens de gestão de risco, ações, treinamentos, melhores práticas, garantias e tecnologias que podem ser utilizadas para proteger os ativos do ambiente cibernético, da organização e dos usuários. […] A cibersegurança busca garantir o cumprimento e a manutenção das propriedades de segurança dos ativos da organização e dos usuários contra riscos relevantes à segurança encontrados no ambiente cibernético (ITU-T - International Telecommunication Union, 2008, p. 06).

A amplitude do conceito evidencia a dificuldade de se explicar de maneira sucinta esse fenômeno. Não se observa uma mobilização na literatura e em discursos securitários acerca da necessidade de um marco conceitual, mas é possível notar o entendimento de que a cibersegurança se refere a um conjunto de medidas a serem aplicadas para a proteção dos ativos digitais que compõem o ciberespaço, das pessoas – físicas ou jurídicas – que usam tais ativos, e que abrange as questões relacionadas à segurança nacional em razão do uso de tais ativos (Dunn Cavelty; Wenger, 2020; Fichtner, 2018a).

Porém, a amplitude terminológica que caracteriza a cibersegurança leva os Estados a absorverem diferentes facetas do conceito, de acordo com suas percepções contextuais, redefinindo-as para suas próprias realidades mediante seus respectivos arcabouços político-institucionais.

A partir da definição da ITU-T e de definições presentes na literatura acadêmica, adota-se, neste trabalho, o entendimento da cibersegurança como um conjunto de iniciativas para promover a segurança de objetos de referência – incluindo pessoas – em face de riscos cibernéticos (Hansen; Nissenbaum, 2009). A partir dessa definição, podemos extrair três elementos centrais: *i)* iniciativas de cibersegurança; *ii)* objetos de referência; e *iii)* riscos cibernéticos.

Iniciativas de cibersegurança podem ser entendidas aqui como um conjunto de políticas públicas, normas, práticas empresariais ou organizacionais, compromissos firmados voluntariamente (tal como acordos, contratos, parcerias, entre outros) ou medidas técnicas que sejam utilizadas para se alcançar a segurança dos objetos de referência, sendo essa entendida como o estado de estar protegido e, idealmente, livre de riscos, podendo esse estado ser alcançado preventivamente ou reativamente.

Os objetos de referência correspondem aos ativos digitais que incluem softwares, hardwares, redes, sistemas, informações e dados, infraestruturas, serviços e pessoas prejudicadas pela materialização do risco cibernético e, por isso, precisam de proteção.[6] Esses ativos podem ser privados, públicos ou híbridos a depender dos atores responsáveis pela respectiva gestão. Assim, para que seja garantida a cibersegurança, todos os objetos de referência devem observar as iniciativas de cibersegurança, inclusive quando se tratar da proteção da parte física desses ativos, pois elas permitem que as informações se mantenham íntegras.

Quanto aos riscos cibernéticos, este trabalho utiliza a definição de risco de segurança da informação proposta pelo Glossário de Segurança da Informação, elaborado pelo GSI, como "risco potencial associado à exploração de uma ou mais vulnerabilidades de um ou mais ativos de informação, por parte de uma ou mais ameaças, com impacto negativo no

6 Como será destacado, é preciso proteger a confidencialidade, disponibilidade e integridade da informação e de dados que circulam pelos sistemas. As práticas relacionadas à segurança da informação serão abordadas na seção 2.3 deste trabalho.

negócio da organização" (GSI, 2021, s.p.). O entendimento de risco que o Glossário de Segurança da Informação traz é complementado pela definição elaborada por Grzegorz Strupczewski, que foi considerada particularmente pertinente, após a realização de revisão bibliográfica sobre riscos cibernéticos. Segundo o autor:

> O risco cibernético é um risco operacional associado ao desempenho de atividades no ciberespaço, que ameaça ativos de informação, recursos de TIC e ativos tecnológicos, que podem causar danos materiais a ativos tangíveis e intangíveis de uma organização, interrupção de negócios ou danos à reputação. O termo "risco cibernético" também inclui ameaças físicas aos recursos de TIC dentro da organização (Strupczewski, 2021, p. 6).

A utilização da definição apresentada por Strupczewski, contudo, é realizada com duas ressalvas. A primeira é que, considerando a definição de cibersegurança adotada neste trabalho, acrescenta-se que o termo "risco cibernético" também inclui ameaças direcionadas às pessoas. A segunda ressalva é que, embora haja incompatibilidade das nomenclaturas adotadas quanto aos objetos de referência, vez que Strupczewski menciona "ativos da informação, recursos de TIC e ativos tecnológicos" enquanto o presente trabalho utiliza o termo "ativos digitais", analisando o significado desses termos referenciados pelo autor, é possível concluir que se relacionam aos mesmos objetos.[7]

A não implementação de medidas de mitigação de riscos pode provocar incidentes de cibersegurança, que podem ter consequências e impactos de amplitudes diversas, afetando a coletividade ou grupos de indivíduos, gerando danos de vários tipos, desde o nível individual até em âmbito nacional. Esta realidade se agrava conforme Estados e demais entidades públicas e privadas se tornam profundamente dependentes de ativos digitais que compõem o ciberespaço para o desenvolvimento de suas atividades.

7 O autor menciona que os objetos que estão expostos a perdas causadas pelo risco cibernético incluem: *i)* ativos de informação (por exemplo, dados, software, sistemas operacionais de computador); *ii)* recursos de TIC (por exemplo, hardware, sistemas de telecomunicações, monitoramento de vídeo); e *iii)* ativos tecnológicos (por exemplo, dispositivos controlados eletronicamente, linhas de montagem, sistemas de computadores industriais, sistemas de transporte, fornecimento de energia). Ainda, o risco cibernético pode ocorrer tanto em um único dispositivo de computador separado ou em redes de computadores (Strupczewski, 2021, p. 06).

Em vista da permeabilidade de tais ativos nas diferentes facetas da sociedade, estas atividades podem envolver desde a manutenção de um pequeno negócio familiar, ao controle de redes logísticas de uma empresa, à continuidade de serviços essenciais, como o fornecimento de energia para as cidades de determinado Estado.

Estabelecidos os elementos da cibersegurança, é possível compreendê-la como um fenômeno que poderá receber tratamento diferenciado a depender do setor econômico ou social ao qual pertence o objeto de referência em foco. Como mencionado anteriormente, esses objetos são diversos, e essa variedade pode exigir abordagens específicas, tornando necessárias medidas de segurança técnicas e administrativas mais ou menos robustas, dependendo do nível de risco envolvido. Dessa forma, é viável conceber um ou mais conjuntos padronizados de práticas aplicáveis a todos os objetos de referência, ao mesmo tempo em que determinados grupos demandarão iniciativas próprias para a proteção de seus ativos, considerando riscos específicos ao seu contexto de análise e controle.

Tamanha variedade gera outra consequência importante: a diversidade de atores que serão necessários para promover a cibersegurança. Nessa perspectiva, comunicação, cooperação e coordenação entre esses atores tornam-se essenciais para uma governança eficaz da cibersegurança, conforme será abordado na seção 2.1. Isso ocorre, porque, para cada objeto de referência, haverá um grupo de atores responsáveis pela implementação das iniciativas de cibersegurança, sejam elas padrões gerais ou padrões específicos.

Por essa razão, a arena em que serão desenvolvidas essas ações torna-se um espaço de potenciais disputas de atores, o que exige o desenvolvimento prioritário de um mecanismo de governança capaz de proporcionar uma comunicação ágil, facilitar a cooperação e estruturar uma sólida coordenação. Na prática, essa realidade suscita desafios na forma de fragmentações regulatórias e, por consequência, possíveis duplicações de competência, além da dificuldade de comunicação entre esses atores (Dunn Cavelty; Wenger, 2020).

Uma última observação sobre a definição de cibersegurança diz respeito ao que ela não é. Este trabalho acompanha o arcabouço político-administrativo brasileiro, diferenciando a Cibersegurança de Ciberdefesa no que tange à carga de valores recebidos por determinados objetos de referência. Destaca-se, ainda, que os dois conceitos não são sinônimos, apesar

de apresentarem iniciativas e objetos de referências extremamente similares, porém a partir de perspectivas diferentes.

Considerando a definição de Defesa Cibernética estabelecida pelo Ministério da Defesa, pode-se observar elementos que se sobrepõem às iniciativas e objetos de referência tipicamente considerados como essência da cibersegurança. Esses elementos, porém, são enxergados por outra perspectiva, o que pode implicar na alteração do tratamento de alguns riscos cibernéticos. Esse enquadramento é extraído do conceito de Defesa Cibernética, definida como:

> […] um conjunto de ações ofensivas, defensivas e exploratórias, realizadas no Espaço Cibernético […] com a finalidade de proteger os sistemas de informação de interesse da Defesa Nacional, obter dados para a produção de conhecimento de Inteligência e comprometer os sistemas de informação do oponente (Ministério da Defesa, 2015, p. 85).

O objeto de referência da defesa cibernética diz respeito à Defesa Nacional. Nesse sentido, embora esteja profundamente relacionada, vai além da segurança dos ativos digitais ou das pessoas especificamente – objetos de referência associados à segurança cibernética. No Brasil, a Defesa Nacional é considerada um conjunto de ações e medidas tomadas pelo Estado para proteger os interesses nacionais, a soberania e o território do país contra ameaças externas, potenciais ou óbvias (Ministério da Defesa, 2023).

Assim, pode haver coincidência entre os objetos de referência em cibersegurança e na ciberdefesa. Porém, estes objetos são baseados em valores distintos ou recebem uma dupla carga valorativa. A consequência é que eles serão implementados por atores de naturezas diferentes e por meio de medidas com alcances diversos. A diferenciação crucial é de que a ciberdefesa possibilita ações de natureza ofensiva, enquanto a cibersegurança gera ações de natureza preventiva ou reparadora.

Dependendo da lente utilizada para interpretar os objetos de referência, poderá haver separação ou complementaridade dos atores responsáveis pela implementação das práticas de securitização. Quando os valores estão atrelados à Defesa Nacional, a competência militar se torna predominante, conforme disposto no artigo 142 da Constituição da República Federativa do Brasil (CRFB), na definição de Defesa Cibernética presente no Glossário

das Forças Armadas e na Doutrina Militar de Defesa Cibernética. Somada ao embasamento constitucional, está a compreensão de que a Defesa Cibernética envolve também ações de caráter ofensivo em situações de conflito (Goldoni *et al.*, 2024). Portanto, a ciberdefesa é operada por militares, em razão de competência constitucional. Com isso, utiliza-se, na leitura das medidas e políticas implementadas, também a lente do sistema militar.

Por outro lado, na ausência de valores ligados à Defesa Nacional, excluem-se os atores militares do processo de securitização[8] e atribui-se a outros atores, responsáveis pela garantia da cibersegurança de setores ou objetos de referência específicos, a determinação dessas práticas. Tais atores podem ser públicos ou privados, segmentados ou não por determinado setor. Ilustrativamente, citam-se os atores interessados pelas normas de segurança cibernética específicas dos setores regulados, como aquelas aplicáveis ao setor financeiro, de telecomunicações, de energia, entre outras. Empresas privadas prestadoras de serviços ou órgãos públicos prestadores de serviços, essenciais ou não, também devem ser orientados em relação às práticas de cibersegurança que devem implementar. Nestes casos, é mais fácil seguir padrões gerais, com diferenciação quanto à categorização dos serviços, tamanho da estrutura e outros critérios elegíveis como adequados pelo regulador de cibersegurança.

Existem, entretanto, situações em que os valores e ações da Defesa Nacional convergem com os da cibersegurança (e vice-versa), promovendo uma inevitável hibridização entre segurança e defesa cibernética. Essa confluência ocorre, por exemplo, no caso das infraestruturas críticas. Esses ativos digitais, por sua relevância estratégica para o desenvolvimento do país e pela vulnerabilidade a ciberataques orquestrados por atores externos, frequentemente refletem os valores que constituem ambos os objetos de referência. Nessas situações, torna-se imprescindível estabelecer mecanismos robustos de coordenação para assegurar a atuação harmônica entre os diversos atores envolvidos.

Dessa forma, a cibersegurança e a ciberdefesa podem ser compreendidas como estratégias de securitização voltadas a objetos de referência

8 Isso não significa que os atores não possam atuar em conjunto, desenvolvendo termos de cooperação para atuação conjunta, inclusive para a edição de atos normativos. Tal aspecto é abordado com mais profundidade na seção de 2.1 Governança.

similares ou até comuns por meio de perspectivas complementares. Enquanto a cibersegurança atrai a multiplicidade de atores, envolvendo diferentes esferas sociais, privadas e públicas, a defesa cibernética possui um foco mais circunscrito, abarcando atores militares, que podem fazer recurso a capacidades ofensivas, em coordenação e cooperação com as entidades civis que compõem a segurança cibernética. Trata-se de uma diferenciação política, conceitual e prática, que modelou as instituições e políticas públicas brasileiras direcionadas à securitização cibernética.

Reconhecendo a importância de compreender essa diferenciação, as duas próximas subseções abordarão esse tema. Primeiro, fala-se sobre as distinções entre ciberdefesa e cibersegurança. Em seguida, será apresentado o caso das infraestruturas críticas como exemplo paradigmático em que esses conceitos se entrelaçam, demonstrando a relevância de uma abordagem coordenada entre segurança e defesa.

1.2 O processo de securitização do ciberespaço e a construção da ciberdefesa brasileira

Seguindo a cronologia de implementação política e institucional, a securitização cibernética começou pela defesa cibernética no Brasil. Em consonância com outros países latino-americanos, esse processo de securitização foi estruturado sob a égide militar. Com a virada do século, documentos estratégicos como a Estratégia Nacional de Defesa de 2008 já destacavam a proeminência do ciberespaço para a proteção da nação,[9] elencando-o como uma prioridade estratégica atribuída ao Exército Brasileiro, acompanhando os setores nuclear e espacial, designados à Marinha e à Força Aérea, respectivamente (Brasil, 2008).

9 É interessante pontuar que há correspondência entre os conceitos "ciberespaço" e "ativos digitais". O presente trabalho se refere ao termo "ciberespaço" para tratar de um domínio ou ambiente a ser securitizado, tipicamente sob uma perspectiva militarizada contra ameaças reconduzíveis a oponentes externos, por meio de ações que podem chegar a ser ofensivas, e, portanto, correspondentes à defesa cibernética. Quando a referência for à segurança cibernética, por sua vez, utilizaremos a expressão proteção dos "ativos digitais" de riscos cibernéticos por entidades não militares. Assim, apesar da interposição e transversalidade dos objetos, a terminologia "ciberespaço" será utilizada em referência a um domínio que engloba objetos referentes à defesa cibernética, enquanto "ativos digitais" será referente a objetos de segurança cibernética.

Este desenvolvimento político foi acompanhado e corroborado por incidentes internacionais de ampla repercussão, que angariaram a necessidade de atenção à temática. Como exemplos, podemos citar os ataques atribuídos à Rússia contra Estônia e Geórgia em 2007 e 2008 (Greenberg, 2019).[10] Somado a estas ocorrências, houve também o caso Stuxnet, considerado uma operação conjunta de agências israelenses e estadunidenses em 2010 e direcionado a minar o desenvolvimento de supostas armas nucleares iranianas.[11]

Tais eventos confirmaram preocupações latentes quanto à possível exploração de vulnerabilidades e de tecnologias digitais para atingir alvos nacionais (Devanny; Goldoni; Medeiros, 2022; Goldoni *et al.*, 2024). Estes incidentes trouxeram à tona o tema da defesa cibernética e exemplificaram como o ciberespaço poderia ser operacionalizado de acordo com interesses internacionais (Lindsay, 2013). Assim, a elevação da urgência da securitização do ciberespaço desencadeou uma série de desenvolvimentos político-administrativos que se desdobraram de forma prática na elaboração de novas políticas públicas e modernização de instituições direcionadas à proteção de ativos digitais em vários países (Dunn Cavelty; Wenger, 2020; Fischer, 2015; Medeiros, 2024; Urbanovics, 2022).

No caso brasileiro, foram as revelações de Edward Snowden, em 2013, que consolidaram a percepção de ameaças perpetráveis por meio de tecnologias digitais e da consequente necessidade de se considerar o ciberespaço como um domínio essencial para a defesa nacional (Belli, 2021a; Goldo-

10 No caso da Estônia, ao longo do ano de 2007, os sites do governo estoniano, de bancos e de jornais foram alvos de vandalismo digital e ataques de negação de serviço (DDoS), repetidamente interrompendo o acesso à internet, que foi particularmente prejudicial devido à grande dependência da Estônia do ciberespaço. O caso da Geórgia, por sua vez, é tido como um caso até então inédito de coordenação e integração de meios cibernéticos e militares que causaram interrupções nas comunicações seguidas de incursões terrestres e aéreas (Connel; Vogler, 2017).

11 O caso Stuxnet foi emblemático do uso de meios cibernéticos para afetar infraestruturas críticas. Notório pela sua complexidade, sofisticação e precisão. O caso também é identificado como a primeira instância de meios cibernéticos causando danos físicos em uma suposta disputa entre Estados. O *malware* Stuxnet infectou sistemas, monitorou operações e depois sabotou o enriquecimento de urânio na usina nuclear de Natanz no Irã. Uma vez que contaminou os sistemas controladores da usina, o *malware* alterava as velocidades das centrífugas, acelerando-as e depois freando-as para causar falhas. Ao mesmo tempo, fornecia feedback falso aos técnicos, ocultando os danos e prolongando a sabotagem. Estima-se que cerca de 20% das centrífugas iranianas foram danificadas entre 2009 e 2010 (Sanger, 2012).

ni *et al.*, 2024). Na ocasião, evidenciaram-se práticas de espionagem global coordenadas pela *National Security Agency* estadunidense (NSA), que teve como alvos diretos o alto escalão do governo brasileiro, incluindo a então presidente Dilma Rousseff, funcionários da Petrobrás, entre outros (Greenwald; MacAskill, 2013).

Durante o ocorrido, Celso Amorim, Ministro da Defesa à época, destacou como as linhas entre a espionagem global e a guerra cibernética estavam se mesclando diante da frequência com que os instrumentos de alta tecnologia eram direcionados contra a soberania do Brasil e de demais países no mundo (Amorim, 2013). Estes incidentes levaram ao reconhecimento de riscos direcionados às infraestruturas críticas brasileiras, que por sua vez passaram a ser securitizadas por atores do setor público, dentre eles os militares.

A falta de clareza acerca de regras e limites às atividades ofensivas no ciberespaço, aferida por Celso Amorim, é emblemática das percepções estatais acerca do processo de securitização no ciberespaço. Por se tratar de um domínio com características diferentes de outros domínios tradicionais, ao passo que o ciberespaço é composto por uma camada física de hardware e complementada por uma camada virtual de software potencialmente acessível globalmente, as noções clássicas de território, jurisdição e legitimidade dos atores são desafiadas (Belli, 2016; Belli *et al.*, 2023b; Medeiros; Goldoni, 2020).

Essa realidade, transposta para um cenário competitivo interestatal, impele processos de mudança e modernização a serem promovidos por diferentes Estados (Medeiros, 2024). Neste contexto, os Estados buscam adaptar seus arcabouços político-institucionais mediante práticas de securitização, alicerçadas em percepções de ameaça referentes ao ambiente competitivo em que estão inseridos – seja este ambiente no nível político, na economia ou no campo militar (Pfaff, 2020).

O processo de securitização preconizado pela escola de Copenhague estabelece que quando os Estados percebem ameaças, iniciam – ou intensificam – narrativas que priorizam determinados objetos a serem protegidos (Dunn Cavelty; Wenger, 2020). Como mencionado, no caso brasileiro, esse processo de securitização se inicia em 2008 com a consideração do ciberespaço como setor estratégico, seguido por sua priorização em decorrência das revelações de Snowden, em 2013.

A mudança na percepção de ameaças foi acompanhada por uma necessidade prática do Brasil atrelada à recepção de megaeventos globais, incluindo o Rio +20 em 2012, a Copa do Mundo de futebol de 2014 e as Olimpíadas de 2016, que representam alvos preferenciais para ciberataques em escala (Goldoni *et al.*, 2024).

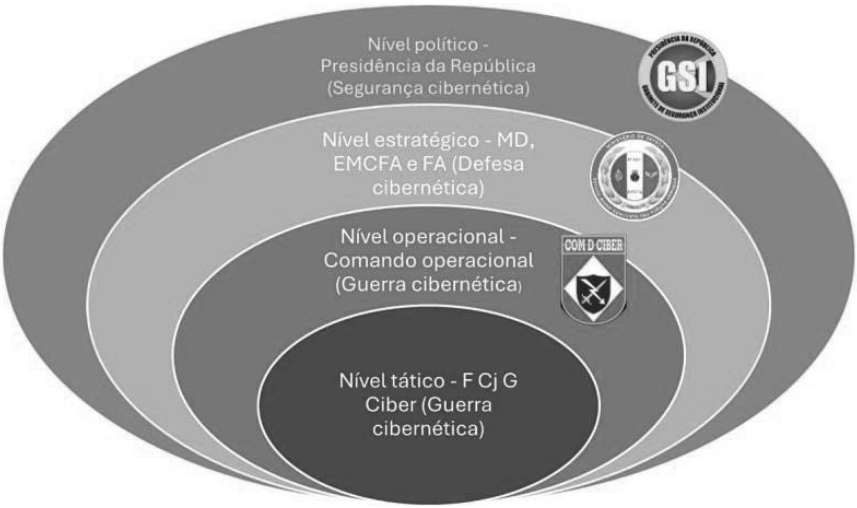
A mudança na percepção de ameaças decorrente dos incidentes cibernéticos supracitados, somada às demandas práticas dos grandes eventos, evidenciou a necessidade de proteção de certos objetos de referência sob o manto de valores da Defesa Nacional; efetivamente contribuindo para a militarização da defesa cibernética ao longo dos anos 2010.

Durante este período e acompanhando os grandes eventos, o Exército Brasileiro participou dos esforços de proteção das telecomunicações através do Centro de Defesa Cibernético (CDCiber), que teve suas capacidades priorizadas na Estratégia Nacional de Defesa de 2012. Subsequentemente, em 2016 foi criado o Comando de Defesa Cibernética (ComDCiber), um comando conjunto, chefiado pelo Exército Brasileiro e integrado por membros da Marinha, Aeronáutica e do Exército. Atualmente, o ComDCiber atua no nível estratégico da defesa cibernética, tendo o CDCiber como seu braço operacional (Devanny; Goldoni; Medeiros, 2022; Goldoni *et al.*, 2024; Ministério da Defesa, 2023).

Em consonância com desenvolvimentos de políticas públicas recentes como as edições de 2020 e 2025 da Estratégia Nacional de Cibersegurança, assim como a publicação da Política Nacional de Cibersegurança de 2023; há uma separação institucional-administrativa entre a defesa cibernética, atribuída ao ComDCiber e a segurança cibernética atribuída ao Gabinete de Segurança Institucional (Devanny; Goldoni; Medeiros, 2022; Goldoni *et al.*, 2024).

Assim, sob uma perspectiva doutrinária, a coordenação da segurança cibernética compete, no nível político, ao Gabinete de Segurança Institucional (GSI), órgão responsável por assessorar à Presidência da República em assuntos de segurança, enquanto a defesa cibernética continua como atribuição do Ministério da Defesa por meio do Estado Maior Conjunto das Forças Armadas (EMCFA) e os Comandos das Forças Armadas (FA), no nível estratégico. Como se demonstra na Figura 1.

Figura 1 - Níveis de decisão e atores no espaço cibernético



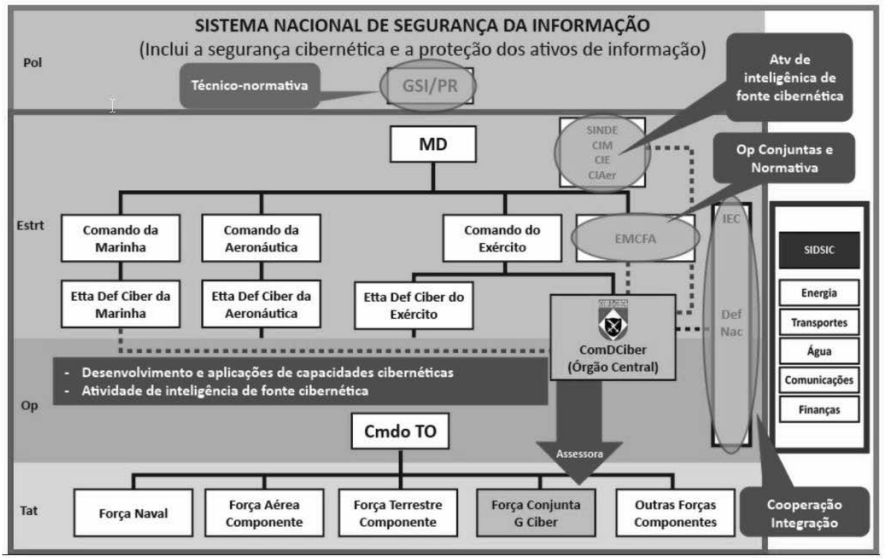
Fonte: Adaptado de Doutrina Militar de Defesa Cibernética (Ministério da Defesa, 2023, p. 15).

Esta separação entre os encargos de competência militar e do GSI se deve a fatores estratégicos e práticos. De forma prática, o escopo expansivo dos incidentes cibernéticos, que afetam áreas além da ciberdefesa, evidenciou a necessidade de uma abordagem mais ampla, também capaz de ir além da ciberdefesa, mas mantendo uma relação colaborativa com ela. Essa colaboração entre os mecanismos de governança da ciberdefesa e da cibersegurança é crucial, devido à inserção de uma pluralidade de ativos digitais no ciberespaço, fato que demanda a participação simultânea – e, idealmente, coordenada – de múltiplos atores da segurança e da defesa cibernética. O caso das infraestruturas críticas, que será analisado na próxima subseção, evidencia essa necessidade.

Em vista da expansão da percepção de ameaças para além de questões de defesa cibernética, a consolidação do inter-relacionamento dos órgãos de cibersegurança e defesa cibernética, inclusive a cooperação com atores civis responsáveis pela cibersegurança de infraestruturas críticas, foi estruturada no Sistema Militar de Defesa Cibernética (SMDC), com objetivo de proporcionar a interoperabilidade sistêmica entre órgãos militares e civis.

Assim, o ComDCiber, órgão que tem a competência de assessorar o Ministro da Defesa (MD) na implementação e gestão do SMDC, conta com a participação de militares das Forças Armadas e civis. No nível estratégico, o ComDCiber, sob a supervisão do MD, coordena e integra o Setor Cibernético das Forças Armadas, com foco na atuação conjunta. Essa interoperabilidade sistêmica ocorre mediante a manutenção de canais técnicos e de coordenação com órgãos civis com competência para segurança cibernética, como CERT.br, CTIR Gov e agências governamentais, como ilustrado na figura a seguir.

Figura 2 - Sistema militar de defesa cibernética (SMDC)



Fonte: Reproduzido de Doutrina Militar de Defesa Cibernética (Ministério da Defesa, 2023, p. 29)[12].

Não obstante a separação doutrinária entre segurança e defesa cibernéticas, sob uma perspectiva holística, ao passo que a segurança nacional

12 Considerando o exposto na seção anterior, é importante destacar que, em conformidade com a Doutrina de Defesa Cibernética, é na proteção cibernética das infraestruturas críticas de interesse da Defesa Nacional que o Sistema Militar de Defesa Cibernética colabora com a segurança cibernética, mediante de cooperação e integração entre militares e civis (Ministério da Defesa, 2023).

pode ser comprometida por falhas na segurança cibernética, é essencial que haja um esforço conjunto de prevenção e resposta entre os atores responsáveis pela cibersegurança e pela ciberdefesa. Nesse sentido, embora a cibersegurança componha uma área predominantemente civil, tendo como objeto de referência ativos digitais e pessoas, quando vulnerabilidades e incidentes são percebidos como ameaças à segurança nacional, a defesa cibernética assume um papel essencial, condizente com seu foco na proteção do país contra ameaças ao nível nacional, inclusive por meio de capacidade ofensiva. Assim, a ciberdefesa tem como objeto de referência a segurança nacional e, tal como ocorre nos outros domínios, os atores securitários são tradicionalmente militares.

Essa interdependência entre segurança e defesa cibernética é particularmente evidente no âmbito das infraestruturas críticas, foco da próxima seção, que englobam ativos digitais passíveis de exploração que, se comprometidos, podem afetar diretamente a segurança do país. Dessa forma, essas infraestruturas se tornam simultaneamente um objeto de interesse tanto da cibersegurança, voltada para a proteção de ativos e pessoas, quanto da defesa cibernética, orientada para a salvaguarda da segurança nacional.

1.3 A análise do caso das infraestruturas críticas digitais e serviços essenciais digitais: multiplicidade de atores e complexidade no tratamento de cibersegurança

Tradicionalmente, o conceito de infraestrutura é entendido como um conjunto de elementos estruturais de grande relevância para sustentar o desenvolvimento eficiente de um país ou organização, abrangendo áreas como educação, saneamento, transporte, energia e telecomunicações, entre outras (INFRASTRUCTURE, 2024). A digitalização dessas infraestruturas serve de pilar essencial para o desenvolvimento das economias e sociedades modernas.

A segurança de tais infraestruturas, na sua dimensão tanto física quanto digital, é essencial. No contexto brasileiro, o Decreto Federal nº 9.573/2018, que instituiu a Política Nacional de Segurança de Infraestruturas Críticas (PNSIC), reconhece a existência de setores que possuem di-

mensão estratégica para o país por representarem um papel fundamental para a soberania nacional e o desenvolvimento econômico. O funcionamento inadequado dessas infraestruturas pode acarretar sérios transtornos à sociedade, à economia e, eventualmente, à democracia.

É neste sentido que o bom funcionamento de tais infraestruturas desempenha uma função crítica para o país. Neste estudo, adota-se a definição de infraestruturas críticas (ICs) fornecida pela PNSIC, que as caracteriza 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" (Presidência da República, 2018a).[13]

É relevante destacar que o Brasil dispõe de um arcabouço normativo para o tratamento das infraestruturas críticas. O Decreto nº 9.573/2018, que aprovou a Política Nacional de Segurança de Infraestruturas Críticas (PNSIC), representou um marco ao estabelecer a segurança dessas infraestruturas como uma atividade de Estado. Complementando esse marco, a Estratégia Nacional de Segurança de Infraestruturas Críticas (ENSIC), aprovada pelo Decreto nº 10.569, de 9 de dezembro de 2020, ainda em vigor, delineou eixos estruturantes e objetivos estratégicos, fornecendo um direcionamento abrangente para ações governamentais e intersetoriais.

Além disso, o Plano Nacional de Segurança de Infraestruturas Críticas (PLANSIC), instituído pelo Decreto nº 11.200, de 15 de setembro de 2022, foi concebido como um instrumento de planejamento institucional destinado a coordenar e articular iniciativas de diversos órgãos e entidades envolvidos na proteção dessas infraestruturas.

Destaca-se que a PLANSIC se refere a uma abordagem propositalmente generalista para a segurança das ICs. Isso se deve à amplitude de vulnerabilidades e riscos a que as ICs estão sujeitas, desde sabotagem e erro humano até desastres naturais; somada ao incentivo a uma resposta sinérgica por parte dos diferentes atores, no caso de incidentes. Nesse sentido, a PLANSIC define áreas prioritárias compostas por planos setoriais

13 Considerando o exposto na seção anterior, é importante destacar que, em conformidade com a Doutrina de Defesa Cibernética, é na proteção cibernética das infraestruturas críticas de interesse da Defesa Nacional que o Sistema Militar de Defesa Cibernética colabora com a segurança cibernética, mediante de cooperação e integração entre militares e civis (Ministério da Defesa, 2023).

de segurança de infraestruturas críticas, atribuídos a ministérios próprios (Presidência da República, 2022b).

Trata-se, portanto, de uma resposta ministerial à prevenção e resposta a incidentes em ICS. Em consonância com esta abordagem, o Governo Federal instituiu o Comitê Nacional de Segurança de Infraestruturas Críticas (CNSIC), por meio da Portaria Interministerial GSIPR/MAPA/MCID/MCTI/MD/MF/MGI/MIDR/MJSP/MS nº 4/2024.

O CNSIC tem como função monitorar a implementação e a evolução da PNSIC, assegurando supervisão contínua e avaliação sistemática das políticas e ações relacionadas à segurança de infraestruturas críticas. Sua atuação reforça o alinhamento estratégico e a eficácia dessas políticas, complementando o acompanhamento já realizado pelo Gabinete de Segurança Institucional (GSI).

Uma questão relevante que se destaca é a distinção entre o objeto do arcabouço normativo mencionado, que trata das infraestruturas críticas no âmbito do PNSIC, e o tratamento que essas infraestruturas poderão receber no contexto da cibersegurança. Neste último campo, as infraestruturas críticas são compreendidas como conjuntos de ativos digitais, abrangendo sistemas de *software* e de hardware e as informações armazenadas nesses sistemas, que suportam o funcionamento de uma ampla gama de produtos e serviços digitais essenciais para o desenvolvimento do país. Esses ativos requerem proteção devido à sua exposição a riscos digitais que, quando se concretizarem, podem gerar impactos significativos nas esferas social, ambiental, econômica, política, internacional e na segurança do Estado e da sociedade.

Uma solução seria conferir a proteção do PNSIC (e as decorrentes ENSIC e PLANSIC), principalmente, à segurança física das "instalações, serviços, bens e sistemas" identificados pela PNSIC, enquanto o enfoque da cibersegurança, no que diz respeito às infraestruturas críticas (ICs), estaria voltado aos ativos digitais que podem apoiar a automatização e digitalização dos objetos do PNSIC, com o intuito de prever, mitigar e conter ameaças cibernéticas a eles associadas.

É importante frisar que a noção de IC sob a lente da cibersegurança deve englobar também os serviços essenciais que se utilizam de sistemas digitais – para armazenar e processar informações – cuja operação ininterrupta é essencial para a segurança e o funcionamento do Estado e da so-

ciedade. Além de o próprio decreto da PNSIC mencionar os serviços (e não só instalações) ao se referir à infraestrutura crítica, cabe enfatizar que há um grupo de "serviços ou atividades essenciais" que a própria Constituição Federal considera ininterruptos para garantir "necessidades inadiáveis da comunidade" (artigo 9º, § 1º, da CRFB).

Se esses serviços, definidos pela Lei 7.783/89, são entendidos como inadiáveis para a sociedade, sua manutenção e continuidade também devem ser consideradas como críticas, de modo que constituam objeto de referência quando digitalizados. Esse entendimento, inclusive, está em conformidade com o disposto no artigo 2º, III, do Decreto que instituiu a PNCiber.

Desse modo, os serviços essenciais correspondem ao tratamento e abastecimento de água; produção e distribuição de energia elétrica, gás e combustíveis; assistência médica e hospitalar; distribuição e comercialização de medicamentos e alimentos; serviços funerários; transporte coletivo; captação e tratamento de esgoto e lixo; telecomunicações; guarda, uso e controle de substâncias radioativas, equipamentos e materiais nucleares; e processamento de dados ligados a serviços essenciais (BRASIL, 1989). Estes serviços também devem ser considerados objetos de referência em cibersegurança para a aplicação de iniciativas voltadas à promoção de segurança em face dos riscos cibernéticos.

Entende-se que esse rol não deve ser considerado taxativo, mas apenas um rol mínimo de atividades que, por lei, já foram consideradas essenciais. Outras atividades, entretanto, podem ser assim consideradas. Por exemplo, não é desarrazoado pensar que aplicativos de mensageria privada com elevado número de usuários sejam considerados como serviços essenciais, devido à função crucial que desempenham. Considerando a natureza evolutiva desses serviços, a regulação em cibersegurança deve se adaptar para abarcar e identificar os tipos de serviços que devem fazer parte desse rol.

Nesse sentido, é relevante destacar que a nova Estratégia Nacional de Cibersegurança (E-Ciber/2025) estabeleceu como eixo temático tanto a resiliência em infraestruturas críticas como os serviços essenciais, motivo pelo qual se entende que o documento está alinhado ao anteriormente mencionado.

Feita a introdução sobre o conceito de infraestruturas críticas e serviços essenciais, passa-se à análise do caso da hibridização da cibersegurança e ciberdefesa, analisando a multiplicidade de atores que podem ter competência para prevenir e eventualmente responder aos riscos cibernéticos nesses ativos digitais.

1.3.1 Multiplicidade de atores responsáveis para a securitização das infraestruturas críticas e serviços essenciais

Consoante o exposto na seção anterior, as ICs poderão sofrer uma hibridização no seu tratamento, isto é, além da incidência de arcabouço das iniciativas de cibersegurança com o gerenciamento feito por seus respectivos atores, elas podem ter a incidência de eventuais ações específicas provenientes da ciberdefesa.

Tal coincidência de processos securitizadores impõe não apenas estratégias e controles de segurança díspares, mas também gerência de atores governamentais, militares e privados, que podem cooperar ou, eventualmente, competir entre si (Dunn Cavelty; Wenger, 2020; Hansen; Nissenbaum, 2009), e cuja comunicação, coordenação e cooperação precisam ser facilitadas no âmbito de um eventual Sistema Nacional de Cibersegurança[14] para que a cibersegurança das ICs seja garantida de forma efetiva e eficiente.

Para ilustrar este ponto, considere a existência de vulnerabilidades nos servidores de uma usina hidrelétrica. Essas vulnerabilidades se relacionam à cibersegurança de uma prestadora de serviço regulado (a de fornecimento de energia elétrica) que podem viabilizar a invasão dos sistemas e, porventura, a sabotagem desta usina por um ator externo, ocasionando a interrupção do fornecimento de energia a uma determinada parte do país. Neste caso, trata-se de uma questão de interesse nacional, competindo à Agência Nacional de Energia Elétrica (ANEEL) e à defesa cibernética, de acordo com o arcabouço político-administrativo vigente no Brasil.

14 O objetivo de tal sistema ou rede multissetorial seria de congregar todos os atores técnicos e regulatórios responsáveis para manter a cibersegurança nacional (BELLI et al, 2023). O papel desse sistema será analisado na conclusão deste trabalho.

Nesse contexto, caso requisitado, o ComDCiber poderia atuar na restauração e eventual resposta a esse incidente, juntamente com os CSIRTs setoriais privados e, eventualmente, o CTIR Gov. Se esse ataque, por exemplo, também resultasse no vazamento de dados pessoais, acrescer-se-ia um novo ativo digital para ser protegido, os dados pessoais, o que atrairia também a competência da Autoridade Nacional de Proteção de Dados (ANPD).

Esta cooperação e integração constituem, de fato, a hibridização entre ciberdefesa e cibersegurança mencionada anteriormente, a qual ocorre de forma prática no âmbito da resposta a incidentes.[15] Como frisado, dentro do escopo da cibersegurança há uma variedade de objetos de referência, dentre os quais existem ativos digitais que também podem ser classificados como infraestruturas críticas. Para cada objeto de referência, podem existir atores responsáveis, com competências previamente determinadas para sua segurança, e que podem possuir regulações próprias.

Além da setorização dos objetos de referência da segurança cibernética, cabe ressaltar também a distinção entre as competências regulatórias e operacionais desses setores. Contribuindo para a complexidade do contexto político-administrativo da cibersegurança, as competências regulatórias da cibersegurança, associadas a diversos órgãos ou entidades reguladoras, distinguem-se das competências operacionais, comumente atribuídas a Grupos de Segurança e Resposta a Incidentes[16] (CSIRTs). Esses grupos desempenham uma função essencial, atuando na linha de frente contra ameaças cibernéticas, e podem pertencer tanto a entes privados quanto públicos, inclusive a entidades multissetoriais.

---

15 Neste sentido, o ComDCiber "representa a Defesa na articulação com o Centro de Prevenção, Tratamento e Resposta a Incidentes Cibernéticos de Governo, como equipe de coordenação setorial". Contudo, no nível estratégico, a doutrina observa a "mudança do viés exclusivo de segurança cibernética para a defesa cibernética". Não obstante a intercessão com a segurança cibernética, a doutrina enfatiza que "[e]mbora medidas de segurança sejam implementadas em todos os níveis, a defesa implica que, além da proteção, a exploração e o ataque são executados neste nível, em cumprimento às demandas das autoridades competentes". Nesse sentido, embora ocorra grande transversalidade e hibridização entre os objetos e agentes securitários, doutrina e constitucionalmente, o fator que diferencia a defesa cibernética, é o emprego de ações ofensivas e de exploração além das medidas securitárias correspondentes a segurança cibernética (Goldoni *et al*., 2024; Ministério da Defesa, 2023, p. 27–28).

16 As características destas entidades e seu papel fundamental no âmbito da governança da cibersegurança serão exploradas na seção 2.1.4.

A competência dos CSIRTs, portanto, é diferente da competência regulatória, que recai sobre órgãos ou entidades, que, além de possuírem CSIRTs próprios, responsáveis por centralizar a notificação de incidentes setoriais, também atuam na liderança e coordenação dos padrões e iniciativas setoriais de cibersegurança.

Assim, observa-se que os atores com competência regulatória, na maioria dos casos, não são responsáveis pela operacionalização/implementação da cibersegurança. Isto é, existem equipes de prevenção, tratamento e resposta a incidentes cibernéticos[17] de origem pública ou privada, que não necessariamente pertencem à estrutura interna do órgão regulador de um respectivo setor.

Para coordenar essas equipes, o Decreto nº 10.748 de 2021 (assim como a Norma Complementar nº 05 /IN01/DSIC/GSIPR, de 14/ago/09) criou a Rede Federal de Gestão de Incidentes Cibernéticos (ReGIC), responsável por coordenar os órgãos e as entidades da administração pública federal no nível operacional.

Nesse sentido, é possível observar a complexidade e a consequente fragmentariedade, bem como eventual sobreposição institucional na governança regulatória e operacional da normativa da cibersegurança (BELLI *et al.* 2023). O Quadro 1 exemplifica isso de forma não exaustiva.

17 Embora variem conforme seu de seu foco, finalidade, origem, escopo e composição estas equipes são comumente referidas como *Computer Security Incident Response Teams* (CSIRTs) ou como *Computer Emergency Response Team* (CERTs).

Quadro 1 – Regulação setorial e atores responsáveis pela operacionalização

Setor	Regulação setorial	Ator responsável pela regulação	CERT responsável pela implementação da cibersegurança em caso de ameaça incidente
Financeiro	Resolução CMN nº 4.893/2021	Banco Central do Brasil BCB	CSIRT BB, CSIRT CAIXA, CSIRT PAGSEGURO, CSIRT Santander, CSIRT SICREDI
Mercado de valores mobiliários	Instrução da CVM nº 35/2021, com as alterações introduzidas pelas resoluções CVM nºs 134/22 e 179/23	Comissão de Valores Mobiliários CVM	*Não Identificado Não se aplica*
Telecomunicações	Resolução nº 740/2020 ANATEL com as alterações propostas pela Resolução nº 767 - 07/08/2024	ANATEL	CSIRT Telefônica, CSIRT TIM, CSIRT TVIT, CSIRT Globo, CSIRT Locaweb, CSIRT UOL
Energia	Resolução nº 964/2021, ANEEL	ANEEL	CSIRT Cemig, CSIRT Petrobras
Acadêmico	*Não Identificado Não se aplica*	*Não Identificado Não se aplica*	CAIS/RNP, CEO/RedeRio, CERT Bahia, CERT-RS, CSIRT Unicamp
Governamental	Decreto nº 10.748/2021	GSI	CTIR.Gov, CCTIR/EB, CLRI-TRF3, CSIRT PRODESP

Fonte: Elaboração própria.

Nota: As informações têm como base as informações disponíveis em: Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil (CERT.br). CSIRTs. **Informações de Contato de CSIRTs Brasileiros**. Disponível em: https://www.cert.br/csirts/brasil/. Acesso em: 21 ago. 2025.

A descrição ilustra a complexidade inerente ao campo da cibersegurança e evidencia a necessidade de investir em ações que promovam a coordenação e a cooperação entre os diversos atores envolvidos de forma sistêmica. A integração de esforços entre esses setores é essencial para enfrentar os desafios crescentes nesse domínio, principalmente no caso das ICs, em que a comunicação, coordenação e comunicação multissetorial são imprescindíveis.

Nesse sentido, o Brasil já apresenta iniciativas que exemplificam a eficácia de abordagens colaborativas e multissetoriais. Dentre elas, o exercício do Guardião Cibernético, realizado anualmente sob a coordenação do Comando de Defesa Cibernética, é um exemplo. Essa ação reúne militares e representantes civis de setores estratégicos, abarcando de CERTS a agências reguladoras para facilitar a comunicação e treinar, de forma conjunta, a resposta e mitigação de incidentes cibernéticos simulados direcionados contra infraestruturas críticas e outros alvos de relevância nacional (Barreto, 2022).

Essa prática retrata o arcabouço político-administrativo descrito até então e tem como efeito não apenas fortalecer a capacidade de resposta em situações de crise, mas também fomentar a construção de um ambiente de colaboração e troca de conhecimentos entre as esferas civil e militar, consolidando um modelo de governança integrada no campo da cibersegurança.

Observando esse cenário, é preciso chamar atenção para o caso das infraestruturas críticas relacionadas à higidez dos processos democráticos. Nesse contexto, a comunicação em massa realizada pelas plataformas digitais, principalmente quando voltada para questões eleitorais, também poderia ser tratada como um objeto de referência da cibersegurança.

Particularmente, há vários anos se considera a desinformação, entendida como a difusão voluntária de conteúdos falsos ou enganosos, como uma técnica de guerra cibernética e, portanto, uma ciberameaça capaz de afetar diretamente o funcionamento da sociedade e capaz de prejudicar o efetivo exercício da soberania de um país (Belli *et al.*, 2023b; Belli; Curzi; Britto Gaspar, 2023; Devanny; Buchan, 2023; ENISA, 2022b; Solar, 2020).

A inclusão de infraestruturas críticas digitais relacionadas à democracia como objetos de securitização apresenta desafios particularmente complexos. A próxima subseção examinará os riscos associados a essa abordagem, com ênfase nas controvérsias decorrentes da consideração da desinformação como uma questão de cibersegurança e segurança nacional. Tal análise é indispensável, considerando que a desinformação e o tratamento da

cibersegurança têm sido crescentemente posicionados como temas centrais no âmbito da segurança nacional (Devanny; Buchan, 2023; Solar, 2020).

A inserção da cibersegurança no processo de securitização requer que os atores responsáveis tomem medidas urgentes para proteger objetos de referência específicos, pautando-se, muitas vezes, por suas próprias concepções políticas e normativas. Como discutido anteriormente, a categorização de ativos digitais como infraestruturas críticas não apenas amplia a responsabilidade de órgãos reguladores setoriais, mas também potencialmente autoriza a intervenção de atores militares, que pode levar a consequências particularmente sensíveis.

Neste sentido, qualquer movimento em direção à securitização de infraestruturas democráticas digitais deve ser conduzido com extremo cuidado e transparência, de forma a preservar os princípios fundamentais de uma sociedade democrática e evitar excessos que possam comprometer direitos fundamentais.

1.4 A segurança das infraestruturas críticas democráticas digitais

Impulsionando as áreas relacionadas ao desenvolvimento tecnológico, a digitalização abriu portas para novos tipos de ataques que podem afetar não só o funcionamento de um país, mas interferir diretamente no seu regime político, tanto por atores externos quanto internos (Belli *et al.*, 2023; ENISA, 2022; ENISA, 2023).

A título de exemplo, podem ser mencionadas novas formas de financiamento para campanhas de desinformação de cunho político, ameaças de ciberataques a sites de instituições com o objetivo de minar seu funcionamento em épocas eleitorais ou de ferir a credibilidade de governos ou candidatos, além da disseminação de desinformação contra entidades associadas a determinados partidos políticos para fomentar polarização nas redes sociais, entre outros tipos de ataques.

Um caso emblemático é a invasão dos servidores do Partido Democrata dos Estados Unidos (EUA), atribuída a grupos de hackers associados à Rússia, com o intuito de influenciar as eleições presidenciais norte-americanas de 2016. Outro exemplo é o monitoramento e direcionamento de

conteúdo para eleitores em disputas presidenciais e plebiscitos ao redor do mundo, como no caso do Brexit, revelado pelo escândalo da Cambridge Analytica em 2018 (Cadwalladr *et al*., 2018).

A existência de um regime democrático íntegro pressupõe um ambiente livre para a circulação de ideias, com respeito à liberdade de expressão e outros direitos fundamentais. O estabelecimento de democracias não faz presumir a sua permanência, ou seja, não significa que ela não possa ser vulnerável a vários tipos de ataque, inclusive de tipo cibernético, e que, portanto, não precisa de proteção. Tal como ilustrado pelo caso norte-americano em 2016 e afirmado pela Comissão do Parlamento Europeu em seu plano de ação para a democracia europeia (European Commission, 2020, p. 01), "a democracia não é algo que pode ser dado como certo: é necessário defendê-la e promovê-la ativamente".

É nesse sentido que se considera que a dimensão de infraestruturas críticas possa abarcar também a proteção às infraestruturas digitais necessárias à manutenção da democracia brasileira. Isto é, é preciso conferir segurança, no âmbito digital, aos serviços, sistemas, bens ou instalações que possam afetar o regime político da democracia (Belli *et al*., 2023b).

Assim, seria possível considerar como infraestrutura crítica digital democrática os sistemas de comunicação digitais exemplificados nas plataformas digitais de redes sociais. Contudo, os discursos securitários de infraestruturas democráticas no ciberespaço são embasados em ocorrências e tendências recentes e as estratégias mais eficientes para lidar com tais riscos são ainda pouco sedimentadas.

No caso específico do Brasil, o aumento da utilização da Internet, a partir da década de 2010, e a utilização principalmente de redes sociais – fenômeno exacerbado pelas práticas de patrocínio de aplicativos ou *zero rating*, cujos principais beneficiários são os aplicativos do grupo Meta (Belli *et al*., 2018; Instituto Locomotiva, 2021) – alteraram a forma de comunicação dos brasileiros.

As redes sociais assumiram papel central, passando a ser não somente o principal instrumento utilizado para se comunicar com amigos e familiares e obter informações a respeito de diversos assuntos, mas também o canal mais popular para comunicação e propaganda política. Como ponto positivo, pode-se mencionar que o debate público se tornou mais inclusivo e participativo, mas, por outro lado, modificou-se a forma como as pessoas

se interessam, acessam e recebem a informação, o que trouxe efeitos colaterais, como desinformação e polarização (Couto, 2022).

O advento das redes sociais possibilita uma ruptura no fluxo e consumo de informações por parte da população, de forma que não só os editoriais trazem a informação a ser consumida, mas também os próprios usuários compartilham notícias online (Couto, 2022). A popularidade e inserção da população nas redes sociais – produzindo e propagando informação – possibilitam a alteração dos papéis do produtor e da audiência, antes previamente fixados, tornando o cenário mais híbrido, descentralizado e vulnerável a potenciais ataques coordenados.

O modelo de plataformas digitais baseadas em conteúdos criados por usuários (redes sociais) e divulgado com base em critérios algorítmicos e econômicos passíveis manipulação e/ou exploração diminui a relevância da criação de notícias de qualidade por veículos profissionais de comunicação, atribuídos a mídia tradicional, fazendo com que os conteúdos oriundos desses veículos compitam por visualizações de conteúdos potencialmente enganosos criados por seus usuários (Cruz *et al.*, 2019).

Esse fenômeno enfraquece os mecanismos de checagem de informações promovidos pelo jornalismo profissional, deixando que a informação seja veiculada sem contar, necessariamente, com padrões de conduta de objetividade e veracidade. Ao mesmo tempo, o modelo de negócios desenvolvido pelas plataformas de redes sociais utiliza os conteúdos compartilhados como veículos para distribuir a publicidade de terceiros (Couto, 2022; Dias *et al.*, 2023; Hartman *et al.*, 2023).

Neste contexto, a recomendação algorítmica com fins lucrativos é o cerne do modelo de negócios das plataformas digitais. Frequentemente, essas plataformas priorizam recomendações que maximizam o engajamento dos usuários, sem avaliar o conteúdo promovido. Esse modelo é explorável e explorado por atores de má-fé para coordenar campanhas de desinformação. Assim, a possibilidade de disseminar conteúdos falsos e discurso de ódio, que podem ser prejudiciais ao interesse público e influenciar indevidamente processos eleitorais, torna-se uma vulnerabilidade da infraestrutura (Couto, 2022).

O papel preponderante de redes sociais e, cada vez mais, de sistemas de inteligência artificial (IA) no âmbito de campanhas eleitorais e processos democráticos traz problemas sistêmicos, como desinformação, propagação de discurso de ódio, assédio, atos extremistas, racismo, dentre

outros. Particularmente, é possível observar ações humanas, muitas vezes coordenadas, para a produção e disseminação de informações falsas, organização de atos de violência, ataques às instituições de um país com o fim de fragilizar a democracia e a credibilidade das instituições políticas (Caramancion *et al*., 2022; Piccone, 2018; Rid; Buchanan, 2018).

Tais atos podem ser considerados ameaças e demandar intervenção para garantir a segurança sobre diferentes objetos de referência que abrangem desde o indivíduo até a segurança nacional. Como ilustrado anteriormente, os atores responsáveis pela securitização irão variar conforme a percepção de ameaças aos respectivos objetos.

Essa dinâmica foi observada nas eleições brasileiras de 2018 e 2022, que também testemunharam a intensificação dos novos formatos de campanha digital no país e o crescente número de casos de desinformação, em decorrência da difusão de sistemas de IA capazes de criar falsificações realistas de áudio e vídeo, conhecidas como "*deepfakes*" (Chesney; Citron, 2018). Essas tecnologias podem ser usadas em uma miríade de práticas, incluindo ataques de engenharia social para manipular indivíduos a divulgar informações sensíveis ou autorizar transações fraudulentas.

Neste contexto, a difusão da IA implica um acesso muito maior e mais fácil a sistemas altamente sofisticados que, até alguns anos atrás, eram acessíveis apenas a especialistas. Isso facilita a criação e difusão de mídias sintéticas altamente convincentes, que podem ser usadas para orquestrar campanhas de desinformação com fins financeiros e políticos. Essas tecnologias representam uma nova ameaça à cibersegurança dos processos democráticos, permitindo que atores maliciosos manipulem informações em uma escala e complexidade sem precedentes (Belli, 2024a).

As eleições presidenciais brasileiras em 2022 ofereceram exemplos eloquentes de campanhas de desinformação nas redes sociais com utilização de conteúdos falsos. Dessa vez, uma das principais táticas utilizadas foi criar suspeição acerca da integridade e confiabilidade das urnas eletrônicas, questionando o resultado das eleições:

> Por mais de um ano, mensagens circularam nas redes sociais espalhando a falsa ideia de que as urnas eletrônicas não eram seguras e de que a Constituição, por meio de seu artigo 142, autorizaria uma intervenção militar em casos excepcionais para restabelecer a ordem (Mota, 2023).

Um dos resultados desse sentimento de fraude sobre o resultado das eleições presidenciais foi os ataques do dia 8 de janeiro de 2023, em que uma multidão invadiu a Praça dos Três Poderes e vandalizou símbolos da República brasileira.[18] Apesar de diversos fatores terem contribuído para que os atos de caráter golpista ocorressem, as campanhas de desinformação e a organização por meio de redes sociais desempenharam, mais uma vez, um papel crucial para a preparação e implementação do evento.[19]

Cabe destacar, porém, que a eventual inclusão da desinformação entre as ameaças que podem justificar uma intervenção securitária não é isenta de controvérsias devido ao risco de intervenção autoritária que tal inclusão pode ocasionar. Portanto, o entendimento a respeito da necessidade de securitização das ações coordenadas para a produção de informações falsas utilizadas nas redes sociais necessita de duas ressalvas. Primeiro, considerar plataformas digitais como infraestruturas críticas sob a égide de cibersegurança, isto é, como sistemas de comunicação digitais que sejam imprescindíveis para o funcionamento da nação, é dizer que elas precisam de medidas urgentes a serem tomadas pelos atores responsáveis pela implementação da segurança.

O problema é que, no Brasil, o setor responsável pela implementação de tais medidas securitizadoras é, historicamente, composto por atores militares e atores públicos. Apenas recentemente se observa, com a criação do novo Decreto nº 11.856/2023, uma abertura para outros atores participarem da formação da agenda de cibersegurança, porém não do monitoramento de sua implementação, em uma perspectiva de governança multissetorial.

---

18 No intuito de ilustrar a dimensão dos ataques empenhados, o gabinete do ministro Alexandre de Moraes, relator dos processos relacionados ao caso no STF, no dia 07 de janeiro de 2025 divulgou balanço com os principais dados e números sobre processos que tramitam na Corte sobre a matéria. São eles: *i)* somam-se 1.552 ações penais abertas sobre o 8 de janeiro de 2023; *ii)* 485 investigações em andamento; *iii)* condenação de 371 pessoas pela execução dos atos de 8 de janeiro de 2023, a maioria deles pelos crimes de abolição violenta do Estado Democrático de Direito, dano qualificado, golpe de Estado, associação criminosa e deterioração de patrimônio público tombado; *iv)* celebração de 527 acordos de não persecução penal, oferecidos para investigados que ficaram acampados em frente ao quartel-general do Exército, em Brasília, enquanto defendiam pautas como intervenção militar e questionavam a confiabilidade do sistema eleitoral brasileiro, sem cometer crimes com violência ou grave ameaça; e *v)* autorização da Operação Lesa Pátria, realizada pela Polícia Federal (Rupp, 2025).

19 (BBC News, 2023).

O Comitê Nacional de Cibersegurança (CNCiber), criado pelo decreto, é um órgão consultivo e não é o ator responsável pela regulação da cibersegurança. E, ainda que o arranjo institucional seja formado por atores civis, a multidimensionalidade da segurança cibernética envolverá também a competência das iniciativas provenientes da defesa cibernética.

A segunda ressalva é que, embora a cibersegurança seja uma ferramenta importante para reduzir riscos e promover a democracia, não é possível afirmar, sem vacilar, que não há outras medidas que sejam igualmente apropriadas e suficientes para fomentar e proteger o regime democrático, como, por exemplo, a regulação de plataformas digitais.

De fato, é preciso adotar a perspectiva da segurança como ponto de vista suplementar. Em outras palavras, deve-se perguntar qual a contribuição única que a cibersegurança oferece para a abordagem da desinformação e, a partir daí, limitar a atuação da estrutura institucional da cibersegurança a essa contribuição.

Uma importante contribuição da cibersegurança na luta contra a desinformação seria a definição de boas práticas e protocolos a serem implementados pelos próprios atores privados que gerenciam as plataformas, com o objetivo de reduzir riscos sistêmicos devidos à exploração indevida das vulnerabilidades dos sistemas que sustentam o funcionamento de tais plataformas para difusão de conteúdos falsos e enganosos.

Após a análise do conceito de cibersegurança, bem como do caso das infraestruturas críticas digitais e dos serviços essenciais, que exemplificam a complexidade envolvida em seu tratamento e desenvolvimento, a próxima seção aprofundará os tipos de ataques mais frequentes, as vulnerabilidades exploradas nesses ataques e suas consequências, com o objetivo de fornecer ao leitor um panorama mais completo dos riscos que afetam os ativos digitais e as infraestruturas críticas (ICs).

1.5 Uma taxonomia de ataques e ameaças cibernéticas e vulnerabilidades exploradas

Como destacamos em publicações precedentes[20] (Belli *et al.*, 2023b), incidentes de cibersegurança não se referem somente aos ataques ou falhas

20 Esta seção baseia-se amplamente no mapeamento desenvolvido na seção 1.2 de Belli *et al.* (2023b).

que levam à perda, destruição, bloqueio ou acesso não autorizado a informações, sistemas ou infraestruturas críticas, comprometendo princípios de confidencialidade, integridade, autenticidade e disponibilidade (conhecidos como tríade CIA), ou processos de controle de acesso, como identificação, autenticação e (conhecidos como tríade IAA)[21] (Van den Berg, 2020, p. 32).

Esses incidentes também se referem a comportamentos inseguros adotados por desenvolvedores(as) e usuários(as) de tecnologias e sistemas digitais (Van den Berg, 2020), incluindo aqueles que podem afetar a segurança das estruturas democráticas e o bom funcionamento da economia e sociedade.

Os efeitos de incidentes de cibersegurança são variados, podem se dar em dimensão coletiva ou individual e ter impactos locais, nacionais ou mesmo transnacionais. É interessante destacar que, no caso do Brasil, a maior parte dos ataques têm origem interna,[22] enquanto os alvos de ataques são extremamente variados, implicando empresas privadas, órgãos e entidades públicas.

Além disso, cabe também frisar que muitos dos ataques combinam diferentes técnicas para explorar as vulnerabilidades das redes e de seus usuários. Um exemplo são os ataques de *ransomware*, nos quais um *malware* é instalado para bloquear informações e sistemas de determinadas organizações, cujo acesso só é restaurado mediante pagamento de resgate ao agente malicioso. Frequentemente, esses ataques têm origem por meio de práticas de *phishing*.

As vulnerabilidades podem ser exploradas não apenas por meio de ataques ativos, mas também pela falta de medidas básicas de segurança (ciber-higiene), como o uso de senhas robustas, a cautela ao realizar downloads de arquivos suspeitos e a adoção de autenticação multifator. Segundo relatório da ENISA (2022a), os principais agentes responsáveis por explorar essas fragilidades são atores patrocinados por Estados, cibercriminosos, hacktivistas e hackers contratados por organizações privadas.

Cabe reiterar que, para além dos problemas no âmbito organizacional, as preocupações em relação aos ataques e demais incidentes cibernéticos afetam várias dimensões interconectadas, como proteção de dados,

21 Boas práticas relacionadas à implementação desses princípios serão abordadas por nós na seção 2.3 deste trabalho.

22 35,92% dos incidentes reportados ao CERT.br de janeiro a dezembro de 2024 tiveram origem no Brasil (CERT.br, 2025).

salvaguardas de interesses financeiros, proteção de infraestruturas públicas e políticas e controle de fluxos de informação e comunicação (Fichtner, 2018b). Os efeitos em qualquer uma dessas dimensões são replicados em cascata, principalmente se as medidas de segurança no momento de crise são desconhecidas, levando à propagação do ataque malicioso.

No quadro 2 são ilustrados alguns dos principais tipos de ataques, as vulnerabilidades que os possibilitam e suas potenciais consequências. Ilustrando as múltiplas facetas das ameaças cibernéticas, os ataques listados podem afetar também a segurança das infraestruturas críticas. No setor de transporte europeu, por exemplo, o *ransomware* figura como o ataque mais significativo (ENISA, 2023). No futuro, é provável que esses ataques impactem cada vez mais a prestação de serviços públicos, diante dos movimentos de transformação digital que abrangem áreas como saúde, justiça e transporte público – todas essenciais para o exercício de outros direitos.

Quadro 2 – Tipos de ataques/ameaças cibernéticas

Tipos de ataques/ameaças	Vulnerabilidades	Consequências
Desinformação	Uso da arquitetura de plataformas digitais (principalmente plataformas sociais) para dispersão de desinformação, afirmações enganosas, ou informações maliciosas.	1. Efeitos aos processos eleitorais; 2. Dispersão de discursos de ódio, intolerância, racismo, machismo, e preconceitos de outras naturezas; 3. Desestabilizar política, instituições e economia local de um país (ou organização social de outra natureza); 4. Impactos de natureza geopolítica, com impactos negativos na relação entre diferentes Estados; 5. Impacto na saúde coletiva e integridade física das pessoas (e.g., narrativas questionando a eficácia das vacinações que foram comuns durante a pandemia de COVID-19).

Tipos de ataques/ameaças	Vulnerabilidades	Consequências
Software ou Código Malicioso (Malware)	Se apresentam em formatos de links e/ou e-mails em que direcionam à instalação de softwares maliciosos no dispositivo. Os tipos mais comuns são os diferentes tipos de dispositivos eletrônicos, softwares *worms* ("vermes"), que se multiplicam para atingir diferentes dispositivos; cavalos de Tróia (arquivos aparentemente normais, infectados por vírus) (ENISA, 2022a).	1. Violação da tríade de princípios CIA ou IAA com a finalidade de solicitar resgate para reversão da atividade maliciosa e retomada da disponibilidade dos ativos; 2. Instalação de softwares maliciosos; 3. Obtenção de dados através do *spyware* (softwares de espionagem); 4. Compromete a operabilidade do sistema.
Esteliona-to de Dados (Phishing)	Tipo de engenharia social que se apresenta em formatos de links e/ou e-mails de comunicação capazes de se assemelhar a uma fonte fidedigna, com objetivo de obtenção indevida de informações por meio do compartilhamento dos seus próprios titulares. Existem diferentes modalidades de phishing (ENISA, 2022): (i) smishing, i.e., phishing realizado por meio de SMS (mensagens de textos enviadas ao celular); (ii) vishing, i.e., phishing realizado por meio de ligações telefônicas (e.g., robô se passando por telefone da instituição bancária da pessoa "alvo" do golpe); (iii) spear phishing, bastante comum no Brasil, em que o ator perpetrador do ataque se passa por outra pessoa (próxima ao ciclo da pessoa "alvo" do ataque), para obter informações ou benefícios – muitas vezes, o ataque é realizado com base em informações públicas ou tornadas públicas pelo/a seu/ua titular;	1. Obtenção de informações e dados sensíveis, cujo vazamento pode gerar graves consequências aos direitos fundamentais de seus titulares (pessoas a quem se referem as informações); 2. Realização de chantagens a partir das informações obtidas, para manipulação de comportamentos; 3. Obtenção de benefícios financeiros, por meio de pagamentos ou transferências indevidas.

Tipos de ataques/ameaças	Vulnerabilidades	Consequências
Estelionato de Dados (Phishing)	(iv) whaling, uma modalidade de spear phishing realizado com pessoas públicas (famosas, políticas ou pessoas que, por alguma razão, possuem grande influência no debate público); (v) QRishing é o uso de códigos QR maliciosos (infectados) para roubo de identidade/credenciais, ou dados em geral (seja pela sobreposição do QR legítimo ou pelo redirecionamento do url correspondente para um url não legítimo), para além de ser usado para fins ilícitos, a partir da mimetização de documentos oficiais, entre outras finalidades.	
Fraudes	No Brasil, são bastante comuns as fraudes bancárias (seja por meio de falsificação de boletos, envio de cobranças indevidas). Se vale da ocultação de informações, mimetização de informações (arquivos, documentos) relevantes. A contrafação, portanto, é uma manifestação da fraude. Também se vale de informações públicas ou obtidas indevidamente para prática da fraude.	1. Prejuízos financeiros a determinada pessoa; 2. Uso indevido de dados; 3. Danos reputacionais a organizações.
Falsidade ideológica/Roubo de identidade	Uso de aplicativos (e.g., plataformas de mídias sociais) para se passar por outra pessoa, valendo-se de informações disponíveis na internet sobre a pessoa que teve a identidade roubada.	1. Violação a garantias fundamentais da pessoa que teve a identidade roubada; 2. Danos aos direitos da personalidade da pessoa que teve a identidade roubada (podendo levar até mesmo a danos à integridade física da pessoa); 3. Possíveis perdas financeiras da pessoa que teve a identidade roubada.

Tipos de ataques/ameaças	Vulnerabilidades	Consequências
Ataque homem do meio (Man-in the middle attack (MitM))	São conhecidos como ataques de espionagem em que os invasores podem adentrar ao sistema da vítima através de: i) locais de acesso à rede Wi-Fi pública não segura; ii) falsificação de IP; iii) instalação de malwares no dispositivo; iv) roubo de cookies do navegador.	Os invasores passam a figurar nas duas pontas de determinada transação com o objetivo de interrompê-la e obter informações e/ou dados da vítima.
Introdução de Linguagem de Questionamento Estruturado (Structured Query Language (SQL) injection)	Ocorre quando os invasores inserem códigos maliciosos no servidor que usa SQL com o objetivo de que este revele informações e dados que normalmente não revelaria. Pode se dar por meio de caixas de pesquisas de websites vulneráveis.	Obtenção de informações e/ou dados pessoais que normalmente não seriam revelados.
Exploração no dia zero (Zero day exploit)	Consiste na descoberta de uma vulnerabilidade de software por invasores não detectada previamente pela própria vítima ou pelo desenvolvedor do sistema. Através desta vulnerabilidade os invasores entram no sistema para roubar informações e/ou dados.	1. Obtenção de informações e/ou dados; 2. Diante de ataques dessa natureza, há o impacto de aumento nos custos organizacionais de defesa (ENISA, 2022a, p. 11).
Reencaminhamento do sistema de nomes de domínio (DNS Tunneling)	Consiste em aproveitar a vulnerabilidade do DNS para realizar o tunelamento não legítimo de informações para o dispositivo do invasor. Pode até ser usado para retornos de chamada de comando e controle da infraestrutura do invasor para um sistema comprometido.	O invasor consegue extrair informações e dados do sistema comprometido para o seu próprio dispositivo.

Tipos de ataques/ameaças	Vulnerabilidades	Consequências
Vazamento de Dados	Pode se valer das técnicas acima para vazar informações disponibilizadas em determinada base de dados, ou de configurações erradas ou erros humanos, que levam à divulgação indevida da base.	1. Violação de direitos fundamentais ou coletivos por meio de tratamento indevido ou discriminatório de dados; 2. Desvios nas finalidades; 3. Uso das informações indevidamente divulgadas para prática de golpes, fraudes, ou outra das ameaças/ataques identificados nessa tabela.
Ataques a cadeias de suprimento	Combina um ou mais dos ataques acima para promover ataque a dois alvos, simultaneamente, i.e., um cliente e um fornecedor.	1. Promover ataque a toda a base de clientes de uma organização, por exemplo; 2. Interromper os serviços ou oferta de produtos por determinada organização; 3. Interromper as atividades de determinada organização, pela interrupção da prestação de serviço ou oferta de produto de determinado fornecedor.

Fonte: A tabela foi elaborada com base na taxonomia disponibilizada pela Cisco (*[S.d.]*) e na taxonomia apresentada no relatório da Ensina (2022a), que agrupa diferentes técnicas em 8 (oito) principais dimensões de ameaças: *ransomware*, *malware*, engenharia social, ameaças contra dados, negação de serviços, ameaças à internet, dispersão de desinformação e informações erradas, e ataques a cadeias de suprimentos (p. 10).

Notas:
(1) Destaca-se que as consequências são meramente exemplificativas.
(2) A taxonomia de tipos de impactos apresentada no relatório da ENISA (2022a, p. 15) reúne os diferentes exemplos em cinco principais eixos: danos reputacionais, impactos digitais (i.e., aos sistemas e tecnologias digitais), impactos econômicos/financeiros, impactos físicos (i.e., "lesão ou prejuízos a empregados, clientes ou pacientes" – acrescentamos eleitores e coletividades específicas) e impacto social.
(3)O DNS, ou Sistema de Nomes de Domínio, se trata de um sistema responsável por fazer a associação entre nomes (que sejam mais facilmente memorizáveis, e tenham maior proximidade com o universo de palavras/linguagem usada no dia a dia das pessoas) para identificação de sistemas, serviços e dispositivos conectados à Internet – aos quais, normalmente, são atribuídos códigos alfanuméricos (cuja compreensão é mais difícil do que nomes comerciais ou próprio.

Diante desta multitude de ameaças e ataques, como será destacado ao longo deste trabalho, o diálogo com instituições técnicas como os CSIRTs e os Centros de Compartilhamento e Análise de Informações (ISACs,[23] na sigla em inglês) é essencial, em função do seu posicionamento privilegiado para acessar informações sobre novas dinâmicas e ameaças à cibersegurança, bem como boas práticas para lidar de maneira efetiva e eficiente com tais fenômenos. Neste sentido, diante do caráter dinâmico e do baixo custo de combinação de múltiplas técnicas para a execução de ataques, uma abordagem multissetorial parece particularmente útil.

Frente ao panorama complexo e em constante evolução das ameaças cibernéticas, fica claro que a resposta técnica aos ataques deve ser complementada por uma abordagem que priorize a proteção dos direitos fundamentais e a independência tecnológica. A garantia da liberdade de expressão, a proteção dos dados pessoais, o acesso à informação e a promoção da literacia digital são pilares fundamentais para que a cibersegurança coloque o indivíduo no centro do seu desenvolvimento. Ao centrar as políticas e práticas nesses direitos, não apenas se fortalece a resiliência dos ativos digitais, mas assegura a construção de ambientes digitais inclusivos, democráticos e que respeitem a dignidade humana e a soberania nacional. A próxima seção será dedicada à análise da abordagem humanista para a cibersegurança, evidenciando sua importância para a soberania digital.

1.6 Direitos fundamentais como base de uma abordagem à cibersegurança centrada nas pessoas

Como apontado até o momento, à luz da teoria da securitização, o conceito de segurança migrou do tradicional enfoque político-militar para uma abordagem ampliada, multidimensional e setorial, envolvendo uma pluralidade de atores. Todavia, ao ser aplicado ao ciberespaço, o processo de securitização raramente foi protagonizado pelos direitos fundamentais dos usuários e das populações impactadas pelas tecnologias digitais.

23 Information Sharing and Analysis Center (ISACs) são centros destinados predominantemente ao compartilhamento de informações, protocolos e boas práticas para segurança cibernética.

Sustentar uma cibersegurança verdadeiramente eficaz exige, portanto, uma perspectiva centrada na proteção e no empoderamento do indivíduo, de modo que a cibersegurança se torne facilitadora, e não limitadora, de liberdades essenciais. Sob esse prisma, a cibersegurança, longe de ser uma mera questão técnica ou de defesa estatal, deve ser entendida como um componente essencial para a efetivação dos direitos humanos, por meio da construção de ambientes digitais seguros, justos e democráticos.

O Decreto nº 11.856/2023, que institui a Política Nacional de Cibersegurança (PNCiber) no Brasil, explicita essa prioridade ao afirmar que a garantia dos direitos fundamentais, em especial a liberdade de expressão, deve balizar as ações de segurança cibernética. Essa orientação normativa reconhece que a proteção da infraestrutura digital não pode se sobrepor ao direito das pessoas de se expressar e de acessar informações, sob pena de comprometer a própria essência da democracia e do pluralismo. Neste sentido, a proteção da liberdade de expressão exige que a cibersegurança assegure espaços digitais onde as pessoas possam manifestar suas opiniões, acessar informações e se comunicar livremente, sem medo de ataques ou repressão.

Paralelamente, a proteção de dados pessoais e a privacidade são pilares fundamentais da cibersegurança orientada por direitos, conforme será abordado na seção 1.6. O avanço das tecnologias digitais intensificou a coleta, o armazenamento e o processamento de dados pessoais, expondo os indivíduos a riscos de violações que podem comprometer sua dignidade, autonomia e segurança. A Lei Geral de Proteção de Dados (LGPD) oferece um bom exemplo de marco regulatório que vincula a segurança da informação à salvaguarda desses direitos, impondo obrigações a agentes públicos e privados para garantir o tratamento adequado e transparente dos dados pessoais, em observância ao princípio da autodeterminação informativa do indivíduo.

O direito ao acesso à informação, igualmente fundamental, está intrinsecamente ligado à cibersegurança, pois a disponibilidade, integridade e autenticidade dos dados e sistemas são condições necessárias para que os cidadãos possam exercer plenamente esse direito (Belli *et al.,* 2023b). Neste sentido, a PNCiber destaca a importância de garantir a confidencialidade, integridade, autenticidade e disponibilidade das soluções e dos dados utilizados para o processamento e transmissão eletrônica ou digital de informações, ressaltando que a cibersegurança deve proteger os serviços es-

senciais prestados à sociedade, garantindo que o acesso à informação não seja comprometido por ataques cibernéticos. Assim, a segurança digital configura-se como condição para a transparência, a participação cidadã e a formação de uma opinião pública informada.

Além disso, a educação em cibersegurança e a autonomia tecnológica são elementos centrais para uma abordagem que coloca os direitos fundamentais no centro da agenda.[24] A capacitação técnico-profissional e a literacia digital são essenciais para que os indivíduos compreendam os riscos e saibam como se proteger no ambiente digital, promovendo uma cultura de segurança que respeite a dignidade humana e estimule a participação ativa e consciente. A autonomia tecnológica, por sua vez, refere-se à capacidade dos usuários e das sociedades de controlar e desenvolver tecnologias que atendam às suas necessidades, sem ficarem submetidos a sistemas opacos ou dependentes de atores que possam comprometer sua privacidade e liberdade. Como será evidenciado neste livro, a autonomia tecnológica é um pilar fundamental da soberania digital.

Esse entendimento encontra respaldo na literatura acadêmica que defende uma abordagem humanista e de direitos fundamentais para a cibersegurança. Deibert enfatiza que a cibersegurança deve ser concebida para proteger os direitos e liberdades das pessoas, e não apenas para defender infraestruturas ou interesses estatais (Deibert, 2018). Singh (2023) destaca a complexidade dessa inter-relação, demonstrando que medidas de segurança podem tanto proteger quanto ameaçar direitos humanos, o que exige equilíbrio e sensibilidade ética. Pawlicka *et al.* (2022) propõem um paradigma de cibersegurança centrado no ser humano, que valorize a participação, a confiança e o empoderamento dos usuários, em vez de tratá-los como vulnerabilidades ou ameaças.

Dessa forma, a abordagem de cibersegurança centrada nas pessoas, inicialmente teorizada por Ron Deibert (2018), propõe uma mudança fundamental na forma como se encara a segurança digital. Diferentemente do modelo predominante, que é centrado na segurança nacional e privilegia o Estado soberano como principal ator, esta abordagem coloca os indivíduos e seus direitos fundamentais no centro das políticas, leis e práticas de cibersegurança.

24 Essas dimensões serão analisadas nas seções 1.6, 2.5, 2.6 e 3.

Como destacado anteriormente, na perspectiva tradicional centrada na segurança nacional, a proteção dos ativos digitais é compreendida a partir da lógica da competição entre Estados, com foco na proteção da infraestrutura crítica e da soberania territorial. Essa visão frequentemente atribui as responsabilidades pela garantia da cibersegurança principalmente a agências militares, de inteligência e policiais, o que pode implicar riscos de práticas autoritárias e repressivas (Deibart, 2018).

Em contraste, a abordagem centrada no ser humano defende que todos os aspectos da cibersegurança devem ser fundamentados nos direitos humanos e na capacitação individual,[25] reconhecendo o ciberespaço como essencial para o exercício das garantias constitucionais e buscando colocar a dignidade, direitos e segurança dos indivíduos em primeiro lugar.

Nesse modelo, o papel do Estado é suportar instituições cuja finalidade é proteger o bem-estar dos indivíduos, e não simplesmente reforçar a segurança do Estado em si. Essa abordagem não almeja eliminar o papel dos órgãos de segurança, mas redefine seu foco para garantir que a segurança digital contribua para a segurança humana. Dessa forma, essa visão desafia a hegemonia da abordagem militarizada de cibersegurança, propondo um modelo no qual a supervisão cidadã e revisão independente desempenham papel essencial.

Assim, a garantia dos direitos fundamentais, como liberdade de expressão, proteção de dados pessoais, privacidade, acesso à informação e educação, bem como a autonomia tecnológica se tornam pilares essenciais para a construção das políticas e práticas de cibersegurança. A efetivação desses direitos no ambiente digital não apenas fortalece a democracia e a cidadania, mas também promove a construção de um ciberespaço mais seguro, inclusivo e respeitador da dignidade humana. Portanto, a cibersegurança orientada por direitos fundamentais representa um avanço indispensável para enfrentar os desafios contemporâneos e assegurar que a tecnologia sirva ao desenvolvimento humano e social.

Como será destacado na próxima seção, uma abordagem baseada na promoção do texto constitucional é essencial para a promoção da autonomia tecnológica, permitindo que indivíduos e a Nação desenvolvam

25 Nesta perspectiva a literacia digital desempenha uma função crucial, como destacaremos na seção 2.5.

a capacidade de compreender o funcionamento das tecnologias digitais, desenvolvê-las e regular efetivamente os riscos a elas associados. Essas capacidades constituem os pilares da soberania digital, tema que será explorado a seguir, destacando-se sua relação com a autonomia tecnológica e a capacidade regulatória dos Estados. Em particular, será analisado como a soberania digital fortalece a segurança cibernética e possibilita a construção de um ecossistema de inovação nacional.

1.7 Soberania digital: entender, desenvolver e regular as tecnologias digitais de maneira soberana e cibersegura

Embora a soberania digital tenha atraído uma atenção crescente tanto dos decisores políticos como dos acadêmicos, este conceito continua a ser fluido, polissêmico e multifacetado, não tendo ainda encontrado uma definição universalmente aceita. A soberania digital pode ser definida como a capacidade de entender o funcionamento das tecnologias digitais, conseguir desenvolvê-las e regulá-las efetivamente, exercendo, portanto, autodeterminação, poder e controle sobre ativos digitais[26] tais como dados, *softwares*, hardwares, redes eletrônicas e bancos de dados (Belli *et al.* 2023; Belli, 2023b; Belli; Jiang, 2024). Ela implica na aptidão dos Estados para estudar e, idealmente, entender os efeitos positivos e negativos que cada escolha tecnológica pode ocasionar, bem como possuir capacidade de definir o seu próprio desenvolvimento tecnológico de maneira autônoma e consciente.

Apesar da amplitude conceitual que abrange tanto a cibersegurança quanto a soberania digital, observa-se também uma relação de sinergia entre esses dois conceitos. Isto é, para alcançar a soberania digital, é preciso que as nações e entidades que as compõem invistam no seu próprio desenvolvimento digital e segurança cibernética. Tal objetivo demanda investimentos estratégicos no fortalecimento de capacidades, na pesquisa e desenvolvimento, bem como na manutenção de infraestruturas digitais robustas; na formação contínua da força de trabalho; na atualização de

26 O ativo digital aqui se refere a todos os tipos de hardware e software que suportam produtos e serviços digitais, e pode ser usado analogamente ao termo "infraestruturas digitais" adotado nos trabalhos de Estudos de Ciência e Tecnologia, que tipicamente incluem protocolos, aplicações de software e infraestruturas de hardware.

hardware e software; e na implementação de práticas organizacionais e técnicas voltadas à proteção da informação.

Assim, à medida que se avança o desenvolvimento digital, a cibersegurança revela-se um elemento fundamental para a materialização da soberania digital (Belli *et al.*, 2023b). Por isso, torna-se pertinente destacar seus principais elementos para que se possa entender como ela se relaciona com a cibersegurança.

Primeiramente, cabe ressaltar que a noção westfaliana de soberania é entendida como a prerrogativa dos Estados-Nação do pleno gozo da integridade territorial, igualdade legal e não interferência em assuntos internacionais junto com o monopólio do uso legítimo da força e autoridade suprema sobre seu território (Belli; Jiang, 2024). Porém, tal noção implica uma centralidade estatal desafiada pelo papel essencial que tecnologias digitais com alcance transnacional – que incluem desde o ciberespaço até sistemas de IA – acabam desempenhando no que diz respeito ao funcionamento de sociedade, economias e democracias (Belli, 2025a; Medeiros; Goldoni, 2020).

Tal evolução tornou a cibersegurança um elemento imprescindível para o exercício da soberania, e a construção da soberania digital uma prioridade inevitável de qualquer Estado intencionado a preservar sua soberania nacional (Castells, 2003; Nye, 2012, 2010; Santos, 2022). Sob essa perspectiva, a construção da cibersegurança não deve ser enxergada como custo, mas como uma oportunidade para promover o desenvolvimento tecnológico, social e econômico do país.

Como será detalhado na seção 2.6, dedicada à política industrial, os fundamentos que articulam soberania digital e cibersegurança devem ser alicerçados em atividades de pesquisa e desenvolvimento, em investimentos estratégicos voltados a trajetórias tecnológicas e educacionais, bem como em modelos de governança efetivos e marco regulatório com padrões mínimos para o setor.

É importante frisar que no Brasil a soberania digital encontra amparo constitucional diretamente na autonomia tecnológica, que é objetivo constitucionalmente protegido. Assim, nos termos do artigo 219 da Constituição da República Federativa do Brasil:

> O mercado interno integra o patrimônio nacional e será incentivado de modo a viabilizar o desenvolvimento cultural e socioeconômico, o bem-estar da população e a autonomia tecnológica do País, nos termos de lei federal.
> Parágrafo único. O Estado estimulará a formação e o fortalecimento da inovação nas empresas, bem como nos demais entes, públicos ou privados, a constituição e a manutenção de parques e polos tecnológicos e de demais ambientes promotores da inovação, a atuação dos inventores independentes e a criação, absorção, difusão e transferência de tecnologia.

Para se alcançar tal autonomia tecnológica, é necessário se adotar estratégias, políticas e mecanismos de governança e regulação aptos a entender e gerir as (inter)dependências e as potenciais vulnerabilidades existentes entre os diferentes elementos que sustentam o funcionamento das tecnologias digitais e, particularmente, dos sistemas de cibersegurança e tecnologias de IA.

Tais elementos podem ser considerados como "facilitadores" da soberania digital. Estes facilitadores estão interligados e é essencial entender esta conexão para regular de maneira eficiente e efetiva. No caso dos sistemas de IA, os "Facilitadores Essenciais da Soberania em IA" são: bancos de dados, modelos algorítmicos, infraestrutura computacional, de conectividade, e elétrica, recursos humanos, marcos regulatórios capazes de mitigar riscos de maneira efetiva (Belli, 2023c, 2024b).

Como destacado anteriormente, o conceito de soberania digital ainda carece de uma definição universalmente aceita, embora tenha evoluído consideravelmente ao longo dos últimos quinze anos (Ayers, Cynthia E., 2016; Belli, 2021a; Belli; Gaspar; Jaswant, 2024; Couture; Toupin, 2018; Floridi, 2020; Jiang; Belli, 2024; Pohle; Thiel, 2020). Trata-se de um conceito polissêmico, ou seja, passível de assumir diferentes significados, com perspectivas positivas ou negativas. Essas interpretações podem visar o empoderamento e desenvolvimento social, mas também podem revestir-se de contornos autoritários e protecionistas, a depender de como o conceito é implementado na prática (Belli, 2025a; Belli; Jiang, 2024).

Por isso, é importante promover uma "boa soberania digital" (Belli, 2023a), entendida como uma abordagem voltada ao fortalecimento das capacidades de pesquisa e desenvolvimento tecnológico autônomo, bem

como à regulação efetiva e eficiente das tecnologias adotadas, sempre em conformidade com os valores constitucionais (Belli; Gaspar, 2023b).

As medidas de soberania digital e de cibersegurança desempenham um papel altamente complementar: o estudo da tecnologia é essencial para identificar e prevenir usos abusivos, enquanto o desenvolvimento tecnológico contribui para a criação de soluções mais seguras. A regulação, por sua vez, desempenha um papel fundamental no equilíbrio do setor, definindo os padrões mínimos a serem implementados para facilitar o desenvolvimento e adoção sustentável das tecnologias digitais, reduzindo e – idealmente – evitando riscos e, caso seja necessário, sancionando comportamentos abusivos.

A construção e fortalecimento da cibersegurança e da soberania digital devem ser enxergados como prioridades estratégicas distintas, porém intimamente conectadas, que cada Estado e organização deve almejar alcançar de forma mais completa possível. Esses dois conceitos sobrepõem-se no seu objetivo final de assegurar a capacidade de manter controle, autonomia e capacidade regulatória sobre ativos digitais. Nesta perspectiva, ser digitalmente soberano é instrumental para ser também ciberseguro e, da mesma forma, ser ciberseguro é instrumental para ser soberano digitalmente. Assim, não é concebível ser ciberseguro numa situação de falta de conhecimento sobre o funcionamento da tecnologia adotada, incapacidade de desenvolver soluções alternativas e de regular os riscos inevitavelmente associados ao uso de tecnologias digitais.

Por fim, é importante frisar que a promoção da soberania digital não significa se isolar e instaurar uma autarquia digital. Ao contrário, representa uma visão desenvolvimentista capaz de promover pesquisa, desenvolvimento e inovação e adoção de tecnologias nacionais voltadas a garantir a cibersegurança do país e empoderar a população.

A segunda parte deste trabalho explorará os elementos que devem permear a abordagem nacional de cibersegurança para que tal abordagem seja completa, eficaz e efetiva, contribuindo ao mesmo tempo ao fortalecimento da soberania digital do país. Serão analisados aspectos como a governança, a importância da promoção da literacia digital, a implementação de uma política industrial robusta, a proteção e segurança da informação, a prevenção e o enfrentamento do cibercrime, bem como o desenvolvimento de tecnologias nacionais.

2 Elementos constitutivos da cibersegurança

A primeira parte deste trabalho apresentou uma análise do fenômeno da cibersegurança. Partindo das bases teóricas da Escola de Copenhague sobre securitização, foi discutido como a segurança, tradicionalmente vinculada ao domínio político-militar, passou a englobar novas esferas, como a econômica e a social, por meio do processo de securitização, caracterizado como um ato discursivo que define objetos de referência que necessitam de proteção.

Neste contexto, a cibersegurança foi identificada como uma área específica dentro dos estudos de segurança, conforme argumentado por Hansen e Nissenbaum (2009). O discurso securitizador no campo cibernético traduz-se na formalização da percepção de ameaças e riscos em documentos estratégicos e políticas nacionais, produzindo impactos político-administrativos em diferentes Estados. No caso brasileiro, verificou-se a evolução do tema desde sua incorporação nas Forças Armadas até sua expansão para políticas públicas civis. Esse processo se reflete na formulação de normativas como a Política Nacional de Cibersegurança, instituída pelo Decreto 11.856/2023; e a Estratégia Nacional de Cibersegurança, instituída pelo Decreto nº 12.573/25.

A análise revelou que a cibersegurança não possui uma definição única na literatura acadêmica. A conceituação mais aceita e universalmente difundida é proposta pela União Internacional de Telecomunicações (ITU-T). Para fins deste trabalho, adota-se a compreensão de cibersegurança como um conjunto de iniciativas para promover a segurança de objetos de referência – incluindo pessoas – em face de riscos cibernéticos.

Ademais, diferenciou-se ciberdefesa de cibersegurança e foi examinado o caso das infraestruturas críticas (ICs) e serviços essenciais, fundamentais para o desenvolvimento e funcionamento da sociedade, e sua relevância para cibersegurança. Observou-se que as ICs e serviços essenciais podem sofrer hibridização no seu tratamento, isto é, podem fazer incidir a regulação de cibersegurança, mas também podem receber regulações e ações específicas da ciberdefesa. Destacou-se um cenário de multiplicidade de atores responsáveis por promover as respectivas ações de cibersegu-

rança ou ciberdefesa (seja no campo regulatório ou operacional). Por essa razão foi ressaltada a necessidade de coordenação e cooperação entre os diversos atores envolvidos nesse ecossistema.

Também foi apresentada uma taxonomia das ameaças e vulnerabilidades exploradas por ataques cibernéticos, bem como daquelas decorrentes da ausência de medidas básicas de cibersegurança. Após isso, destacou-se a importância de adotar uma abordagem baseada nos direitos fundamentais, colocando o ser humano no centro das ações de cibersegurança, pois somente dessa forma é possível construir um ambiente digital seguro e democrático.

Por fim, discutiu-se o conceito de soberania digital e sua sinergia com a cibersegurança. A interdependência entre soberania digital e cibersegurança torna essencial a criação de políticas industriais e mecanismos de governança que promovam investimentos estratégicos, além da promoção da literacia digital, que compreende a capacitação, educação, formação e capacitação contínua da força de trabalho em cibersegurança.

A segunda parte deste trabalho busca enumerar as vertentes que são essenciais para o desenvolvimento e efetivação da cibersegurança, estabelecendo, assim, as bases indispensáveis à consolidação da soberania digital. Serão abordados os seguintes eixos: *i)* governança; *ii)* mecanismos de segurança da informação; *iii)* combate ao cibercrime; *iv)* literacia digital; *v)* política industrial; e *vi)* tecnologias disruptivas, com especial atenção à inteligência artificial (IA).

Essas ações funcionam como elementos estratégicos mínimos que devem permear o universo da cibersegurança, podendo haver outras ações necessárias em razão das especificidades enfrentadas. O importante, porém, é que haja uma política nacional que implemente uma estratégia basilar, um *framework* a ser desenvolvido em âmbito nacional.

Neste sentido, a E-Ciber/2025 representa um avanço em termos da implementação da política pública instituída pela PNCiber (Decreto nº 11.856/2023), pois permite o fortalecimento da cibersegurança no Brasil, protegendo os ativos digitais sem descuidar dos direitos fundamentais e da soberania digital. Conforme poderá ser observado nas próximas seções, os eixos estabelecidos neste trabalho, anteriormente descritos, correspondem aos eixos estabelecidos pela própria E-Ciber, ainda que essa tenha adotado nomes distintos.

2.1 Governança

À luz do exposto na primeira parte deste trabalho, a cibersegurança, conforme debatido pela literatura, possui múltiplos objetos de referência, que são regulados e impactados pela atividade de diversos atores, o que demanda comunicação, coordenação e cooperação para conseguir uma atuação efetiva e eficiente (Belli, 2016; Belli *et al.*, 2023b; Dunn Cavelty; Wenger, 2020).

Para compreender melhor o escopo da cibersegurança, é importante considerar que a globalização das tecnologias digitais e a própria arquitetura da Internet como rede de redes reduzem e desafiam o papel centralizador do Estado no que diz respeito à entrega de soluções aptas a implementar políticas públicas (Castells, 2003; Nye, 2012, 2010). A cibersegurança é um tema que se desenvolve dentro desse contexto de digitalização proporcionado pelo uso das tecnologias digitais, no âmbito do qual a governança multissetorial se torna essencial para incrementar a qualidade da elaboração regulatória e a efetividade da implementação das soluções designadas (Belli, 2016).

Conforme destacado na seção anterior, o cenário atual aponta para um quadro complexo e dotado de múltiplos atores, o que gera fragmentação na regulação. Essa situação não foi resolvida na promulgação do Decreto nº 11.856 de 2023 (Presidência da República, 2023b), que implementou a Política Nacional de Cibersegurança (PNCiber), pois sua validade é limitada ao âmbito federal, sem vincular a temática de cibersegurança aos demais entes federativos e Poderes,[27] além dos setores regulados pelas Agências Reguladoras, como a ANATEL e a ANEEL, e outras autarquias e órgãos federais, tais como o Banco Central e SUSEP, que regulam setores econômicos brasileiros.

A E-Ciber (Decreto nº 12.573/25) também não solucionou a questão, vez que, embora preveja um eixo sobre governança e soberania nacional,

27 A título de exemplo pode-se mencionar a Resolução nº 396/2021 do Conselho Nacional de Justiça (CNJ), que instituiu a Estratégia Nacional de Segurança da Informação e Cibernética do Poder Judiciário (ENSEC-PJ); a proposta, via Resolução CNMP nº 260/2023, que institui a doutrina da inteligência, para criação da Política Nacional de Cibersegurança do MP (PNCiber-MP); o Decreto Estadual nº 48891/2024 do Governo do Estado do Rio de Janeiro, que, apesar de não ser específico para a cibersegurança, regulamenta a política de segurança da informação do Estado; e outros.

na forma do artigo 1º, inciso IV, não apresenta qualquer menção de um arranjo institucional que, em nível nacional, seja capaz de promover maior harmonização, cooperação e coordenação. Tal arranjo poderia aprimorar a comunicação, indicando diretrizes e vinculando, quando necessário, todas as partes que desempenham um papel essencial no setor.

Dessa forma, essa seção analisa, a partir de considerações sobre o ambiente em que ocorre a atividade de segurança cibernética, o tipo de estrutura administrativa que seria mais adequado para exercer essa governança.[28] Também se apresentam um panorama da regulação setorial existente e as funções exercidas por alguns dos atores que integram esse ecossistema em nível federal.

2.1.1 Funções inerentes à governança em cibersegurança

Conforme anteriormente destacado (Belli *et al.*, 2023b), é essencial que seja estabelecida uma estrutura de governança capaz de direcionar as ações em cibersegurança, exercendo funções regulatórias (normativas, fiscalizatórias e sancionatórias), bem como funções coordenatórias entre os diversos órgãos regulatórios que possuam competência normativa em cibersegurança e entre os atores operacionais.

A estrutura de governança deve ser responsável por implementar, em sua esfera de atribuições, a PNCiber e seus instrumentos, o que inclui a E-Ciber/2025, assegurando que as diretrizes nacionais sejam efetivamente traduzidas em ações concretas e coordenadas com as outras autoridades reguladoras, bem como órgãos e entidades que atuam no campo operacional, como os CSIRTs.

Nesse sentido, a E-Ciber em seu artigo 6º, II, estabelece a necessidade de mecanismos de regulação, fiscalização e controle como ações necessárias para a manutenção dos serviços essenciais e infraestruturas críticas digitais. O exercício de competências regulatórias, especialmente normativas, não implica, entretanto, a subordinação de setores já regulados. É importante

28 É importante registrar que a indicação de um arranjo institucional mais adequado neste trabalho não implica em invalidar outras modalidades de arranjo, o que será abordado ao longo desta seção. Cada tipo de arranjo apresenta pontos negativos e positivos. O que se defende é que, seja qual for a estrutura, essa deve conseguir desempenhar as funções inerentes à governança de cibersegurança de forma efetiva e eficiente.

considerar que, ainda que o arranjo adotado tenha competência em nível nacional, devem ser respeitadas as normas regulatórias já elaboradas, bem como a competência previamente atribuída a outros órgãos reguladores no campo da cibersegurança, quando existente (artigo 6º, I, da E-Ciber).

Também é necessário considerar, quanto à competência regulatória, que essa atribuição não significa a formulação de política única, sem a consideração de assimetrias setoriais. As especificidades dos ativos digitais (atividade desenvolvida, tecnologia e infraestruturas utilizadas, informações armazenadas etc.) e dos grupos que os titularizam apresentam questões particulares que nem sempre devem ser observadas em todos os setores a depender do grau de risco cibernético identificado.

A comunicação entre essa autoridade de cibersegurança e os demais órgãos reguladores, especialmente aqueles encarregados de regular serviços essenciais e infraestruturas críticas, deve ser facilitada justamente para que a coordenação seja mais efetiva, além de garantir a troca de experiência e aplicação dos instrumentos de coordenação regulatória. Neste ponto, é interessante mencionar que a E-Ciber traz como um dos seus eixos a cooperação e integração entre órgãos e entidades (públicas ou privadas), na forma dos artigos 7º e 8º da referida estratégia.

A função de coordenação implica, também, conferir ao arranjo institucional de cibersegurança, responsável pela governança, a competência para gerenciar os atores operacionais responsáveis pela resposta a incidentes cibernéticos e mecanismos eficazes de prevenção. Conforme destacado na seção anterior, além dos atores com competência regulatória pertencentes a setores específicos, há atores que atuam no campo operacional e que atuam na linha de frente para a promoção da securitização cibernética: são os Grupos de Segurança e Resposta a Incidentes (CSIRTs, na sigla em inglês) e os Centros de Análise e Compartilhamento de Informações (ISACs, na sigla em inglês), que podem ser públicos ou privados.[29]

Para esses atores, é preciso estabelecer canais de comunicação para o compartilhamento de informações sobre os riscos cibernéticos identificados e estratégias de mitigação. Aliás, essa é uma das preocupações des-

29 Destaca-se que A E-Ciber/2025 prevê como parte da cooperação o estímulo à criação e desenvolvimento de equipes de prevenção e resposta a incidentes de cibersegurança (CSIRTs) e centros de análise e compartilhamento de informações (ISACs), conforme artigo 8º, I, b e c. Tais pontos serão abordados nas subseções 2.1.4 e 2.1.5.

tacadas pela E-Ciber/2025 quando estabelece a necessidade de criação de um mecanismo nacional de notificação de ciberincidentes, nos moldes do artigo 8º, II, e o cabimento, no âmbito da governança, de ações para estimular o uso de sistemas para trocas seguras de informações (artigo 10, VI).

Esses canais de comunicação devem funcionar não apenas entre os próprios atores operacionais, mas também entre eles e a estrutura de governança a ser implementada, pois a atuação operacional gera dados valiosos para a elaboração de boas estratégias regulatórias. É fundamental ressaltar que esse intercâmbio informacional entre os órgãos operacionais e a estrutura regulatória não deve ter como objetivo a fiscalização ou a aplicação de sanções, mas sim o aprimoramento contínuo dos mecanismos de prevenção e resposta a incidentes cibernéticos.

Nesse sentido, a função de coordenação requer que a estrutura de governança ultrapasse a mera imposição de comandos regulatórios rígidos e vinculantes, atuando como um facilitador e coordenador da comunicação entre os setores. Por esse motivo, é interessante que o arranjo adote estratégias regulatórias menos verticalizadas e mais horizontais. Tais estratégias podem ser híbridas, combinando atores governamentais e não governamentais, multifacetadas, combinando diferentes abordagens.

Essas características levantam uma série de questões que influenciam e, em certa medida, restringem a definição do desenho do futuro arranjo institucional a ser adotado. Um dos principais questionamentos é se tal arranjo poderá ser estruturado dentro da Administração Pública centralizada, por meio de um órgão específico, como, por exemplo, secretarias.

Além disso, outro questionamento importante refere-se ao instrumento normativo utilizado. A limitação ao âmbito federal decorrente do uso de um decreto, conforme previsto no artigo 84, inciso VI, alínea "a", da Constituição da República Federativa do Brasil, revela-se uma escolha restritiva. Isso ocorre porque tal modelo reduz a atuação do órgão ao governo federal, limitando sua capacidade de coordenação e a formação de um sistema nacional de cibersegurança.

Restrições orçamentárias e escolhas políticas, contudo, podem apontar para tal modelo. Nesse caso, então, o ideal é que esse órgão integrante da Administração Direta seja instituído por lei, pois assim poderia apresentar abrangência nacional e competência regulatória.

Destaca-se que há diversos órgãos federais que possuem competências regulatórias e podem servir de modelo para a criação de uma secretaria de cibersegurança. Um exemplo atual e interessante é a criação da Secretaria de Prêmios e Apostas, vinculada ao Ministério da Fazenda. O Decreto nº 11.907/2024, amparado por lei prévia, em seu artigo 55, atribui à Secretaria amplas competências regulatórias, incluindo a normatização, fiscalização e sanção.

Atualmente, não existe nenhum órgão ou entidade, seja pública ou privada, capaz de desempenhar essa função de forma abrangente. Conforme já mencionado, a PNCiber e a E-Ciber foram omissas nesse aspecto. Hoje, o Gabinete de Segurança Institucional (GSI) tem atribuição para coordenar ações em cibersegurança, mas enfrenta limitações decorrentes de seu modelo institucional. Entre essas restrições, destaca-se o fato de ser uma estrutura centralizada no Poder Executivo, sem competência para editar normas vinculantes para outros Poderes ou entes federativos, além da ausência de atribuição para monitorar a implementação das ações na área. Ademais, sua composição majoritariamente formada por militares reforça a dificuldade de dissociar cibersegurança de ciberdefesa, contrariando a separação já consolidada entre essas duas áreas.

O panorama institucional atual, com exceção do atual Comitê Nacional de Cibersegurança (CNCiber), cujo papel é exclusivamente propositivo, não promove o desenvolvimento da coordenação, cooperação, seja entre atores públicos e privados, seja intersetorial, tampouco favorece o exercício da participação social. A lacuna de uma autoridade que possa concentrar tais ações correlatas à implementação da Política Nacional de Cibersegurança e da E-Ciber/2025 precisa ser preenchida. É o que será analisado na próxima subseção.

2.1.2 Qual tipo de estrutura administrativa deve ser criada para a governança de cibersegurança?

Para o exercício das funções anteriormente mencionadas, é preciso escolher um arranjo institucional que possa desempenhá-las e que seja estabelecido por lei para gerar vinculação em âmbito nacional. Ele precisa ser descentralizado para que suas ações possam ser mais dinâmicas, efi-

cientes e efetivas, bem como separadas do processo de tomada de decisão que envolva questões de governo.

O Brasil já adota, desde a reforma gerencial administrativa, um modelo de agências reguladoras para a governança de certas políticas públicas em determinados setores, no qual se pressupõe um Estado mais voltado à normatização e ao monitoramento do que à produção de bens ou serviços (Majone, 1998). Esse modelo possui características que são importantes para o exercício da governança em cibersegurança, embora não esteja isento de desafios.

A independência das Agências Reguladoras em relação aos demais Poderes centrais do Estado é uma das características mais atraentes desse modelo de governança. A autonomia funcional e financeira das agências permite que essas entidades consigam regular um determinado setor com mais tecnicidade e trabalhar na busca do equilíbrio do setor e na facilitação da comunicação entre os diversos sistemas sociais (Aragão, 2013).

Por serem independentes,[30] as agências reguladoras são autarquias especiais que se situam fora do aparelho estatal e, portanto, não estão sujeitas à subordinação hierárquica do órgão ao qual estão vinculadas. Essa emancipação é garantida por uma autonomia reforçada, prevista no artigo 3º da Lei nº 13.848/19, além da concessão de garantias orgânicas, tais como inamovibilidade do dirigente e mandato por prazo certo, entre outras. Essas garantias fornecem à instituição posição e força para enfrentar interesses políticos e econômicos, garantindo o equilíbrio do setor e a defesa dos interesses públicos.

O modelo de Agência Reguladora para o exercício da governança em cibersegurança também é favorecido em razão da alta capacitação exigida dos agentes públicos a cargo da regulação do setor, uma vez que as entidades reguladoras precisam de mão de obra especializada para acompanhar o constante desenvolvimento da área.[31]

---

30 Não se ignora que existem vários obstáculos para as Agências exercerem suas autonomias de forma plena na prática. Foge ao escopo deste trabalho listá-los aqui, porém para um aprofundamento sobre o tema o leitor pode consultar Natasha Salinas (Salinas, 2019) e, Eduardo Jordão e Maurício Ribeiro (Jordão; Ribeiro, 2017).

31 É claro que para ser positiva essa característica precisa de ações específicas vindas da Administração Pública: constante aperfeiçoamento do agente público, bem como o desenvolvimento de medidas

A concentração das funções de governança em uma autoridade nacional facilita a coordenação entre os diversos setores que formam a rede de atores envolvidos no tema, podendo contribuir para a diminuição da fragmentação existente e harmonização do estoque regulatório. Uma Agência Nacional de Cibersegurança poderia, assim, assumir a atribuição de coordenar os diversos atores que formam esse ecossistema e atuar como ponto central de comunicação entre eles, atendendo à necessidade de um canal para o compartilhamento de informações sobre riscos cibernéticos e mediação para a celebração de acordos de cooperação ou outros instrumentos normativos conjuntos quando o tema perpassar por mais de um setor.

É interessante mencionar que a Lei Geral das Agências (Lei nº 13.848/2019) prevê instrumentos de cooperação e coordenação entre agências e órgãos da administração pública (artigos 25 a 30), tais como a realização de acordos de cooperação, edição normativa em conjunto, criação de comitês para intercâmbio de experiências, sendo esses alguns exemplos que podem ser ampliados pela lei-quadro de regência no caso de se optar por uma futura agência de cibersegurança.

Não se ignoram, por outro lado, os desafios desse desenho institucional. Dois desafios gerais que costumam ser mencionados são o fenômeno da captura e a manutenção da independência financeira. A literatura aponta que a captura de uma agência ocorre quando esta, encarregada de proteger o interesse público, passa a se identificar com a indústria regulada, defendendo seus interesses em detrimento daquele (Stigler, 1971). Contudo, a evolução dos estudos empíricos para aplicação dessa teoria demonstrou que existem muitos outros fatores que precisam ser considerados antes de se afirmar a ocorrência da captura do regulador.

Becker (1983), por exemplo, ressalta que a teoria da captura deve ser entendida de forma dinâmica. Isso porque, em um ambiente onde diversos agentes atuam, o esforço de um grupo para influenciar políticas públicas a seu favor tende a gerar reações por parte de outros grupos que se sintam prejudicados por eventual influência. Por outro lado, Bernstein (1966) observa que os ciclos de vida de uma agência importam para a ocorrência da captura, sendo as mais novas menos suscetíveis de serem capturadas

destinadas a atrair a permanência desse funcionário junto ao Administração, evitando, com isso, o esvaziamento da Agência.

por existir um grande vigor em servir o interesse público. Já Levy e Spiller (1994) apontam que as instituições de um país, desde que sólidas, também se importam e podem se contrapor aos interesses da indústria. Sem a pretensão de esgotar os contrapontos realizados à teoria da captura, os argumentos apresentados, se não a enfraquecem, tornam-na mais complexa de ser observada na realidade.

A segunda dificuldade seria a manutenção da independência financeira da Agência, ou seja, a disponibilidade de recursos para que se possa criar e gerenciar uma entidade com pessoal qualificado e estrutura administrativa robusta para o desenvolvimento de suas atividades. Além da previsão orçamentária, as taxas regulatórias aparecem como uma alternativa, em razão do exercício do poder de polícia pelas Agências Reguladoras, especialmente por ordenarem a vida econômica e social ao promover a segurança cibernética. Apesar de não serem medidas populares (Holanda; Garcia, 2023), é essencial garantir a independência financeira de fato, sem depender de transferências ou nomeações sujeitas ao controle do processo político.

A autonomia orçamentária vem sofrendo limitações, visto que, na prática, em razão do princípio da unicidade orçamentária, o Executivo ou os outros Poderes podem impor contingenciamentos ao orçamento inicialmente proposto (Aragão, 2013, p. 352-354), de modo que é possível restringir o controle e atuação técnica das agências. Conforme esclarecido por Jordão e Ribeiro (2017, p. 187-188), esse princípio tem sido interpretado como exigência de que todos os recursos arrecadados pela agência voltem para a conta única da União, restando dependentes de realocação para retornar à agência.

Destaca-se, todavia, a necessidade de maiores reflexões a respeito da relação custo/benefício desta escolha[32] e considerações políticas relacionadas à implementação desse tipo de arranjo – o que foge do escopo deste trabalho. Sabe-se que a criação de uma agência demanda recursos financeiros para a implementação de estrutura, aquisição de equipamentos e contratação de pessoal qualificado, além do tempo necessário para o pleno funcionamento institucional. Considerando as restrições orçamentárias e a necessidade de otimização dos recursos públicos, uma alternativa mais

32 Apesar de se considerar o tema importante para desenvolvimento, foge do escopo deste trabalho uma análise econômica sobre a escolha do arranjo institucional a ser feito.

viável seria aproveitar estruturas institucionais já existentes que possuam competências correlatas ou que possam ser adaptadas para absorver as novas atribuições.

Dessa forma, seja qual for o arranjo adotado, é preciso que ele possua funções regulatórias – atividade normativa, fiscalizadora, sancionatória – e funções inerentes à governança, com destaque para a coordenação, cooperação e comunicação.

2.1.3 A Agência Nacional de Cibersegurança como coordenadora de um Sistema Nacional de Cibersegurança

A criação de uma Agência Nacional de Cibersegurança representa um avanço fundamental para a governança da segurança cibernética no Brasil, refletindo tendências internacionais e respondendo à crescente complexidade dos riscos digitais que permeiam todos os setores da sociedade (Belli *et al.*, 2023b; Belli; Goldoni; Karina, 2023). Como destacamos na subseção precedente, a criação de uma Agência Nacional de Cibersegurança deveria ser acompanhada, e fortalecida, pelo estabelecimento de um Sistema Nacional de Cibersegurança.

De um lado, a Agência Nacional de Cibersegurança, concebida como órgão central de tal sistema da governança da Política Nacional de Cibersegurança, assumiria um papel multifacetado, abrangendo competências normativas, fiscalizatórias e sancionatórias, além de atribuições de coordenação, de certificação, de resposta a incidentes e de representação internacional. Sua atuação é estratégica para garantir a integridade, a resiliência e a confiança no espaço cibernético brasileiro, especialmente diante do aumento exponencial de ameaças, da sofisticação dos ataques e da interdependência das infraestruturas críticas.

A criação de um Sistema Nacional de Cibersegurança deve ser vista como essencial para estabelecer um arranjo institucional e colaborativo destinado a valorizar, reforçar e promover a coordenação. Entre seus objetivos fundamentais, deveriam estar a integração e a articulação entre os diversos atores públicos e privados, bem como a promoção da harmonização normativa e da colaboração efetiva entre seus integrantes nos temas de cibersegurança.

Para que tal sistema seja participativo, inclusivo e efetivo, é essencial que sejam incluídos nele os principais órgãos regulatórios setoriais que tenham competência para a cibersegurança, o que inclui agências reguladoras setoriais e outros órgãos federais, estaduais, distritais e municipais que atuam na promoção de cibersegurança, além de organizações públicas e privadas com pertinência temática.

Nesse sentido, para garantir o diálogo permanente, cooperação e coordenação no sistema, observa-se a necessidade da estruturação de um canal permanente para a fluência da comunicação e da realização de ações conjuntas, como a instituição de um Conselho de Reguladores de Cibersegurança.

Esse Conselho funcionaria como um fórum permanente coordenado pela Agência Nacional de Cibersegurança, no âmbito do Sistema Nacional de Cibersegurança, para facilitar a definição de diretrizes de atuação conjunta, a produção normativa colaborativa e a celebração de acordos de cooperação e outros instrumentos formais para a realização de ações integradas em cibersegurança. O papel de um Conselho de Reguladores de Cibersegurança seria, portanto, de potencializar essa função de coordenação e gestão de riscos.

Como órgão central do Sistema, a Agência Nacional de Cibersegurança deveria, portanto, coordenar a atuação de órgãos e entidades, públicos e privados, promovendo a integração e a colaboração entre os diversos atores envolvidos na proteção do ciberespaço. Nesse contexto, a Agência deveria atuar em total sinergia com os CSIRTs, em coordenação da Rede Nacional de Gestão de Incidentes de Cibersegurança (ReGIC) e em parceria com outros centros nacionais e internacionais, fortalecendo a capacidade de resposta do país frente a incidentes de grande impacto.

Para alcançar uma cooperação e coordenação eficaz, a Agência deveria estabelecer protocolos e canais de comunicação seguros com setores de infraestruturas críticas e serviços essenciais, viabilizando o compartilhamento de informações sensíveis e a adoção de medidas rápidas e eficazes em situações de risco. Além disso, fomentar o desenvolvimento de capacidades, mecanismos, processos e produtos de cibersegurança nos setores público e privado, inclusive por meio de parcerias público-privadas, estimulando a inovação e a resiliência do ecossistema nacional (Belli *et al.*, 2023a).

Por fim, uma função essencial da Agência seria o desenvolvimento da cultura de cibersegurança, ou seja, a integração pelo tecido social da im-

portância da cibersegurança e da capacidade de lidar com ameaças. Nesse sentido, como será destacado na seção 2.5, a literacia digital é o alicerce da cibersegurança e da soberania digital e, para que essa literacia seja fortalecida, é essencial que a Agência seja também promotora de ações de educação, formação e capacitação, considerando as necessidades e vulnerabilidades de diferentes grupos populacionais.

Dessa forma, a Agência Nacional de Cibersegurança desempenharia funções estratégicas e transversais, sendo o pilar central da Política Nacional de Cibersegurança. Seu fortalecimento por meio de um Sistema Nacional de Cibersegurança estruturado e colaborativo é condição indispensável para que o Brasil possa enfrentar os desafios existentes, proteger seus ativos digitais e garantir a soberania digital (Belli *et al.*, 2023b).

Diante da complexidade dos desafios impostos pela cibersegurança, conforme já explicitado, a entidade responsável pelas iniciativas de governança nesse campo deve articular-se de forma integrada com os demais atores que compõem o ecossistema nacional de cibersegurança. Nesse sentido, merecem destaque estruturas como os *Computer Security Incident Response Teams* (CSIRTs) e os *Information Sharing and Analysis Centers* (ISACs), que, embora não detenham funções regulatórias, desempenham papel estratégico na detecção, análise e resposta a incidentes, bem como no compartilhamento de informações críticas. Por essa razão, nas próximas subseções serão examinados esses dois atores, com o objetivo de compreender seu funcionamento, suas atribuições e as interfaces que mantêm com a governança da cibersegurança.

2.1.4 O papel e a estrutura dos Grupos de Resposta a Incidentes de Segurança de Computadores - "CSIRTs"

A gestão de crises ocupa posição central nas estratégias nacionais e organizacionais de segurança cibernética, sendo os Grupos de Resposta a Incidentes de Segurança de Computadores ou *Computer Security Incident Response Teams* (CSIRTs) os agentes operacionais fundamentais para a contenção e mitigação de ameaças digitais em ambientes cada vez mais complexos e interconectados. A compreensão do papel, da estrutura e das atribuições desses grupos revela-se indispensável para o fortalecimento da

cibersegurança e da resiliência cibernética, sobretudo na perspectiva da definição de um mecanismo de governança eficaz.

Um CSIRT é uma organização formalmente constituída, ou eventualmente um grupo *ad hoc*, responsável por receber, analisar e responder a notificações e atividades relacionadas a incidentes de segurança em sistemas computacionais e redes de computadores (European Union Agency for Cybersecurity, 2024; Internet Governance Forum, 2015). O tipo de ativo digital ou comunidade atendida por um CSIRT pode variar desde uma única organização, como uma empresa, universidade ou órgão governamental, até comunidades mais amplas, como países inteiros, redes de pesquisa ou grupos de clientes que contratam seus serviços.

Do ponto de vista jurídico, a constituição de um CSIRT deve estar ancorada em um arcabouço normativo que confira segurança jurídica para sua atuação. A título de exemplo, existem leis, como a LGPD, normas de responsabilidade civil e normas processuais criminais no Brasil que são de importante conhecimento para a equipe. Este ponto é particularmente relevante no que concerne à coleta, tratamento e compartilhamento de informações – tipicamente sensíveis – relativas a incidentes, principalmente nos casos de notificação compulsória. Nesses casos, é interessante que os CSIRT atuem em colaboração com áreas jurídicas e de *compliance* para garantir que as notificações legais/regulatórias sejam feitas no prazo e formato exigidos.

Os CSIRTs desempenham um papel estratégico na governança da segurança cibernética, atuando como ponte entre a resposta técnica imediata e a gestão política e institucional das crises. Assim, sua missão transcende a simples resolução de incidentes, incluindo a promoção da resiliência do ecossistema digital por meio da antecipação de ameaças, aconselhamento em políticas públicas e coordenação de recursos durante crises simultâneas (Internet Governance Forum, 2015).

Na prática, os CSIRTs atuam na identificação proativa de vulnerabilidades e ameaças emergentes, por meio de monitoramento contínuo de fontes diversas, como fóruns clandestinos na Internet e bases de dados de vulnerabilidades. Essa atividade de monitoramento, também conhecida como "*horizon scanning*", permite a antecipação de ataques e a preparação de respostas adequadas. Além disso, os CSIRTs exercem função de mediação entre os aspectos técnicos dos incidentes e as necessidades regulatórias

e políticas, traduzindo dados técnicos em recomendações para reformas normativas e estratégias de prevenção.

A operacionalização dessas funções exige um modelo estruturado de resposta que, conforme o padrão internacional, se organiza em três níveis interdependentes: o primeiro nível é dedicado à triagem e detecção, utilizando ferramentas como sistemas de gerenciamento de eventos e informações de segurança (SIEM), redes *honeypot* e inteligência artificial para identificar anomalias[33] (Belli, 2025c); o segundo nível concentra-se na contenção e erradicação, aplicando técnicas forenses digitais, isolamento de *malwares* e gerenciamento de atualizações (*patches*); e o terceiro nível abrange a recuperação e a análise pós-incidente, com foco na continuidade dos negócios e na incorporação das lições aprendidas para aprimorar a resiliência futura (Internet Governance Forum, 2015).

Exemplos recentes ilustram a eficácia desse modelo. Durante os ataques de negação distribuída de serviço (DDoS) que atingiram infraestruturas financeiras europeias em 2024, os CSIRTs conseguiram detectar padrões anômalos em poucos minutos, neutralizar a maior parte dos nós maliciosos da *botnet* e implementar melhorias técnicas nos sistemas afetados, como a adoção de novos protocolos de criptografia (European Union Agency for Cybersecurity, 2024).

Pode-se considerar que um dos fatores essenciais para o sucesso dos CSIRTs é o conhecimento do setor ou das entidades em que atuam, aliado à confiança que conseguem estabelecer com essas organizações. Esses elementos também explicam a diversidade estrutural dos CSIRTs, que tendem a se adaptar às particularidades das entidades cuja cibersegurança são responsáveis por proteger.

Assim, apesar da existência de boas práticas sobre a maneira de se estruturar um CSIRTs, a estrutura organizacional destas entidades não é padronizada e pode variar conforme as características da organização ou do setor mantenedor, os recursos disponíveis e a comunidade atendida. Alguns CSIRTs estão inseridos em departamentos de Tecnologia da Informação ou Segurança da Informação, outros podem integrar áreas de auditoria, segurança física ou até atuar como unidades independentes. In-

33 Como destacaremos na seção 2.7, o uso defensivo da IA desempenha um papel cada dia mais estratégico para suportar a implementação de medidas efetivas de cibersegurança e ciberdefesa.

dependentemente da localização, é imprescindível que o CSIRT conte com o apoio institucional da alta administração, garantindo-lhe autoridade para executar suas atividades e acesso aos recursos necessários (Internet Governance Forum, 2015).

Os membros de um CSIRT devem possuir um conjunto diversificado de competências técnicas e interpessoais. Entre as funções essenciais, destacam-se a liderança e coordenação da equipe, a triagem inicial dos incidentes, a análise aprofundada dos artefatos digitais, o tratamento e mitigação dos incidentes, o acompanhamento de vulnerabilidades e a capacitação contínua da equipe e da comunidade atendida. A composição da equipe geralmente reflete as necessidades específicas da organização e o perfil dos serviços oferecidos. Por exemplo, um CSIRT que atende uma instituição financeira pode demandar especialistas em segurança de sistemas bancários e conformidade regulatória, enquanto um CSIRT acadêmico pode focar em proteção de redes de pesquisa e educação.

Por fim, é importante frisar que as ações dos CSIRTs podem ser classificadas em duas grandes categorias: reativas e proativas. As atividades reativas englobam o tratamento de incidentes propriamente dito, que compreende a recepção de notificações, análise detalhada, resposta e mitigação e compartilhamento de informações e lições aprendidas. A recepção centralizada das notificações permite a coleta e correlação de dados, facilitando a identificação de tendências e padrões de ataques, o que contribui para o aprimoramento das estratégias preventivas (European Union Agency for Cybersecurity, 2024).

A análise dos incidentes envolve a avaliação do escopo, da gravidade e da ameaça representada, bem como a pesquisa de estratégias eficazes para erradicação e recuperação. A resposta pode variar desde a emissão de recomendações técnicas para os responsáveis pelos sistemas afetados até a implementação direta de medidas corretivas, dependendo da autoridade e dos recursos do CSIRT. A disseminação de alertas e boletins técnicos para a comunidade atendida é parte fundamental do processo, promovendo a conscientização e a preparação coletiva.

Paralelamente, os CSIRTs desenvolvem atividades proativas que visam prevenir incidentes e reduzir o tempo de resposta quando eles ocorrem. Essas ações incluem treinamentos de conscientização em segurança da informação, realização de testes de intrusão (*penetration testing*), análise de

vulnerabilidades, desenvolvimento de documentação técnica e políticas de segurança, além da participação em projetos de melhoria contínua dos sistemas. Essas iniciativas são comparáveis às ações preventivas de uma brigada contra incêndio, que não apenas apaga incêndios, mas também promove campanhas educativas e inspeções regulares para evitar sinistros.

Neste contexto, o papel dos CSIRTs reflete a complexidade crescente do ambiente cibernético e a necessidade de respostas integradas que articulem aspectos técnicos, jurídicos e organizacionais. A importância desses atores no ecossistema da cibersegurança é fundamental para compreender que sua atuação deve ir além da resposta técnica para assumir uma posição estratégica na governança. Essa transformação possibilita uma colaboração mais efetiva entre reguladores e operadores, promovendo uma atuação conjunta e eficaz diante dos desafios cibernéticos.

2.1.5 O papel e a estrutura dos Centros de Análise e Compartilhamento de Informações "ISACs"

Os Centros de Análise e Compartilhamento de Informações, conhecidos como ISACs (*Information Sharing and Analysis Centers*), são estruturas organizacionais destinadas à promoção da cooperação, do intercâmbio e da análise conjunta de informações relacionadas à segurança cibernética para os seus associados (GSI, 2025a, art. 7º e 8º, I, b). Conforme estabelecido pela Portaria nº 148, de abril de 2025, do Gabinete de Segurança Institucional da Presidência da República (GSI/PR), que institui a Diretriz de Estímulo à Criação de ISACs, a finalidade primordial é fortalecer a resiliência cibernética nacional por meio da coordenação e do compartilhamento de dados sobre ameaças, vulnerabilidades e incidentes cibernéticos.

Atuando como plataformas colaborativas, os ISACs reúnem entidades públicas, privadas e acadêmicas, facilitando a troca de informações estratégicas e operacionais com o objetivo de prevenir, detectar e responder de forma coordenada a ataques cibernéticos (European Network and Information Security Agency., 2017; GSI, 2025a, art. 8º, I, a-b). Entre suas responsabilidades destacam-se a gestão de compartilhamento seguro de informações, a garantia da confidencialidade dos dados trocados e a promoção de uma cultura de segurança entre os participantes.

Nesse contexto, os ISACs funcionam como hubs de inteligência estratégica, facilitando a detecção precoce de ameaças, a disseminação de alertas e a implementação de contramedidas colaborativas. Tais ações ajudam a reduzir significativamente o tempo de detecção e resposta a incidentes (Digi Americas Alliance, 2025). Também lhes cabe fomentar a capacitação e a conscientização dos seus membros, além de estabelecer políticas internas claras para o compartilhamento e tratamento das informações.

Essa inteligência compartilhada permite transformar eventos isolados em alertas preventivos para todo o ecossistema setorial, fortalecendo a capacidade de reação coordenada, aspecto relevante em países de dimensões continentais e com setores compostos por um grande número de atores, como o Brasil.

Portanto, a articulação entre os membros de um dado setor por meio dos ISACs não apenas permite a identificação antecipada de ameaças emergentes, mas também viabiliza a disseminação de boas práticas, a harmonização de procedimentos e a mitigação de riscos cibernéticos. Nesse sentido, a adoção da Portaria nº 148/2025 reflete o reconhecimento institucional dos ISACs como instrumentos estratégicos para a governança da cibersegurança no Brasil, integrando esforços de múltiplos setores e promovendo uma resposta coordenada e eficaz às ameaças cibernéticas que transcendem fronteiras institucionais e setoriais.

Em termos operacionais, os ISACs geralmente contam com capacidades técnicas avançadas para a coleta, processamento, análise e disseminação de dados sobre ameaças cibernéticas, seguindo o ciclo de vida da inteligência de ameaças (European Network and Information Security Agency, 2017). Esse ciclo inclui a contextualização de indicadores de comprometimento e a automação das respostas por meio da integração com plataformas de inteligência de ameaças, sistemas de gerenciamento de eventos e informações de segurança (SIEM), além de ferramentas de orquestração, automação e resposta (Digi Americas Alliance, 2025).

Quanto à sua estrutura organizacional, os ISACs são normalmente segmentados por setores econômicos (como finança, transportes ou telecomunicações), domínios técnicos (como saúde ou educação) ou áreas geográficas (como regiões ou consórcios municipais). Essa segmentação permite maior precisão na contextualização de ameaças e maior eficácia

das respostas. Ademais, destaca-se o potencial papel dos ISACs na implementação prática da regulação setorial sobre cibersegurança.

A implementação de ISACs, contudo, não está isenta de desafios. Dentre os principais, destaca-se a necessidade de estabelecer e manter a confiança mútua entre os participantes, essencial para o compartilhamento aberto e tempestivo de informações (GSI, 2025a, art. 8o, III). Também se impõem obstáculos relacionados à proteção de dados e ao sigilo empresarial, bem como a necessidade de harmonização de padrões técnicos e operacionais para assegurar a interoperabilidade entre sistemas e organizações. Ademais, a escassez de profissionais qualificados e a constante evolução das ameaças cibernéticas exigem investimentos contínuos em capacitação e inovação tecnológica.

A próxima seção ilustra a complexidade normativa e multissetorial existente em cibersegurança e a consequente necessidade de se criar um sistema de cibersegurança coordenado por um arranjo institucional nacional. Os marcos regulatórios existentes em setores econômicos diversos serão analisados. Essa análise possibilita a percepção sobre a necessidade da função coordenatória defendida nesta seção.

2.2 Regulação setorial existente em cibersegurança

Embora o Brasil ainda esteja no processo de elaboração de um arcabouço normativo para regulação em cibersegurança, quando o Brasil promulgou a Política Nacional de Cibersegurança, em dezembro de 2023, e a Estratégia Nacional de Cibersegurança, em agosto de 2025, alguns setores já possuíam regulações específicas com obrigações de cibersegurança para as empresas que neles operam.

No que se refere aos órgãos reguladores independentes, verificou-se, conforme pode ser observado no Quadro 2 apresentado nesta subseção, que nem todas as agências existentes no Brasil regulam o setor que atua na área de cibersegurança. Entre as que já emitiram regulações específicas sobre cibersegurança, destacam-se a Agência Nacional de Telecomunicações (ANATEL) e a Agência Nacional de Energia Elétrica (ANEEL). Outros órgãos reguladores, como o Banco Central do Brasil (BCB), a Comissão de Valores Monetários (CVM), a SUSEP (Superintendência de Seguros Priva-

dos) e a Secretaria de Prêmios e Apostas do Ministério da Fazenda (SPA), também implementaram regulações no setor.

A Agência Nacional de Transportes Terrestres (ANTT), embora não tenha uma regulação específica sobre o tema, possui normas dispersas em seu estoque regulatório com obrigações aos regulados que podem ser inferidas como relacionadas à segurança cibernética, embora indiretas[34]. Outros reguladores, como a Agência Nacional de Aviação (ANAC) e a Agência Nacional de Saúde Suplementar (ANS), regulamentam padrões para registro, guarda ou compartilhamento de informações eletrônicas pelos regulados. Outra abordagem adotada é a regulação por determinadas categorias de regulados, de forma contextualizada, como a adotada por reguladores como a Agência Nacional de Vigilância Sanitária (Anvisa), Agência Nacional de Transportes Aquaviários (ANTAQ) e Agência Nacional do Cinema (ANCINE).

Por fim, a Autoridade Nacional de Proteção de Dados (ANPD), autarquia especial criada para emitir regulações sobre proteção de dados pessoais, não possui regulação específica sobre cibersegurança, porém lançou um guia (não vinculante) sobre segurança da informação para agentes de tratamento de pequeno porte[35] e um Regulamento de Comunicação de Incidente de Segurança.[36]

As informações que serão discutidas nesta seção foram compiladas em um quadro-resumo disponível a seguir. Ainda, foi disponibilizado um quadro completo com a respectiva fundamentação legal em um repositório on-line[37]. A construção adotou uma abordagem qualitativa, baseada na interpretação dos dispositivos previstos nas resoluções de cada entidade. Para a investigação da regulação vigente, como parâmetros de seleção foram considerados os setores que possuem autoridades com poder regulatório, sejam agência reguladora, autarquia ou órgão, desde que no âmbito

34 Por conta da peculiaridade no estoque regulatório da ANTT, tais obrigações inferíveis foram compiladas para consulta no Anexo 3 deste livro.

35 O leitor pode consultar a seção 2.3 sobre Segurança da informação para maior aprofundamento deste ponto.

36 Consideramos pelo menos peculiar a escolha da ANPD de regular somente a comunicação do incidente de segurança e não definir obrigações para prevenir a ocorrência de incidentes.

37 MEDEIROS, Breno Pauli; COUTO, Natalia; BELLI, Luca; *et al*. Panorama da Regulação de Cibersegurança Federal. Disponível em: https://hdl.handle.net/10438.3/FK2/I88DAP.

federal. Isso significa que foram mapeadas entidades com competência para expedir normas vinculantes para os entes regulados, bem como capacidade de fiscalização e sanção em caso de descumprimento.

Delimitado esse critério, foi realizada uma busca por disposições normativas específicas relacionadas à "cibersegurança", "segurança cibernética" e "segurança da informação" nos estoques regulatórios disponíveis nos sites oficiais das agências reguladoras e dos órgãos selecionados. É importante destacar que as normas pesquisadas se relacionaram àquelas voltadas para o setor regulado, e não normas voltadas a sua estrutura interna.[38]

Os documentos normativos obtidos foram, então, analisados quanto às obrigações impostas, sendo os dados organizados no quadro comparativo a seguir.[39] Deve ser ressaltado que foram excluídos deste quadro-resumo os seguintes órgãos: *i)* ANA; *ii)* ANM; *iii)* PREVIC - Superintendência Nacional de Previdência Complementar; *iv)* MEC - Ministério da Educação; *v)* ANTT (Ver Anexo B); *vi)* CNEN - Comissão Nacional de Energia Nuclear (Resolução CD nº 329/2024).

Esta exclusão decorreu da ausência de normas ou obrigações de cibersegurança voltada para seus regulados (caso da ANA, ANM, PREVIC e MEC), da falta de acesso público à norma (caso do CNEN), ou ainda da par-

38 É interessante pontuar que, no que se refere a normas internas de cibersegurança, isto é, normas que servem para estruturar a política interna do órgão federal foram mapeadas as seguintes regulamentações: *i)* Resolução nº 253/2025 (ANA); *ii)* Instrução Normativa nº 128/2018 com redação dada pela Instrução Normativa nº 173 de 2021 (ANAC); *iii)* Resolução nº17/2021 (ANATEL); *iv)* Portaria n.º 589-E/ 2022 (ANCINE); *v)* Resolução nº 6.143/2019 (ANEEL); *vi)* Resolução nº 206/2025 (ANM); *vii)* Portaria nº 102 (ANP); *viii)* Resolução nº 62/2015 e atualizada pela Resolução nº 81/ 2023 (ANS); *ix)* Portaria nº 423/2022 (ANTAQ); *x)* Resoluções nº 6.029/2023 e nº 6.045/2024 (ANTT); *xi)* Portaria n.º 1.440/2018 atualizada pela Portaria n.º 72/2023 (ANVISA); *xii)* Resolução nº 45/2024 (SUSEP); *xiii)* Portaria nº 155/2021 (CVM); *xiv)* Resolução nº 115/2021 atualizada pela Resolução nº 287/2023 (BCB); *xv)* Portaria nº 11/2021 (CNEM); *xvi)* Portaria nº 495/2022 (MEC); e *xvii)* Portaria nº 295/2023 (PREVIC).

39 As colunas do quadro baseiam-se na análise dos seguintes documentos: a) BCB (Resolução nº 4.893/21 e Resolução nº 454/2025); b) CVM - (Instrução normativa nº 35/2021, com as alterações 134/22 e 179/23); c) ANATEL (Resolução nº 740/2020 e Resolução nº 767/2024); d) ANEEL (Resolução nº 964/2021); e) SUSEP (Circular SUSEP nº 638/2021); f) Secretaria de Prêmios e Apostas do Ministério da Fazenda (Portaria SPA/MF 722/2024); g e h) ANPD (Resolução nº 15/2024 e GUIA ANPD SI para Agentes de Tratamento de Pequeno Porte - v.1.0); i) ANTAQ Resolução nº 53/2020 - Item 2.10 e "Minuta PSP"); j) ANAC (Resolução nº 458/2017 e RBAC Nº 108); k) ANVISA (RDC n.º 654/2022, RDC n.º 848/2024, RDC nº 657/2022 e IN 134/2022); l) ANS (RN 501/2022, RN 443/2019 e Padrão TISS); m) ANCINE (IN 123/2015); n) ANP (Manual de Comunicação de Incidentes da ANP/ 2024).

ticularidade na forma de regular o assunto pela ANTT, como já mencionado. Tais órgãos constarão apenas no quadro inserido no repositório on-line.

Quadro 3 - Resumo dos quesitos

Obrigações	Presente na norma setorial	Ausente na norma setorial
1. Há obrigação do setor regulado estabelecer políticas de segurança cibernética (ou "segurança da informação")?	ANATEL, ANEEL, ANTAQ, Banco Central do Brasil, CVM, SUSEP	ANAC, ANCINE, ANP, ANPD, ANPD (Guia), ANS, ANVISA, SPA
2. Há obrigação de publicidade dessa política em linguagem compreensível no site dos atores regulados?	ANATEL, Banco Central do Brasil, CVM	ANAC, ANCINE, ANEEL, ANP, ANPD, ANPD (Guia), ANS, ANTAQ, ANVISA, SPA, SUSEP
3. A regulação estabelece como obrigação a criação de alguma "unidade", "equipe", "orgão" ou qualquer outra estrutura para governança (e "liderança")?	ANAC, ANATEL, ANEEL, Banco Central do Brasil	ANCINE, ANP, ANPD, ANPD (Guia), ANS, ANTAQ, ANVISA, CVM, SPA, SUSEP
4. É obrigatória a inclusão de controles ou procedimentos internos na política, destinados ao mapeamento dos riscos cibernéticos?	ANATEL, ANEEL, ANTAQ, Banco Central do Brasil, CVM, SPA	ANAC, ANCINE, ANP, ANPD, ANPD (Guia), ANS, ANVISA, SUSEP
5. É obrigatória a realização de monitoramento contínuo dos riscos cibernéticos mapeados?	ANAC, ANATEL, ANVISA, Banco Central do Brasil, CVM, SPA	ANCINE, ANEEL, ANP, ANPD, ANPD (Guia), ANS, ANTAQ, SUSEP
6. É obrigatória a inclusão de controles ou procedimentos internos na política, destinados à identificação dos dados?	Banco Central do Brasil, CVM	ANAC, ANATEL, ANCINE, ANEEL, ANP, ANPD, ANPD (Guia), ANS, ANTAQ, ANVISA, SPA, SUSEP
7. É obrigatória a inclusão de controles ou procedimentos internos na política, destinados a garantir a confidencialidade, a autenticidade, a integridade e a disponibilidade de dados e informações?	ANATEL, ANEEL, ANS, Banco Central do Brasil, CVM, SPA, SUSEP	ANAC, ANCINE, ANP, ANPD, ANPD (Guia), ANTAQ, ANVISA

Obrigações	Presente na norma setorial	Ausente na norma setorial
8. É obrigatória a manutenção de listas com softwares autorizados e não autorizados pela organização?	SPA	ANAC, ANATEL, ANCINE, ANEEL, ANP, ANPD, ANPD (Guia), ANS, ANTAQ, ANVISA, Banco Central do Brasil, CVM, SUSEP
9. É obrigatória a manutenção de listas com os hardwares da organização?	ANTAQ, SPA	ANAC, ANATEL, ANCINE, ANEEL, ANP, ANPD, ANPD (Guia), ANS, ANVISA, Banco Central do Brasil, CVM, SUSEP
10. É obrigatória a implementação de acesso controlado?	ANAC, ANPD (Guia), ANS, ANVISA, Banco Central do Brasil, CVM, SPA, SUSEP	ANATEL, ANCINE, ANEEL, ANP, ANPD, ANTAQ
11. É obrigatória a inclusão de controles ou procedimentos internos na política, destinados à classificação de dados e informações?	ANEEL, Banco Central do Brasil, CVM, SPA, SUSEP	ANAC, ANATEL, ANCINE, ANP, ANPD, ANPD (Guia), ANS, ANTAQ, ANVISA
12. É obrigatório identificar e implementar controles de segurança específicos relacionados aos dados pessoais?	ANATEL, ANPD (Guia), ANS	ANAC, ANCINE, ANEEL, ANP, ANPD, ANTAQ, ANVISA, Banco Central do Brasil, CVM, SPA, SUSEP
13. É obrigatória a capacidade de recuperação de dados?	ANAC, ANPD (Guia), ANTAQ, ANVISA, Banco Central do Brasil, CVM, SPA	ANATEL, ANCINE, ANEEL, ANP, ANPD, ANS, SUSEP
14. É obrigatória a previsão de medidas para reduzir a vulnerabilidade contra ataques cibernéticos da instituição, empresa, entidade ou órgão (com "avaliação e correções contínuas")? É obrigatória a previsão de medidas para reduzir vulnerabilidades?	ANATEL, ANEEL, ANPD (Guia), Banco Central do Brasil, CVM, SPA, SUSEP	ANAC, ANCINE, ANP, ANPD, ANS, ANTAQ, ANVISA

Obrigações	Presente na norma setorial	Ausente na norma setorial
15. É obrigatória a previsão de um plano de resposta a incidentes, definindo ações, recursos e responsabilidades no caso de um incidente?	ANATEL, ANEEL, ANTAQ, ANVISA, Banco Central do Brasil, CVM, SPA, SUSEP	ANAC, ANCINE, ANP, ANPD, ANPD (Guia), ANS
16. É obrigatória a adoção de controles e procedimentos internos para registro de incidentes cibernéticos?	ANEEL, ANPD, ANPD (Guia), ANTAQ, ANVISA, Banco Central do Brasil, CVM, SUSEP	ANAC, ANATEL, ANCINE, ANP, ANS, SPA
17. No intuito de manter melhorias contínuas, é obrigatória a revisão e a implementação de "lições aprendidas"?	ANEEL, Banco Central do Brasil, CVM	ANAC, ANATEL, ANCINE, ANP, ANPD, ANPD (Guia), ANS, ANTAQ, ANVISA, SPA, SUSEP
18. A regulação estabelece o dever de reportar incidentes ao órgão regulador?	ANATEL, ANCINE, ANEEL, ANP, ANPD, ANPD (Guia), Banco Central do Brasil, CVM, SUSEP	ANAC, ANS, ANTAQ, ANVISA, SPA
19. É obrigatória a criação de formas de participação em iniciativas para o compartilhamento de informações sobre ameaças, vulnerabilidades ou incidentes relevantes no setor?	ANATEL, ANEEL, Banco Central do Brasil, CVM, SUSEP	ANAC, ANCINE, ANP, ANPD, ANPD (Guia), ANS, ANTAQ, ANVISA, SPA
20. É obrigatória a inclusão de controles ou procedimentos internos na política, destinados à classificação dos incidentes de segurança?	ANEEL, Banco Central do Brasil, CVM, SUSEP	ANAC, ANCINE, ANP, ANPD, ANPD (Guia), ANS, ANTAQ, ANVISA, SPA
21. É obrigatória a realização de testes sobre o funcionamento do plano ou política de cibersegurança?	ANEEL, ANS, Banco Central do Brasil, CVM, SPA, SUSEP	ANAC, ANATEL, ANCINE, ANP, ANPD, ANPD (Guia), ANTAQ, ANVISA
22. É obrigatória a realização de algum tipo de avaliação para analisar a disponibilidade/dependência de fornecedores?	ANAC, ANATEL, SUSEP	ANCINE, ANEEL, ANP, ANPD, ANPD (Guia), ANS, ANTAQ, ANVISA, Banco Central do Brasil, CVM, SPA

Obrigações	Presente na norma setorial	Ausente na norma setorial
23. É obrigatória a realização de algum tipo de avaliação para analisar a conformidade legal de terceiros, relacionado à cibersegurança/segurança da informação ("gestão de contratos")?	ANATEL, ANPD (Guia), Banco Central do Brasil, CVM, SPA, SUSEP	ANAC, ANCINE, ANEEL, ANP, ANPD, ANS, ANTAQ, ANVISA
24. Há obrigação de avisar ao regulador sobre a contratação de serviço de terceiros (ex.: serviços de processamento e armazenamento na nuvem)?	ANTAQ, Banco Central do Brasil	ANAC, ANATEL, ANCINE, ANEEL, ANP, ANPD, ANPD (Guia), ANS, ANVISA, CVM, SPA, SUSEP
25. É obrigatória a inclusão de controles ou procedimentos internos na política, destinados ao usuário final do serviço como dever de conscientização?	ANATEL, ANEEL, Banco Central do Brasil, CVM	ANAC, ANCINE, ANP, ANPD, ANPD (Guia), ANS, ANTAQ, ANVISA, SPA, SUSEP
26. A regulação estabelece alguma sanção para o descumprimento de alguma das obrigações?	ANAC, ANATEL, ANPD, ANS, ANVISA, Banco Central do Brasil, CVM, SPA	ANCINE, ANEEL, ANP, ANPD (Guia), ANTAQ, SUSEP
27. A regulação prevê a obrigatoriedade de atualização da política?	ANATEL, ANEEL, ANPD (Guia), ANTAQ, Banco Central do Brasil	ANAC, ANCINE, ANP, ANPD, ANS, ANVISA, CVM, SPA, SUSEP
28. Auditoria externa ou do órgão regulador referente à implementação da política de segurança é obrigatória?	ANAC, ANATEL, Banco Central do Brasil, SPA, SUSEP	ANCINE, ANEEL, ANP, ANPD, ANPD (Guia), ANS, ANTAQ, ANVISA, CVM
29. Treinamento periódico/contínuo de funcionários	ANEEL, ANPD (Guia), Banco Central do Brasil, CVM, SUSEP	ANAC, ANATEL, ANCINE, ANP, ANPD, ANS, ANTAQ, ANVISA, SPA

Fonte: Elaboração própria.

As obrigações impostas pelas normas analisadas variam conforme o setor, mas estão alinhadas às boas práticas globalmente recomendadas mencionadas na subseção seguinte, que trata sobre a segurança da informação. Essas obrigações, que serviram de categorias para a análise, foram extraídas a partir da leitura dos próprios documentos normativos. De maneira geral,

pode-se afirmar que essas obrigações se inspiraram nos padrões ISO sobre segurança da informação,[40] particularmente no padrão ISO 27001.

Foram analisadas 29 obrigações impostas pelos reguladores. A verificação da presença ou ausência de cada obrigação na norma de determinada entidade resultou nos seguintes achados: de forma geral, observou-se que, entre os reguladores que estabeleceram ao menos uma obrigação relacionada à cibersegurança (14 entidades avaliadas), apenas cinco endereçaram metade das obrigações listadas (15 dentre os 29 itens).

Entre os 14 reguladores elencados, as obrigações mais exigidas entre eles foram:

Quadro 4 - Obrigações mais reguladas

Norma regulada	Frequência (entre 14 reguladores)
Previsão do dever de reportar incidentes ao órgão regulador	9 ocorrências
Obrigatoriedade de implementação de acesso controlado	8 ocorrências
Obrigatoriedade de um plano de incidentes, definindo ações, recursos e responsabilidades em caso de incidentes	8 ocorrências
Obrigatoriedade de adoção de controles e procedimentos internos para registro de incidentes cibernéticos	8 ocorrências
Previsão de sanções para o descumprimento de obrigações	8 ocorrências
Obrigatoriedade de inclusão, na política interna, de controles ou procedimentos internos na política destinados a garantir a confidencialidade, a autenticidade, a integridade e a disponibilidade de dados e informações	7 ocorrências
Obrigatoriedade de adoção de medidas para reduzir a vulnerabilidade contra ataques cibernéticos da instituição, empresa, entidade ou órgão, incluindo avaliação e correções contínuas	7 ocorrências

Fonte: Elaboração própria.

Por outro lado, as obrigações menos estabelecidas foram:

40 Este assunto será analisado detalhadamente na seção 2.3.

Quadro 5 - Obrigações menos reguladas

Norma regulada	Frequência (entre 14 reguladores)
Obrigatoriedade de manutenção de listas com softwares autorizados e não autorizados pela organização	1 ocorrência
Obrigatoriedade de inclusão, nas políticas internas, de controles ou procedimentos destinados à identificação dos dados	2 ocorrências
Obrigatoriedade de manutenção de listas com os hardwares da organização	2 ocorrências
Obrigação de informar ao regulador sobre a contratação de serviço de terceiros (por exemplo, serviços de processamento e armazenamento na nuvem)	2 ocorrências

Fonte: Elaboração própria.

O estabelecimento de uma política de cibersegurança é o primeiro passo; entretanto, considerando as constantes atualizações e transformações tecnológicas, é preciso que essas políticas sejam periodicamente revisadas e testadas. Contudo, em relação à revisão periódica, apenas BCB, ANATEL, ANEEL e o Guia Orientativo da ANPD preveem expressamente essa obrigação. A CVM, embora não estabeleça essa obrigação de forma literal, permite por interpretação conjunta dos artigos 41, II, com 45, V, "b" de seu regulamento, que se alcance tal determinação. Por outro lado, a realização de testes constitui obrigação nas normas do BCB, CVM, ANS, SUSEP, SPA e ANEEL.

Curiosamente, uma obrigação atendida por apenas quatro reguladores é a criação de uma "unidade", "equipe", "órgão" ou outra estrutura específica para governança de cibersegurança. Especificamente, o BCB exige das instituições financeiras a nomeação de um diretor dedicado à segurança cibernética. No caso da ANATEL, está prevista a obrigação para criação do Grupo Técnico de Segurança Cibernética e Gestão de Riscos de Infraestrutura Crítica (GT-Ciber). No setor elétrico, a ANEEL delega aos agentes a responsabilidade de estruturar suas próprias medidas de governança cibernética, sem especificar um órgão próprio para isso. Já a ANAC, em um escopo mais limitado, dispõe que, em sistemas de guarda e registro de informações, será necessário identificar a pessoa ou equipe que terá autoridade e responsabilidade geral pela integridade e segurança de tais sistemas.

A criação dessas estruturas é importante para que possam funcionar como ponto de contato nas ações de coordenação e cooperação entre os di-

versos atores operacionais, contribuindo para a prevenção, mitigação dos riscos e gestão de incidentes cibernéticos.

Quanto à obrigatoriedade de inclusão de controles ou procedimentos internos na política de cibersegurança voltados ao mapeamento de riscos cibernéticos, o BCB, a CVM, a SPA, a ANTAQ, a ANATEL e a ANEEL exigem tal mapeamento. Entre esses reguladores, com exceção da ANEEL e da ANTAQ, também é imposto o dever de monitoramento contínuo dos riscos mapeados, obrigação essencial considerando o caráter dinâmico de tais riscos. Neste ponto, é interessante destacar que o Guia da ANPD sobre agentes de tratamento de pequeno porte e a Resolução nº 15 da ANPD, relativa à comunicação de incidente de segurança, não trazem essa previsão.

No que diz respeito à obrigatoriedade de inclusão de controles e procedimentos destinados a garantir a confidencialidade, a autenticidade, a integridade e a disponibilidade de dados e informações, o BCB, a CVM, ANATEL, ANEEL, SPA, SUSEP e ANS exigem essa conduta dos regulados. Contudo, na especificação desses controles, a previsão de procedimentos internos destinados à identificação dos dados somente é prevista pelo BCB e pela CVM, enquanto BCB, CVM, SPA, SUSEP e ANEEL determinam também a obrigatoriedade de classificação dos dados.

A identificação de dados e a respectiva classificação são importantes padrões de proteção das informações. Um programa de governança maduro impõe a elaboração de um inventário dos dados tratados institucionalmente, o que permite identificar a criticidade e eventual necessidade de implementar controles de segurança mais ou menos robustos, específicos para as categorias identificadas.

No que se refere ao controle de acesso, que consiste em identificar os profissionais que devem efetivamente – em razão de seus cargos ou funções – operar determinadas bases de dados, BCB, CVM, SUSEP, SPA, Anac, ANVISA e ANS trazem essa obrigação de forma expressa. A ANATEL e ANEEL, embora não falem textualmente sobre tal exigência, possuem obrigações genéricas para adoção de padrões nacionais e internacionais de boas práticas, entre as quais o controle de acesso é comumente recomendado. A título de exemplo, pode-se citar a recomendação do *National Institute of Standards and Technology* (NIST), bem como o Guia de Segurança da Informação para agentes de tratamento de pequeno porte, que orienta a implementação de controle de acesso aos dados pessoais.

Outra obrigação importante no contexto de proteção de dados e informações, referenciada pelo BCB, CVM, SPA, ANTAQ, ANAC, ANVISA e ANS e pelo Guia Orientativo da ANPD, refere-se à capacidade de recuperação de dados. Essa obrigação é importante porque a perda de determinadas informações pode acarretar desde entraves administrativos até suspender por completo as atividades das instituições, a depender da base de dados afetada. Trata-se, portanto, de medida essencial para os planos de continuidade operacional principalmente no contexto de resposta a incidentes, como em ataques de *ransomware*.

Obrigações alusivas à manutenção de listas com softwares autorizados e não autorizados pela organização e à existência de inventário dos ativos digitais: somente a SPA exige um procedimento para mudanças sobre ativos e restrições sobre mudanças em softwares.

Quanto às ações para lidar com incidentes cibernéticos, foram analisadas a existência de obrigações sobre: (a) a adoção de medidas para reduzir vulnerabilidades contra ataques cibernéticos à instituição, empresa, entidade ou órgão; (b) a elaboração de um plano de resposta a incidentes, definindo ações, recursos e responsabilidades no caso de um incidente cibernético; (c) a adoção de controles e procedimentos internos para registros dos incidentes cibernéticos; (d) a existência do dever de reportar incidentes ao órgão regulador; (e) a classificação dos incidentes de segurança.

Quanto à obrigação de adotar medidas para redução de vulnerabilidades, BCB, CVM, ANATEL, ANEEL, SUSEP, SPA abordaram o assunto. O número de reguladores que exigem a elaboração de planos de resposta a incidentes, contudo, é maior (BCB, CVM, ANATEL, ANEEL, SUSEP, SPA, ANTAQ, ANVISA). O Guia de Segurança da Informação da ANPD, embora recomende que os agentes de tratamento de pequeno porte realizem gestão de vulnerabilidades, não menciona a elaboração de um plano de resposta. Tal omissão merece atenção, considerando que o conhecimento prévio de como responder a incidentes é uma etapa subsequente ao conhecimento das vulnerabilidades que podem afetar o negócio.

Quanto à adoção de controles e procedimentos internos para registros de incidentes cibernéticos, todas as normas do BCB, CVM, ANEEL, SUSEP, ANTAQ, ANPD (tanto em seu guia quanto em sua Resolução) e ANVISA trazem essa previsão expressa. Neste ponto, cabe reiterar que, embora a ANATEL não aborde diretamente essa obrigação, suas normas

determinam que as empresas reguladas adotem padrões nacionais e internacionais de boas práticas, diretriz que, indiretamente, pode incluir a implementação desses controles.

No que se refere ao dever de comunicação de incidentes cibernéticos ao regulador, trata-se da obrigação mais frequentemente prevista, sendo estabelecida por 9 dos 14 reguladores que possuem normas sobre cibersegurança. Tal exigência, inclusive, encontra respaldo no art. 48 da Lei Geral de Proteção de Dados Pessoais (LGPD), quando envolver dado pessoal. A CVM, além de exigir a comunicação ao órgão regulador, também traz a obrigação de informar os órgãos de administração das instituições. A ANTT, embora não trate expressamente do caso de reporte sobre incidentes cibernéticos ou de segurança da informação, exige a comunicação de incidentes nos casos graves de paralisia das operações dos regulados, o que poderia ser interpretado também como uma obrigação análoga.

A classificação de incidentes de segurança é uma medida necessária para a estruturação do modelo de resposta interna a incidentes, ação que envolve não somente profissionais focais para acionamento, mas medidas técnicas que devem ser acionadas imediatamente para não comprometer mais sistemas ou dados. Embora da relevância para a gestão dos riscos cibernéticos, somente o BCB, a CVM, a SUSEP e a ANEEL trazem essa previsão.

Ainda, buscando o aprimoramento da resposta a incidentes cibernéticos, destacam-se duas obrigações adicionais: *i)* revisão e implementação de lições aprendidas; *ii)* participação em iniciativas de compartilhamento de informações sobre ameaças, vulnerabilidades ou incidentes relevantes no setor. A primeira é exigida apenas pelo BCB, CVM e ANEEL, enquanto a segunda é prevista pelo BCB, CVM, SUSEP, ANATEL e ANEEL.

Outra obrigação relevante diz respeito à verificação de conformidade legal na contratação de terceiros, isto é, gestão de contratos, o BCB, a CVM, a ANATEL, a SUSEP, a SPA e o Guia Orientativo da ANPD estabelecem que há políticas de avaliação sobre os processos de segurança da informação de prestadores de serviço. O BCB acrescenta, ainda, o dever de comunicar a contratação de serviços relevantes de processamento, armazenamento de dados e de computação em nuvem para as instituições por ele autorizadas a funcionar.

Outra obrigação relevante é a avaliação pelos regulados sobre a disponibilidade e dependência de fornecedores que eventualmente sejam por

eles contratados. Essa medida visa identificar o grau de comprometimento desses parceiros em relação à proteção de dados e mapear e distribuir as responsabilidades da operação contratada. Sobre esse aspecto somente a ANATEL traz essa obrigação.

Alguns reguladores – BCB, CVM, ANATEL e ANEEL – ampliam suas preocupações para incluir os usuários ou consumidores, determinando que as políticas das entidades reguladas incorporem ações de conscientização, com o objetivo de fornecer informações sobre precauções na utilização de seus serviços ou produtos.

Todas essas obrigações, contudo, tornam-se menos eficazes sem treinamento periódico de colaboradores. A capacitação contínua constitui elemento estratégico para a gestão de riscos cibernéticos em programas de cibersegurança, conforme mencionado na subseção 2.5.2.4 deste livro. Tais iniciativas não apenas promovem conformidade normativa, mas fortalecem a primeira linha da defesa da organização ao atribuir aos colaboradores a responsabilidade de reconhecer ameaças cibernéticas, como *phishing* e falhas de senha, o que reduz a probabilidade de incidentes causados por erro humano. As Resoluções do BCB, CVM, ANEEL, SUSEP e Guia Orientativo da ANPD trazem obrigações nesse sentido.

Para finalizar, duas últimas análises são relevantes: *i)* a existência de mecanismos de fiscalização ou auditoria sobre a adoção das políticas pelo setor regulado; e *ii)* a previsão de sanção para o descumprimento de alguma dessas obrigações pelo regulador. Quanto à primeira obrigação, o BCB e ANATEL, SUSEP, SPA e ANAC trazem essa previsão. A ANEEL, embora não estabeleça essa obrigatoriedade de fiscalização, determina a existência de registros a serem disponibilizados sempre que solicitados. Quanto à segunda, as regulações que dispõem sobre cibersegurança do BCB, CVM, ANATEL, SPA, ANAC, ANVISA, ANS e a ANPD estabelecem previsão de sanção em caso de descumprimento.

Diante do levantamento realizado, constata-se que apenas um número restrito de entidades federais assumiu, até o momento, a iniciativa de regular diretamente aspectos relacionados à cibersegurança nos setores sob sua competência. Essa constatação evidencia uma lacuna regulatória significativa, o que enseja necessidade de um futuro arranjo institucional voltado à governança da cibersegurança no Brasil, seja para apoiar os regu-

ladores inertes sem expertise, seja para estabelecer padrões mínimos para os casos em que não houver regulador prévio determinado.

A nova estrutura de governança deverá operar de modo articulado com os diversos órgãos reguladores setoriais, promovendo um ambiente normativo harmônico. Para tanto, será necessário recorrer a instrumentos de coordenação regulatória, especialmente nos casos em que se identificarem sobreposições normativas ou competências concorrentes. Além disso, é essencial que a regulação setorial seja desenvolvida e implementada em sinergia com as informações prestadas pelas entidades de natureza técnica e setorial, os ISACs e CSIRTs, analisados na subseção precedente, que são entidades essenciais para o fortalecimento da cibersegurança e resiliência cibernética setorial.

A próxima subseção volta-se à análise da segurança da informação, com intuito de apresentar a complexidade temática e os possíveis âmbitos de alcance e proteção, focando no tratamento normativo nacional e nos mecanismos de harmonização dos modelos de governança da informação a serem implementados institucionalmente, sobretudo considerando a ubiquidade do ciberespaço.

2.3 Segurança da informação

Consoante o propósito do capítulo em explorar aqueles elementos que circundam a eventual abordagem nacional de cibersegurança de modo que seja robusta e que igualmente fortaleça a soberania digital nacional, essa seção se debruça sobre o fio condutor da cibersegurança: a segurança da informação. Portanto, a seção analisa tanto questões conceituais quanto regulatórias relativas aos dados e ao respectivo processamento pelos atores públicos, privados, nacionais e internacionais.

O tratamento de dados, sejam pessoais ou não, é uma atividade importante para a organização de atividades públicas e privadas. Sem olvidar os dados físicos, o aprofundamento do paradigma informático tem transformado o modo de se gerir negócios e governos e de se travar relações interpessoais, com a produção e o registro de informações em bancos de dados digitalizados compondo uma atividade central em quase qualquer processo gerencial ou produtivo.

De fato, a informação tem se consolidado como um ativo intangível em uma economia descrita por diversas denominações – economia da informação em rede (Benkler, 2006), capitalismo de informação (Fuchs, 2010), capitalismo de dados (Srnicek, 2017; West, 2019), capitalismo de vigilância (Zuboff, 2019a), capitalismo cognitivo e tecnofeudalismo (Colombini, 2023, em perspectiva crítica aos conceitos).

Esse tratamento da informação como ativo toma a forma tanto de direitos de propriedade intelectual sobre distintas formas de manifestação do conhecimento e da cultura, quanto a forma de controle sobre bases de dados úteis, por exemplo, para o aperfeiçoamento de sistemas algorítmicos, a produção de inteligência de negócios ou, mais recentemente, para a composição de modelos linguísticos destinados ao treinamento e aprimoramento de inteligências artificiais.

Para além de seus efeitos econômicos, a "datificação" da sociedade se evidencia no ímpeto de mensurar e traduzir em dados registrados em formato eletrônico todos os aspectos da realidade, inclusive o provimento de serviços públicos, a operacionalização da administração pública, o que pode incluir informações sobre o funcionamento das infraestruturas críticas e dos processos democráticos.

Conforme estabelecido na primeira seção deste trabalho, a informação é um dos possíveis objetos de referência que precisam ser protegidos dos riscos cibernéticos. Para garantir a disponibilidade, integridade, confiabilidade e autenticidade das informações, é preciso adotar ações que implementem segurança e controle nesses processos de tratamentos e nos ativos que permitem a fluência dessas informações, como os sistemas de software e as demais infraestruturas de hardware.

Nesse sentido, a proteção dos dados (pessoais ou não) e de todo o aparato (infraestrutura e sistemas) desenvolvido e pensado para garantir o fluxo de informação precisa ser protegida. Por isso, a segurança da informação é destacada neste trabalho como o elo central dos objetos de referência. As infraestruturas, críticas ou não, os bens de consumo, os serviços e sistemas operacionais serão enquadrados como ativo digital e, portanto, objeto de referência em cibersegurança, quando fizerem parte de redes e sistemas para fluência de informações digitais.

Figura 3 - Segurança da informação como elo central entre os objetos de referência da cibersegurança

Fonte: Elaboração própria

Em consonância com a lógica exposta e, portanto, corroborando com a centralidade sugerida e transversalidade do tema, a recente alteração da Política Nacional de Segurança da Informação (PNSI) brasileira, promovida pelo Decreto nº 12.572/2025 (Brasil, 2025), prescreve como alvos de proteção: os dados, os ativos de informação e os seus respectivos ambientes físicos e eletrônicos, os processos organizacionais dedicados a tais informações e as pessoas envolvidas em processos de tratamento e "ciclos de vida" dos dados (artigo 2º).

A atual Política Nacional de Cibersegurança – PNCiber, instituída com Decreto nº 11.856/2023, também se preocupa em proteger as informações ao estabelecer como objetivo "garantir a confidencialidade, a integridade, a autenticidade e a disponibilidade das soluções e dos dados utilizados para o processamento, o armazenamento e a transmissão eletrônica ou digital de informações" (Presidência da República, 2023b).

Reconhecida a importância da informação como ativo digital para a cibersegurança, passam-se às próximas subseções. Inicialmente, examina-se o tratamento normativo dedicado às informações pessoais; na sequência, analisam-se os demais instrumentos regulatórios aplicáveis à segurança da informação *lato sensu* (e, portanto, não pessoais) e, por fim, discutem-se os referenciais regulatórios aplicáveis à segurança da informação, como guias e procedimentos padrões internacionalmente aceitos e recomendados.

2.3.1 Segurança de dados pessoais no Brasil

Conforme mencionado, o termo "informação" abrange um amplo leque de (tipos) de dados. Muito além de um conceito legal bivalente, cuja referência é a definição legal do que se entende por dados pessoais (toda "informação relacionada a pessoa natural identificada ou identificável", conforme previsto no inciso I, do artigo 5º, da Lei Geral de Proteção de Dados - LGPD), de forma excludente, todo o universo das demais possibilidades, como aquelas acercas da própria organização. Em todos os cenários, porém, a depender da criticidade e exposição ao risco, serão classificadas nas corporações de modo a guiar a estruturação do futuro programa de governança interna (privada) e a implementação de medidas de segurança mais ou menos robustas.

Compreendidas essas noções introdutórias, e considerando uma abordagem centrada no indivíduo, exploram-se primeiro as problematizações referentes aos dados pessoais que, inclusive, detém o conjunto normativo mais relevante, como se justifica à frente, para, na subseção da sequência, seguir para as demais informações.

Dito isso, sublinha-se que a relevância normativa supracitada circunda os direitos à privacidade e à proteção dos dados pessoais. Ambos os direitos compõem, viabilizam e promovem a dignidade humana, bem como são instrumentos de defesa da democracia, na medida em que permitem o desenvolvimento da personalidade, a autodeterminação e a autonomia dos indivíduos enquanto cidadãos (Sauaia, 2018).

Pelo direito à privacidade protegem-se a intimidade, a vida privada, a honra e a imagem das pessoas (art. 5º, inciso X, da CRFB). Isso o caracteriza como um direito arquitetural (Bioni, 2019). O direito à proteção de dados pessoais, por sua vez, não possui essas multidimensões da esfera

pessoal. É procedimental, na medida em que protege as informações sobre determinado indivíduo de tratamentos que não respeitem as diretrizes mínimas preestabelecidas e positivadas nos mais variados territórios.

No Brasil, os direitos à privacidade e à proteção de dados têm assento na Constituição Federal de 1988 em uma série de direitos fundamentais. Um primeiro conjunto está relacionado aos direitos da personalidade e inclui a inviolabilidade da intimidade, da vida privada, da honra e da imagem (art. 5º, X); a inviolabilidade da propriedade (art. 5º, XI); e o sigilo das comunicações, correspondências, comunicações de dados e comunicações telefônicas (art. 5º, XII).

Em fevereiro de 2022, mediante promulgação da Emenda Constitucional n. 115, incluiu-se no artigo 5º da Constituição Federal o inciso LXXIX, tratando especificamente do direito à proteção de dados pessoais em qualquer meio, inclusive o digital. Para além deste, cumpre ressaltar o direito ao *habeas data*, inscrito no inciso LXXII, concernente ao direito de acessar informações pessoais contidas em bases de dados públicas ou de interesse público e de corrigi-las.

Em sede infraconstitucional, diversos instrumentos normativos poderiam ser citados que apresentam relevância para se desenhar um quadro da proteção de dados e segurança da informação no Brasil. Como referência mais ampla e de caráter normativo mais geral, cita-se, em termos de proteção de dados pessoais, a Lei Geral de Proteção de Dados (LGPD), que institui um regime geral de proteção de dados pessoais no Brasil baseado na autodeterminação informacional e na obrigação de segurança de dados desde a concepção. Esse regime implica a operacionalização do controle individual sobre dados pessoais a partir de critérios de garantia de direitos individuais e de mensuração e mitigação de riscos.

Ademais, normas como o Código de Defesa do Consumidor, a Lei de Acesso à Informação, a Lei do Habeas Data e o Marco Civil da Internet contêm provisões a respeito de privacidade e proteção de dados que precedem a LGPD e se mantêm incidentes ainda hoje sobre relações de processamento de dados pessoais.

No âmbito infralegal, sublinha-se a Resolução nº 15 da ANPD, que aprova o Regulamento de Comunicação de Incidente de Segurança. Conforme previsão expressa, conceitua-se incidente de segurança como qualquer evento atípico confirmado, atrelado à violação da confidencialidade,

integridade, disponibilidade e autenticidade da segurança de dados pessoais (inciso XII do art. 3º) (ANPD, 2024b).

Sendo ou não um incidente proveniente de uma ação criminosa, sempre que houver a possibilidade de ocasionar risco ou dano ao titular de dados, o fato deverá ser comunicado tanto à ANPD quanto aos titulares pelo controlador – pessoa física ou jurídica a quem compete as decisões acerca do tratamento de dados –, em regra, no prazo de três dias úteis (arts. 5º, inciso VI, da LGPD e 4º e 6º, *caput*, da Resolução nº 15 da ANPD (2024b).

A condicionante da obrigação legal é a possibilidade de o incidente de segurança gerar risco ou dano ao titular de dados. Portanto, a comunicação será necessária quando o incidente puder afetar significativamente interesses e direitos fundamentais dos titulares e, cumulativamente, envolver *i)* dados pessoais sensíveis; *ii)* dados de crianças, de adolescentes ou de idosos; *iii)* dados financeiros; *iv)* dados de autenticação em sistemas; *v)* dados protegidos por sigilo legal, judicial ou profissional; ou *vi)* dados em larga escala, compreendidos como aqueles que abrangem um número significativo de titulares, sem desconsiderar o volume de dados envolvidos, a periodicidade, a duração e a extensão geográfica de localização desses titulares (art. 5º da Resolução nº 15 da ANPD).

Esse reporte deverá ser realizado por meio de formulário eletrônico disponibilizado pela ANPD e contemplar a natureza e a categoria dos dados afetados; o número de titulares afetados, se possível, destacando o número de crianças, de adolescentes ou de idosos; quais foram as medidas técnicas e de segurança adotadas antes e após o incidente, respeitados os segredos de negócio ou industrial; quais os riscos de possíveis impactos aos titulares; a justificativa de demora, quando a comunicação for realizada fora do prazo legal; quais medidas foram ou serão adotadas para mitigar ou reverter os efeitos do incidente sobre os titulares; quando possível, determinar a data da ocorrência do incidente e a de conhecimento pelo controlador; as informações do encarregado pelo tratamento de dados[41] ou de quem represente o controlador, bem como do próprio controlador e, se for o caso, a declaração de que se trata de agente de tratamento de pequeno

41 O encarregado pelo tratamento de dados é a pessoa indicada pelo controlador e operador para atuar como canal de comunicação entre o controlador, os titulares dos dados e a Autoridade Nacional de Proteção de Dados (ANPD) (art. 5º, inciso VIII, da LGPD)

porte – também do operador, caso seja necessário; a descrição do incidente, relatando a causa principal sempre que possível identificar; e o total de titulares cujos dados são tratados na atividade vulnerada pelo incidente (art. 6º da Resolução nº 15 da ANPD).

As complementações das informações são autorizadas desde que fundamentadas e no prazo de vinte dias úteis após o envio da comunicação original. Ressalta-se que os atores de tratamento de pequeno porte têm a prerrogativa dos prazos contados em dobro (art. 14 da Resolução CD/ANPD nº 2/2022). Quando para o titular, os responsáveis pela comunicação deverão atentar-se tanto para a linguagem simples e de fácil compreensão quanto para o direcionamento no formato direto e individualizado (art. 9º, § 1º). Por fim, o registro do incidente de segurança, comunicável ou não, deverá ser mantido pelo prazo mínimo de cinco anos.

Dessa forma, observa-se que a ANPD estabelece procedimentos rigorosos para a comunicação de incidentes de segurança envolvendo dados pessoais, porém a autoridade ainda não adotou regulação sobre este assunto, conforme foi observação da seção 2.2. É, portanto, essencial abordar outras fontes normativas sobre segurança da informação *lato sensu* para definir quais controles podem ser adaptados para garantir a segurança de dados pessoais.

A seguir, como inicialmente anunciado, serão abordados os aspectos relativos à proteção de informações não pessoais.

2.3.2 Proteção de informações não pessoais

Conforme explorado na subseção anterior, todos os dados que não sejam relativos a uma pessoa ou a um grupo de pessoas identificadas ou identificáveis serão aqui contemplados pela proteção. Refere-se, por exemplo, aos dados negociais, estratégicos, estatísticos e de gestão pública e privada.

Nesses termos, os direitos fundamentais afetados serão aqueles de cunho econômico e os relacionados ao acesso à informação. Assim, pode-se citar o inciso XXXIII do artigo 5º da Constituição Federal, que dá fundamento ao direito de acesso à informação; a porção relativa à ordem econômica (art. 170 e seguintes), especialmente pensando-se na proteção da concorrência face a atos de concorrência desleal, incluindo espionagem industrial; e, apesar de não mencionar explicitamente o segredo industrial,

o inciso que trata dos direitos de propriedade intelectual (art. 5º, XXIX). Além disso, pode-se citar algumas obrigações ou termos organizativos contidos na Constituição, como o inciso IX do artigo 93, relativo à publicidade dos julgamentos; o princípio geral da publicidade dos atos administrativos (art. 37); e o compartilhamento de cadastros e informações fiscais pelas administrações tributárias de todas as esferas da administração (inciso XXII do art. 37).

No âmbito infraconstitucional, e mesmo infralegal, uma miríade de normativas são potencialmente aplicáveis, como normas setoriais destacadas a respeito de padrões de segurança de sistemas;[42] as normas específicas dos poderes da União;[43] e normas e diretrizes do Gabinete de Segurança Institucional a respeito de diversos aspectos da gestão de sistemas informáticos na Administração Pública[44] (Presidência da República, 2021b).

É igualmente relevante mencionar que alguns materiais, embora não sejam obrigatórios, são orientações aos regulados e, quando implementados, provavelmente serão considerados positivamente em eventual avaliação administrativa ou judicial. Nessa trilha, cita-se o "Guia Orientativo de Segurança da Informação para Agentes de Tratamento de Pequeno Porte", publicado pela ANPD (ANPD, 2021), documento oficial de boas práticas que compila tanto a segurança da informação quanto a proteção de dados pessoais. Conforme a Resolução CD/ANPD nº 2/2022, os agentes de tratamento de pequeno porte – definidos no art. 2º –possuem a flexibilização de algumas regras previstas na LGPD e, portanto, o guia visa iluminar esse percurso na temática específica a que se propõe.

---

42 Norma do CNJ (2021) que institui requisitos de segurança da informação a serem seguidos por órgãos do Poder Judiciário. Disponível em: https://atos.cnj.jus.br/atos/detalhar/3975. Acesso em: 9 maio 2024.

43 Como, por exemplo, a Estratégia Nacional de Segurança Cibernética do Poder Judiciário. Inclusive, uma relação exaustiva de instrumentos normativos vigentes, a partir de publicações do MGISP e do GSI-PR, está disponível na forma de linha do tempo desenvolvida pelos autores, disponível em: https://redeciber.seg.br/linha-do-tempo-de-instrumentos-normativos-em-ciberseguranca/. Acesso em: 09 maio 2024.

44 Citam-se, como exemplos: NC nº 08 /IN01/DSIC/GSI-PR, sobre gerenciamento de incidentes em redes computacionais nos órgãos e entidades da Administração Pública Federal; NC nº 12 /IN01/DSIC/GSIPR, referente ao uso de dispositivos móveis nos órgãos e entidades da Administração Pública Federal direta e indireta; e outros.

O referencial desse Guia, em linha com os *standards* internacionais explorados mais à frente, organiza-se classificando as medidas de segurança da informação em medidas *i)* administrativas (ANPD, 2021, p. 8–10), atribuindo especial destaque aos programas de conscientização e treinamento e, em outros planos, à elaboração de política de segurança da informação e ao gerenciamento de contatos; e *ii)* técnicas (ANPD, 2021, p. 10–17), elencando o controle de acesso orientado pelo princípio "menos privilégio" (*need to know*), a segurança no armazenamento de dados pessoais, nas comunicações, a manutenção de programa de gerenciamento de vulnerabilidades, além de recomendações concernentes ao uso de dispositivos móveis e aos controles de segurança ao serviço de nuvem (*cloud*) (Presidência da República, 2022a). Evidencia-se, pelo respectivo conteúdo, que as preocupações de segurança são reproduzidas em diversos ambientes, devendo contemplar controles mais ou menos abrangentes, a depender do risco das atividades de tratamento de dados pessoais e da criticidade de demais informações negociais ou de Estado.

O amplo escopo da segurança da informação, como elemento que perpassa atividades em todos os setores de atividade, desde a economia até a execução de políticas públicas, se traduz, igualmente, em uma ampla variedade de entes controladores, reguladores e executores, o que já restou evidenciado na seção anterior. Citam-se:

1. a Autoridade Nacional de Proteção de Dados, autarquia de caráter especial com capacidade de sancionar administrativamente e regular a aplicação da LGPD;
2. o sistema de proteção ao consumidor, – incluindo Procons estaduais, Senacon e considerando a atuação do Ministério Público – que é aplicado concomitantemente à LGPD e vem servindo de base para casos relacionados a incidentes de segurança ou malversação de dados pessoais;
3. as agências reguladoras setoriais, como ANATEL, ANEEL, entre outras etc. e sua capacidade de regular matérias relativas ao processamento de informações pelos entes regulados;
4. o CNJ, na definição de padrões de tratamento de dados e segurança da informação no âmbito do Poder Judiciário;

5. os mais variados órgãos da Administração Pública, considerando os meios de compartilhamento de dados entre órgãos (por exemplo, pelos procedimentos regidos pelo Decreto nº 10.046/2019 (Presidência da República, 2019) e a implementação de normas de segurança;
6. o sistema de fiscalização tributária, que apresenta um capítulo à parte do compartilhamento de dados entre esferas da Federação;
7. o próprio STF, como intérprete último dos direitos constitucionais já comentados (veja-se, a este respeito, o caso IBGE, que cristalizou a interpretação da proteção de dados como direito fundamental autônomo no ordenamento brasileiro);[45] etc.

Enfim, um sem-número de atores institucionais têm áreas de influência sobre a regulação e o controle quando se trata de proteção de dados pessoais e segurança da informação. A garantia de funcionamento seguro de sistemas digitais, especialmente em um contexto de digitalização cada vez mais aprofundada nos serviços públicos e privados, dependerá de coordenação das competências de todos esses entes – não apenas por questões políticas, mas pelo próprio modo de funcionamento da cibersegurança.

Essa característica, conforme mencionado na seção sobre governança, somada ao fato de que vulnerabilidades em um ponto de um complexo de sistemas podem abrir caminho para estratégias de penetração em outros pontos do mesmo complexo, exige ações de cooperação e integração entre os órgãos e entidades, públicas e privadas, o que é reconhecido na E-Ciber (artigo 1º, II, e artigos 7º e 8º).

Concluindo esta seção, fica evidente que a segurança da informação demanda não apenas atenção contínua, mas também uma abordagem estratégica e integrada por parte das organizações. Diante de um cenário em constante transformação e de desafios impostos pela evolução tecnológica, torna-se fundamental compreender como as práticas de segurança da informação podem ser incorporadas de forma eficaz aos processos internos.

Na próxima seção, exploraremos como as ações de segurança devem ser implementadas, desde a concepção e por padrão, analisando a importância dessas premissas para suprir lacunas legislativas e garantir a segu-

45 Sobre o caso, ver Bioni; Dias, (2020); Doneda, (2019).

rança de dados pessoais e não pessoais, frente à multiplicidade de agentes e contextos de tratamento.

2.3.3 Demais referenciais de orientação

Após compreender as definições e os arcabouços regulatórios referentes aos dados pessoais e não pessoais, dedica-se agora à revisão de outros percursos que igualmente fortalecem os programas de governança da segurança da informação em cada organização e, para além, auxiliam no processo de homogeneização quando sitiado em contexto relacional mais amplo, que inclui agentes de tratamento de dados público e privado.

Em face de desafios materiais ("o que fazer?") e formais ("como fazer?"), Destaca-se que as ações correlatas à segurança da informação tanto devem ser implementadas desde a concepção (*by design*[46]) de processos e projetos quanto por padrão (*by default*). Essas duas premissas firmam-se justamente perante a insuficiência regulatória – ainda embrionária e carente de reforço e implementação –, no que diz respeito à imposição e garantia de segurança de dados especialmente pessoais.

Nessa linha, conscientes dessas regras gerais e específicas a determinados contextos mencionados nas duas últimas subseções deste trabalho, as organizações, nos âmbitos público e privado, buscam, em prol de eventual harmonização do modelo de governança da informação a ser implementado internamente: *i)* guias orientativos (boas práticas, estruturas e

46 No período pós-Segunda Guerra Mundial, a necessidade de uma postura proativa conduziu à adoção por diversos países das "Práticas Justas de Informação" (sigla em inglês: FIPs - *Fair Information Practices*), com a implementação de princípios universais de privacidade para o manuseio de dados pessoais desde o início, bem como durante todo o percurso de eventual tratamento de dados. A privacidade desde a concepção (*privacy by design*) remete ao ideal de integração das medidas assecuratórias da privacidade diretamente na arquitetura e no ciclo de vida de determinado processo ou projeto com primazia. Conforme (Cavoukian, 2012), essa abordagem baseia-se em sete princípios, quais sejam, (i) "Proativo, não Reativo; Preventivo, não Remediativo"; (ii) "Privacidade como Configuração Padrão"; (iii) "Privacidade Incorporada no Design" e, portanto, à arquitetura do sistema, ao produto ou serviço prestado; (iv) "Funcionalidade Completa – Soma Positiva, não Soma Zero", no sentido de acomodar todos os interesses legítimos de forma positiva, em oposição à falsa dicotomia "privacidade vs. Segurança"; (v) "Segurança de Ponta a Ponta – Proteção ao Longo de Todo o Ciclo de Vida"; (vi) "Visibilidade e Transparência – Mantenha Aberto"; e (vii) "Respeito à Privacidade do Usuário – Mantenha Centrado no Usuário".

padrões) provenientes de entidades especializadas, eventualmente promotoras de selos ou certificações; *ii)* a formação e a capacitação de colaboradores e de terceiros engajados com as atividades desenvolvidas naquele ambiente; *iii)* a produção e/ou a incorporação de códigos de conduta; *iv)* a contratação de seguros contra riscos cibernéticos; e *v)* a adoção de cláusulas-tipo (padrão) ou de regras corporativas vinculativas que definam controles de segurança da informação (Belli *et al.*, 2023b, p. 54–55). Esses pontos serão explorados em seguida, para oferecer uma apresentação não exaustiva de seu conteúdo ao leitor.

Sobre os guias orientativos (normas não vinculantes), destacam-se aqueles comumente utilizados, cuja observância é considerada boa prática internacional e que, portanto, são tipicamente adotados como referenciais para organizações públicas e privadas, quais sejam:

- ISO/IEC 27.001 (*International Organization for Standardization*): norma de sistema de gerenciamento da segurança da informação baseada em risco. O seu primeiro versionamento foi publicado em 2005. Hodiernamente, é considerada um dos referenciais mais utilizados. A entidade conta com 167 países-membros, dentre eles o Brasil. Trata-se de modelo aplicável a todos os tipos de organizações, seja nelas integralmente, seja somente em áreas específicas. É passível de certificação;
- NIST *Cybersecurity Framework* (CSF): regras relativas à gestão de riscos de segurança cibernética em infraestruturas críticas. Embora seja de um nicho específico, é igualmente uma base de referência ampla para todos os tipos de organizações, passível de aplicação focal (escopo delimitado) ou integral, conforme necessidade e/ou capacidade daqueles que a implementam. O enfoque da normativa direciona-se aos efeitos da segurança nas dimensões físicas, cibernéticas e de pessoas;
- NIS 2.0, Diretiva (UE) 2022/2555 do Parlamento Europeu e do Conselho: diferentemente dos exemplos supracitados, esta Diretiva representa um instrumento regulatório compreensivo que ambiciona identificar controles capazes de promover um nível elevado de segurança cibernética na União Europeia. Precisa-

> mente, avança ao criar mecanismos de cooperação entre as autoridades de seus Estados-membros, enrobustecer a lista de setores e atividades sujeitas aos deveres correlatos à cibersegurança, e padronizar as diretrizes de supervisão e de execução para os Estados-membros;

Em que pese as peculiaridades desses documentos de fontes plurais – sendo, respectivamente, uma organização internacional de natureza técnica, uma agência nacional e uma organização intergovernamental supranacional –, todos convergem ao *i)* adotar uma abordagem embasada em risco; *ii)* demandar um alinhamento com a estruturação de sistemas de gestão da segurança da informação coerentes com os objetivos, a visão e a missão da atividade-fim desenvolvida; *iii)* descrever controles de segurança a serem implementados em camadas; *iv)* evidenciar a compreensão de uma governança de movimento cíclico e, portanto, impulsionado por monitoramento e aperfeiçoamento contínuo; e, por fim, à pretensão comum de *v)* fomentar a confiança na economia digital, por meio da resiliência de infraestruturas críticas e da manutenção da segurança cibernética (Belli *et al.*, 2023b, p. 59).

As dimensões mencionadas são incorporadas conforme as especificidades de cada organização. São incontáveis os modelos adaptados, portanto, somente a título ilustrativo, mencionam-se os documentos "Programa de Privacidade e Segurança da Informação elaborado pelo Ministério da Gestão e Inovação em Serviços Públicos"[47] e os "Cinco controles de segurança cibernética para ontem" definidos pelo Tribunal das Contas da União (BRASIL, 2022). Esses últimos controles, destacados pelo TCU e embasados na oitava versão do *framework* definido pelo *Center for Internet Security,* estruturam-se na seguinte forma:

47 O framework, os guias e os modelos do Programa de Privacidade e Segurança da Informação (PPSI) podem ser acessados no site dedicado, junto com uma ampla gama de material de grande utilidade pública. Ver https://www.gov.br/governodigital/pt-br/privacidade-e-seguranca/framework-guias-e-modelos .

Quadro 6 - Controles de segurança de informação

Controle	Finalidade
1. Inventário e controle de ativos corporativos	Identificar e impedir a utilização de ativos de TI não autorizados/gerenciados como vetores de ataques cibernéticos.
2. Inventário e controle de ativos de software	Identificar e impedir a utilização de softwares não autorizados/gerenciados como vetores de ataques cibernéticos.
3. Proteção de dados	Garantir a confidencialidade, integridade e disponibilidade dos dados, protegendo-os contra acessos não autorizados, perda ou corrupção.
4. Configuração segura de ativos corporativos e software	Assegurar que os ativos e softwares estejam configurados conforme as melhores práticas de segurança para minimizar vulnerabilidades.
5. Gestão de contas	Controlar a criação, modificação e exclusão de contas de usuários para garantir que apenas pessoas autorizadas tenham acesso aos sistemas.
6. Gestão de controles de acesso	Restringir e monitorar o acesso a sistemas e informações conforme os privilégios necessários para cada usuário.
7. Gestão contínua de vulnerabilidades	Evitar a exploração de vulnerabilidades conhecidas nos ativos corporativos de TI por meio de identificação, avaliação e correção contínua.
8. Gestão de registros (logs) de auditoria	Registrar e monitorar eventos relevantes para detectar e analisar incidentes de segurança.
9. Proteção de e-mail e navegador da web	Prevenir ataques e ameaças que utilizam e-mail e navegadores como vetor, como phishing e malwares.
10. Defesa contra malware	Detectar, bloquear e remover softwares maliciosos para proteger os sistemas e dados.
11. Recuperação de dados	Garantir a restauração rápida e segura de dados em caso de perda, corrupção ou ataque.
12. Gestão de infraestrutura de rede	Assegurar a segurança e disponibilidade da infraestrutura de rede, prevenindo acessos e ataques indevidos.
13. Monitoramento e defesa de rede	Detectar e responder a atividades suspeitas e ataques na rede em tempo real.
14. Conscientização e treinamento	Reduzir a possibilidade de incidentes e ataques derivados do comportamento humano – engenharia social.
15. Gestão de provedores de serviço	Garantir que provedores externos cumpram requisitos de segurança compatíveis com a organização.
16. Segurança de aplicações de software	Desenvolver e manter aplicações seguras, prevenindo vulnerabilidades e ataques.
17. Gestão de respostas a incidentes	Melhorar a capacidade de identificar potenciais ameaças e ataques, evitar que se espalhem e recuperar rapidamente dados e sistemas eventualmente corrompidos.
18. Teste de invasão	Avaliar a eficácia das defesas de segurança por meio de simulações controladas de ataques para identificar e corrigir vulnerabilidades.

Fonte: Elaboração própria.

Qualquer que seja a referência eleita como padrão, enaltece-se a relevância das iniciativas e dos programas de formação e capacitação de profissionais. Essa talvez seja a principal ação a ser planejada em todo e qualquer modelo de governança da segurança cibernética. Portanto, controles técnicos de segurança em redes, sistemas e aplicações devem ser acompanhados por capital humano treinado e qualificado apto a utilizá-los.

Ademais, as atividades internas não são estanques e precisam ser atualizadas ou redefinidas periodicamente, demandando a preparação e colaboração orgânica de seus membros (colaboradores e terceiros intervenientes nos processos da organização), por meio de exercícios conjuntos, palestras, boletins de notícias, treinamentos, simulações, entre outros. Nessa linha, nada obstante somente a ISO/IEC 27.001 ser passível de certificação, sobrevalem-se outros mecanismos para atestar os esforços direcionados à cibersegurança: aqueles endereçados às pessoas físicas.[48]

Junto a sensibilização e capacitação, cuja relevância será analisada especificamente em seguida,[49] é particularmente relevante destacar sete pilares fundamentais da segurança da informação: *i)* a organização estrutural e documental da segurança da informação; *ii)* o inventário e a gestão de ativos; *iii)* a limitação (por preferências) de acessos físicos e digitais à informação; *iv)* a criptografia e o *backup* (cópias de segurança); *v)* a segurança dos processos de recursos humanos e da cadeia de suprimentos; *vi)* a segurança na comunicação; e *vii)* a gestão de incidentes de segurança da informação.

Dentre os vários documentos norteadores a serem elaborados e aplicados, a produção ou a adoção de códigos de conduta – nessa última hipótese, redigidos por partes interessadas – é largamente recomendada. No mesmo sentido, cabe a cada entidade interessada avaliar a viabilidade da celebração de um contrato de seguro contra riscos cibernéticos, ação que pode resultar particularmente positiva não somente para a imagem da entidade segurada,

48 Alguns cursos de formação sobre segurança da informação já ganharam particular destaque e reconhecimento, como o "Certified Information Systems Security Professional (CISSP)", "Certified Information Security Manager (CISM)" e o "*Certified in Risk and Information Systems Control* (CRISC)", todos dedicados aos profissionais com atuação em cargos gerenciais no âmbito da segurança da informação.

49 Ver seção 2.5.

mas também pela necessária auditoria de cibersegurança que a seguradora deverá impor antes de concluir o contrato de seguro em cibersegurança.[50]

Face à premissa da inexistência de risco zero, os contratos de seguro desempenham duplo papel: primeiro, teleológico e, portanto, compensatório ante a ocorrência de prejuízos provenientes de incidentes de segurança da informação; segundo, de eventual corregulação da organização contratante, na medida em que o acordo interpartes contempla listagem de requisitos de medidas de segurança técnicas e organizacionais a serem rigorosamente implementadas e seguidas para que, perante o sinistro, o contrato seja executável (Talesh; Gonçalves, 2023).

Por último, porém de equivalente importância, faz-se alusão às cláusulas-padrão contratuais ou às regras corporativas vinculativas (setoriais). Essas cláusulas padronizadas costumam versar sobre questões tocantes à responsabilidade, à transferência de dados, ao foro para dirimir conflitos, às legislações aplicáveis e às medidas técnicas e organizacionais mínimas exigidas (Belli *et al.*, 2024). As regras corporativas vinculativas, de forma díspar, são políticas de proteção de dados – que incluem a definição de requisitos mínimos de segurança de dados pessoais – para transferências internacionais de dados pessoais dentro de um grupo de empresas. Essas regras devem *i)* incluir os princípios gerais de proteção de dados e os direitos aplicáveis para garantir as salvaguardas adequadas para as futuras transferências de dados; *ii)* ser submetidas à aprovação da autoridade competente; e *iii)* ser juridicamente vinculantes e aplicadas a todos os envolvidos.

Diante da complexidade da lógica atrelada à realidade cibernética, os profissionais envolvidos nos programas de governança, independentemente do âmbito de atuação, são compelidos a acompanhar as constantes e rápidas mutações de cenários, tecnologias disruptivas e ofensas cibernéticas, incluindo-se aqui a problemática concernente ao cibercrime. Este último ponto é particularmente relevante, sendo ampla parte dos riscos e ameaças cibernéticas de origem criminosa.

Neste sentido, a próxima seção será dedicada à análise dos instrumentos voltados ao combate ao cibercrime, destacando os avanços, mas também as lacunas do sistema jurídico brasileiro neste âmbito.

50 (Belli *et al.*, 2023b).

2.4 Combate ao cibercrime

Como foi destacado nas seções precedentes, a transformação digital trouxe uma multiplicidade de riscos que contribuem para uma crescente sensação de insegurança social. Esses fenômenos podem exigir a atuação do direito penal como instrumento de proteção.[51] O aumento do acesso à internet e sua utilização para atividades sociais, bem como a digitalização de infraestruturas empresariais e públicas, geraram novas formas de desvios que ameaçam tanto ativos tangíveis, como o patrimônio, quanto ativos intangíveis, como a honra, a propriedade intelectual e a preservação de um ambiente online saudável. Essas ameaças impactam organizações governamentais, empresas privadas e os próprios indivíduos enquanto usuários.

O ambiente digital abriu novas possibilidades para que criminosos explorem e causem lesão a bens jurídicos protegidos, utilizando conhecimentos tecnológicos especializados ou explorando assimetrias informacionais para induzir vítimas ao erro. Além disso, a internet, a IA e as demais tecnologias digitais amplificam a repercussão de ilícitos "tradicionais", seja pela expansão do alcance a potenciais vítimas, como ocorre em fraudes e falsificações com danos patrimoniais, seja pelo impacto agravado das ofensas contra bens jurídicos, como nos casos de crimes contra a honra, racismo e ameaças.

A gravidade dos crimes cibernéticos é evidenciada por dados recentes que posicionam o Brasil como um dos países mais vulneráveis a esse tipo de delito. Estudos indicam que o país já foi classificado como o "epicentro de uma onda global de crimes cibernéticos" (Muggah; Thompson, 2015) e ocupou a segunda posição entre os mais afetados pelo cibercrime (BNamericas, 2020). Mais recentemente, o Brasil figura entre os cinco principais

51 A resposta penal é a criação de crimes de perigo, o que acarreta na expansão do direito penal. Sobre essa, Flávia Goulart Pereira, afirma que a sociedade pós-industrial, com sua crescente insegurança, apresenta algumas características que causam esse alargamento. São elas: *i)* surgimento de novos bens jurídicos e aumento do valor de alguns existentes; *ii)* aparecimento de novos riscos; *iii)* sentimento social de insegurança; *iv)* configuração de uma sociedade de novos "sujeitos passivos"; *v)* pressão de novos grupos sociais para tutela de seus interesses (feministas, pacificistas, consumidores etc.); e, *vi)* o descrédito de outras instâncias de proteção (Pereira, 2004). Silva-Sánchez (2013, p. 34) pontua que a informática surge como novo elemento social, que justifica nova expansão normativa do Direito Penal de forma legítima, já que esse passa a se relacionar com uma nova realidade (Silva-Sánchez, 2007).

países com maiores perdas financeiras associadas a crimes cibernéticos, totalizando cerca de US$ 20 bilhões anuais, o equivalente a 0,9% do PIB nacional (The Economist, 2024).

Os cibercrimes, entendidos como atividades ilegais que envolvem o uso de computadores ou outros ativos digitais no ambiente digital, podem ser classificados em próprios ou impróprios, conforme a relação com o ciberespaço.[52] Os crimes cibernéticos próprios são aqueles que não poderiam ocorrer sem o uso de tecnologias digitais, como a invasão de dispositivo informático, prevista no artigo 154-A do Código Penal, que protege contra acessos não autorizados a sistemas de informação. Já os crimes informáticos impróprios correspondem a delitos que também poderiam ser realizados no ambiente físico, mas cuja prática no meio digital amplia sua eficácia ou alcance, como no caso do estelionato digital, cometido por meio de e-mails fraudulentos ou redes sociais para obtenção de vantagens financeiras.

Atualmente, não existe no Brasil uma "Lei Geral contra Crimes Cibernéticos", capaz de definir e disciplinar de maneira sistematizada todos os potenciais crimes cometidos no ciberespaço. No entanto, à medida que esses ocorrem, têm-se realizado alterações pontuais e reativas na legislação penal, majoritariamente relacionadas a cibercrimes impróprios. Nesse cenário, a adesão do Brasil à Convenção de Budapeste sobre Cibercrime, em 2022, e sua internalização por meio do Decreto nº 11.491/2023 representam um marco significativo no avanço e combate ao cibercrime (Belli, 2022).

A importância da Convenção reside na padronização de uma lista mínima comum de crimes que devem ser tipificados por todos os Estados-partes signatários. Essa harmonização legislativa busca superar um obstáculo frequente no âmbito da cooperação internacional, em que um país se recusa a colaborar porque determinada conduta não é considerada crime em seu ordenamento jurídico. Além disso, a Convenção introduz medidas processuais específicas para enfrentar desafios inerentes ao cibercrime,

52 A menção à classificação de cibercrimes próprios ou impróprios encontra respaldo na literatura que adota a referida classificação sob a nomenclatura de "crimes informáticos" próprios, que se referem aqueles cometidos em face do bem jurídico informático ou virtualidade, e impróprios, quando a prática do crime ocorre por meio da infraestrutura informática. Nesse sentido, Croze e Bismuth (1986, p. 207); Ferreira (2001, p. 214–215); Sydow (2024, p. 224 e ss.); Vianna (2003, p. 13–26) e Lage (2013, p. 17–18).

como a dificuldade de coleta de provas em ambiente digital, caracterizado pela volatilidade e transnacionalidade das informações.

A internalização de tratados e convenções internacionais por meio de Decreto Legislativo confere às suas disposições força de lei no ordenamento jurídico brasileiro. Esse procedimento distingue-se do decreto do Poder Executivo, pois não se trata de um ato meramente administrativo, mas de um mecanismo legislativo que incorpora normas internacionais ao direito interno. Assim, as regras previstas na convenção tornam-se obrigatórias e aplicáveis no âmbito nacional, salvo em matérias que exijam reserva de lei formal.

No que se refere à criminalização de condutas, a Constituição Federal, em seu artigo 5º, inciso XXXIX, e o Código Penal, em seu artigo 1º, estabelecem que somente uma lei em sentido formal, aprovada pelo Poder Legislativo, pode tipificar infrações penais e estabelecer sanções. Dessa forma, ainda que uma convenção internacional internalizada contenha disposições criminais, sua aplicação depende de posterior normatização por meio de lei ordinária ou complementar.

Entretanto, essa exigência não se estende às normas de caráter processual. Portanto, as medidas processuais previstas em convenções internacionais possuem aplicação imediata após a promulgação do decreto internalizador, tornando-se instrumentos fundamentais para a investigação e persecução penal. Tais medidas incluem técnicas especiais de obtenção de provas, aprimoramento dos mecanismos de cooperação internacional e ampliação das capacidades das autoridades competentes no enfrentamento de crimes complexos, especialmente aqueles cometidos no ciberespaço.

Outro avanço proporcionado pela Convenção é o fortalecimento da cooperação internacional, indispensável para enfrentar crimes cibernéticos, cuja prática muitas vezes ultrapassa fronteiras e demanda articulação entre diversas jurisdições.

Dentro desse contexto, o Decreto Federal nº 11.856/2023, que instituiu a Política Nacional de Segurança Cibernética (PNCiber), atribui como um de seus objetivos "contribuir para o combate aos crimes cibernéticos e às demais ações maliciosas no ciberespaço" (Presidência da República, 2023b, art. 3º, IV).

A Estratégia Nacional de Cibersegurança (E-Ciber/2025) não dedicou um eixo para o cibercrime, mas estabeleceu como ações o incentivo e a capacitação e ao aprimoramento dos órgãos de persecução penal na repres-

são dos cibercrimes (artigo 4º, XIV). Também indicou como ação inerente à cooperação e integração entre os atores que atuam em cibersegurança o combate ao cibercrime e outros ilícitos cometidos no ciberespaço (artigo 8º, III, d, da E-Ciber/2025).

Dessa forma, nesta subseção, será abordada a importância de estabelecer mecanismos que possam fomentar ações que enfrentem o cibercrime e a neutralização de outras ações maliciosas no ciberespaço, reforçando a proteção dos bens jurídicos informáticos/digitais, e que possam fomentar a cooperação entre os atores competentes para a persecução penal. Para fins de compreensão do cenário jurídico atual, antes será apresentado um breve panorama das normas vigentes no ordenamento jurídico brasileiro em contraste com as prescrições normativas internalizadas pelo Decreto Federal relacionadas ao cibercrime.

2.4.1 Normas penais vigentes no ordenamento brasileiro para o enfrentamento do cibercrime

Conforme mencionado na introdução desta seção, não existe no Brasil um regramento sistemático para crimes cometidos exclusivamente no ciberespaço. Entretanto, à medida que esses ocorrem, têm-se realizado alterações pontuais e reativas[53] na legislação penal, de maneira que a legislação penal pode conter também disposições que tenham como objetivo proteger a segurança no ambiente digital, sobretudo a confidencialidade, integridade e disponibilidade de dados e sistemas informáticos e dos indivíduos que utilizam esses dados e sistemas.

Os primeiros crimes informáticos específicos na legislação brasileira foram tipificados nos artigos 313-A e 313-B do Código Penal (CP), criados pela Lei nº 9.983/2000. Esses dispositivos passaram a prever crimes funcionais contra a integridade de sistemas informáticos da Administração Pública. O artigo 313-A do CP criminaliza a inserção de dados falsos nos sistemas de informações por servidores públicos com a finalidade de obter

53 Silva Sánchez critica a falta de sistematização das legislações penais, o que se aplica ao Brasil, entendendo que constrói-se uma verdadeira "colcha de retalhos", que exige muito trabalho ao intérprete para a correta tipificação das condutas, o que, por consequência, também dificulta a persecução penal (2013).

vantagens indevidas ou prejudicar outrem, enquanto o artigo 313-B do CP pune a modificação ou alteração de sistemas de informações sem autorização ou justificativa legal.

Após um longo período sem avanços significativos, somente em 2012 houve a promulgação de novos tipos penais relacionados ao cibercrime. A Lei nº 12.737/2012, popularmente conhecida como "Lei Carolina Dieckmann", introduziu o artigo 154-A, que passou a dispor sobre a criminalização da invasão a dispositivos informáticos, desde que a invasão se dê mediante violação de mecanismo de segurança e com a finalidade de obter, adulterar ou destruir dados ou informações sem autorização do titular, além de prever penalidades para a interrupção ou perturbação de serviços telegráficos, telefônicos, informáticos, telemáticos ou de informação de utilidade pública.

Nos anos que se seguiram, a legislação brasileira continuou a ampliar o escopo de delitos relacionados ao uso de meios informáticos, abordando diferentes práticas ilícitas associadas ao uso de tecnologias digitais. Em 2018, a Lei nº 13.718 tipificou o crime de divulgação de cena de estupro, incluindo-o no artigo 218-C do Código Penal. Esse dispositivo criminaliza a conduta de oferecer, compartilhar ou divulgar, por qualquer meio, cenas de estupro ou estupro de vulnerável, com pena aumentada se a divulgação ocorrer por meio da internet ou de redes sociais. Ainda naquele ano, a Lei nº 13.772 criou o artigo 216-B, que passou a punir o registro não autorizado da intimidade sexual, buscando proteger a privacidade das vítimas contra exposições indevidas, especialmente no ambiente digital.

Em 2019, o legislador ordinário deu continuidade ao fortalecimento do arcabouço penal ao introduzir o agravamento das penas para crimes contra a honra (calúnia, difamação e injúria) praticados por meio de dispositivos informáticos, conforme o artigo 141, §2º, e ao modificar o artigo 122, §4º, para tipificar a instigação, induzimento ou auxílio ao suicídio ou à automutilação, ampliando a abrangência dessas condutas no ambiente digital.

Em 2021, a Lei nº 14.155 introduziu os artigos 155, §4º-B, e 171, §§2º-A e 2º-B, que trouxeram qualificadoras e causas de aumento de pena para os crimes de furto mediante fraude e de estelionato. Esses dispositivos visam punir fraudes realizadas por meio de dispositivos informáticos, como o envio de mensagens falsas para obtenção de dados bancários ou a práti-

ca de golpes virtuais em plataformas digitais, reconhecendo o aumento significativo desses crimes na sociedade conectada. Além disso, realizou a reforma no art. 154-A, anteriormente mencionado, simplificando sua redação, retirando alguns elementos subjetivos e normativos do caput, o que resultou na ampliação do tipo penal. A redação anterior exigia que a invasão fosse em "dispositivo informático alheio" e "mediante violação indevida de mecanismo de segurança". A primeira parte da redação foi modificada para considerar crime a "invasão em dispositivo informático de uso alheio" e a segunda parte da redação foi suprimida pela reforma. Alterações nos limites da causa de aumento de pena e da qualificadora também foram realizadas para majorá-las.

Em 2022, a Lei nº 14.478 trouxe o artigo 171-A, que trata do estelionato envolvendo ativos virtuais, valores mobiliários ou ativos financeiros, buscando penalizar fraudes em transações que envolvem criptomoedas ou outros ativos digitais, cada vez mais utilizados no mercado financeiro. Mais recentemente, em 2024, a Lei nº 14.811 introduziu o parágrafo único ao artigo 146-A, tipificando a prática de intimidação sistemática virtual, conhecida como *cyberbullying*. Essa norma reconhece a gravidade do impacto psicológico das práticas de intimidação no ambiente digital, estabelecendo penalidades para condutas que visem humilhar, ameaçar ou constranger vítimas de maneira sistemática e reiterada, com foco em proteger a incolumidade psicofísica do indivíduo enquanto usuário de tecnologias digitais.

Antes de finalizar essa seção, é interessante fazer uma ressalva no que se refere à regulação do uso de dados pessoais para a persecução penal. A Lei Geral de Proteção de Dados Pessoais (LGPD), diploma responsável pela proteção de dados pessoais no Brasil, excluiu de seu escopo a regulação do uso de dados pessoais para persecução criminal, conforme previsão do artigo 4º. Em que pese tal exclusão, há projetos de lei em andamento no Congresso Nacional brasileiro que discutem o tema. São eles o anteprojeto de Lei da Câmara de 2019[54] e o Projeto de Lei nº 1515/2022.[55] Embora sir-

54 Texto disponível em: https://static.poder360.com.br/2020/11/DADOS-Anteprojeto-comissao-protecao-dados-seguranca-persecucao-FINAL.pdf.

55 Texto disponível em: https://www.camara.leg.br/proposicoesWeb/fichadetramitacao?idProposicao=2326300#tramitacoes.

vam como ponto de partida ao debate, ambos os textos possuem lacunas e disposições que devem ser debatidas e amadurecidas.[56]

A ausência de um marco normativo específico sobre a proteção de dados pessoais na persecução penal tem levado a uma abordagem casuística por parte do Poder Judiciário, com decisões baseadas em normas que frequentemente não priorizam a proteção de dados pessoais.[57] Legislar sobre essa matéria é essencial para garantir o acesso das autoridades a dados relevantes para combate ao cibercrime, de maneira legal e efetiva, ao mesmo tempo em que protege os cidadãos contra abusos e vigilância indiscriminada, estabelecendo diretrizes claras sobre a coleta, armazenamento e uso de informações pessoais em investigações criminais.

Dessa forma, ainda que possamos considerar como realizada uma ampliação do arcabouço jurídico, é importante destacar que a maioria das iniciativas legislativas priorizou os crimes informáticos impróprios, ou seja, aqueles em que o ativo digital é utilizado como meio para a realização de condutas ilícitas tradicionais. Em contraste, os crimes informáticos próprios, que afetam diretamente a proteção da informação e de outros ativos digitais, receberam pouca atenção normativa, sendo o artigo 154-A uma das poucas exceções relevantes. Nesse sentido, a adesão do Brasil à Convenção de Budapeste sobre Cibercrime, em 2022, formalizada internamente pelo Decreto nº 11.491/2023, representa um marco importante e será abordada na próxima subseção.

---

56 Como referência, é válido citar a Diretiva Europeia 2016/680 ("Diretiva (UE) 2016/680", 2016) que regula o tratamento de dados pessoais para fins de *law enforcement*, e acompanha a principiologia do GDPR. Esta norma, por ser uma Diretriz para países europeus, está mais preocupada em traçar os princípios e temas que não são permitidos ao Estado, sem, contudo, adentrar no mérito de como deve ocorrer o tratamento da matéria.

57 Somente em 2024 foram abordados os temas relacionados: (a) Portaria nº 648/2024, que estabelece diretrizes sobre o uso de câmeras corporais pelos órgãos de segurança pública; (b) uso de softwares de espionagem na ADPF 1143; (c) Discussão sobre o uso de *hacking* estatal como forma de obtenção de provas e o PL nº 4939/2020; (d) Uso de programas automatizados para reconhecimento facial na esfera penal e a discussão sobre discriminação algorítmica; (e) Uso de câmeras com reconhecimento biométrico em espaços públicos de forma indiscriminada; (f) A requisição de dados pessoais a empresas privadas fora da Jurisdição brasileira para investigação e persecução penal; e, (g) A readequação do Banco Nacional de Perfis Genéticos.

2.4.2 A importância da Convenção de Budapeste

A criminalidade cibernética tornou-se uma preocupação do Conselho da Europa ainda na década de 1980, resultando na elaboração de um tratado que buscou conferir segurança jurídica e adaptabilidade às mudanças tecnológicas (Murata; Torres, 2023, p. 13). Como resultado, a Convenção sobre o Crime Cibernético foi aberta para assinatura em 2001, na cidade de Budapeste. Passados vinte anos desde sua entrada em vigor na ordem internacional, a Convenção mantém-se relevante, sendo o principal instrumento sobre este assunto e tendo sido ratificada por 72 Estados, incluindo outros países não membros do Conselho da Europa.[58]

Apesar de ter sido elaborada originalmente pelo Conselho da Europa, a Convenção possui escopo global, distinguindo-se de outros instrumentos regionais, como, por exemplo, a convenção da União Africana sobre Cibersegurança e Proteção de Dados Pessoais, pela abrangência e especificidade em crimes cibernéticos e tratamento de provas eletrônicas. Embora este tópico não se proponha a uma análise exaustiva das ciências penais, é possível identificar aspectos importantes promovidos pela norma, que é considerada um verdadeiro *framework*[59] para os países aderentes.

O tratado estabelece conceitos comuns, define medidas a serem adotadas pelas jurisdições nacionais e delineia formas de cooperação internacional no combate ao cibercrime. Ele exige de seus países aderentes que implementem em ordenamentos jurídicos um conjunto de tipificação pe-

---

58 Para consultar o status de ratificações, acessar: https://www.coe.int/en/web/conventions/full-list?module=signatures-by-treaty&treatynum=185.

59 A organização das Nações Unidas (ONU) está em fase avançada de elaboração de seu primeiro tratado internacional específico sobre cibercrime, cujo texto-base foi recentemente finalizado pelo Comitê Ad Hoc criado pela Resolução 74/247 da Assembleia Geral. Embora ainda pendente de adoção formal, a chamada "Convenção da ONU contra o Cibercrime" visa complementar instrumentos anteriores, como a Convenção de Budapeste, ampliando a abrangência dos crimes previstos e fortalecendo mecanismos de cooperação internacional, incluindo medidas de assistência técnica e capacitação para países em desenvolvimento. Há convergências entre ambas as convenções no que se refere à criminalização de delitos cibernéticos e à importância de salvaguardas processuais. No entanto, o projeto da ONU apresenta um escopo ampliado, abordando temas como a proteção de infraestruturas críticas e a tipificação de crimes de maior gravidade (puníveis com penas de quatro anos ou mais), além de incluir disposições inspiradas em outros tratados do sistema ONU voltados ao combate à corrupção e ao crime organizado. A versão preliminar oficial do tratado foi disponibilizada em 24 de dezembro de 2024 e pode ser acessada em https://docs.un.org/en/A/79/460.

nal mínima (cujas ações típicas estão detalhadas à frente), como forma de facilitar a cooperação e superar os conflitos de aplicação extraterritorial das leis penais, extradição e cumprimento de pena em outras jurisdições (Lei nº 13.445 de 2017, art. 82, II, por exemplo).

O Brasil, que ratificou a Convenção em fevereiro de 2023 e a internalizou por meio do Decreto nº 11.491/23, comprometeu-se a implementar uma série de medidas para adequar seu ordenamento jurídico às disposições do tratado. Um dos principais impactos dessa adesão é a necessidade de harmonização legislativa, especialmente na tipificação de crimes cibernéticos, já que, como analisado anteriormente, há uma lacuna normativa na definição de crimes cibernéticos específicos no país.

A lista de crimes previstos na Convenção objetiva padronizar a legislação dos estados-partes do Tratado, com especial foco na cooperação internacional. Ao exigir a criminalização de determinadas condutas, elimina-se um obstáculo comum: a recusa de cooperação por parte de países onde a infração não é considerada crime. Obviamente, o texto convencional não impede que os países criem outros dispositivos relacionados com a prática de crimes cibernéticos ou aprofundem garantias e proteções.

Ao todo, a Convenção prevê dez condutas criminalizáveis. Os artigos 2º ao 6º tratam de tipos penais dependentes do uso de dispositivos informáticos, conhecidos como crimes informáticos puros, como o acesso ilegal a sistemas informáticos, a interferência em dados e sistemas, e a interceptação ilegítima de dados informatizados. Já em consonância com parte dos preceitos da Convenção, o Brasil dispõe de legislações específicas, como a Lei nº 12.737/2012 (Lei Carolina Dieckmann), que trata da invasão de dispositivos eletrônicos. Por outro lado, os crimes definidos nos artigos 7º a 10º referem-se àqueles potencializados pelo uso de dispositivos informáticos, como a violação de propriedade intelectual e a prática de fraudes.

Para facilitar a compreensão do panorama legislativo atual sobre o cibercrime, é pertinente uma breve comparação entre a Convenção de Budapeste e o ordenamento jurídico brasileiro a fim de compreender quais condutas precisam ainda ser legisladas na área criminal. A Convenção exige a tipificação penal do "Acesso ilegal" (Artigo 2º, Convenção). O ordenamento brasileiro já possui essa conduta tipificada no artigo 154-A, CP, e de forma especial, na Lei 9.504/1997, artigo 72, I, quando ocorrer em contexto eleitoral. A chamada "Interceptação ilícita" (Artigo 3º, Convenção) equivale ao ar-

tigo 10 da Lei 9.296/96, sobre interceptações telefônicas e telemáticas. Dessa forma, o ordenamento pátrio já atende ao exigido pela Convenção.

Em relação ao artigo 4º da Convenção ("Violação de dados"), contudo, não há correspondência exata na legislação brasileira. A Convenção exige a tipificação da conduta que proteja a integridade dos dados, ao passo que o artigo 313-A do CP é um tipo penal estritamente funcional, exigindo finalidade específica de "obtenção de vantagem ou causar dano". Considerando a existência do vácuo normativo, há quem sustente a possibilidade de aplicação do artigo 163 do CP (dano patrimonial) em razão do valor econômico dos dados, mas essa subsunção é um exercício hermenêutico controverso.

Quanto ao artigo 5º da Convenção ("Interferência em sistema"), também não se verifica correspondência exata. As figuras típicas que mais se aproximam do exigido são as previstas nos artigos 313-B e 266, §1º, do Código Penal e no artigo 2º, §1º, IV, da Lei 13.260/16. Porém, o artigo 313-B é crime funcional, enquanto o artigo 266 trata apenas de serviços telemáticos. Já a Lei 13.260/2016 tipifica a sabotagem cibernética como ato de terrorismo, mas somente dentro de contextos específicos, não abrangendo, portanto, de forma geral a interferência em sistemas informáticos.

Da mesma forma, pode-se aperfeiçoar o atendimento ao artigo 6º da Convenção ("uso indevido de aparelhagem"). O uso indevido de dispositivos ou programas informáticos (aparelhagem), previsto nos parágrafos 1º, 2º e 3º do artigo 154-A do CP, está condicionado à ocorrência de invasão indevida prevista no caput. Portanto, há lacuna e necessidade de complementação legislativa, como por meio da tipificação penal da obtenção indevida de credenciais de acesso.

No que diz respeito ao artigo 7º da Convenção (crime de "falsificação informática"), também não existe correspondência exata. Os tipos penais brasileiros mais próximos (artigos 154-A, 297 e 298 do CP), diferentemente do artigo 4º da Convenção, que protege os dados, têm como bem jurídico protegido a informação. Entretanto, é possível encontrar na jurisprudência a aplicação dos artigos 297 e 298 do CP para a proteção de dados, ampliando, assim, a interpretação dos tipos penais.

De igual modo, não há correspondência exata ao artigo 8º da Convenção ("Fraude informática"). A Convenção busca proteger o patrimônio da vítima quando há comprometimento da confidencialidade, integridade ou disponibilidade de dados. Embora a jurisprudência brasileira venha apli-

cando o conceito de furto mediante fraude (artigo 155 §4º, CP), em casos envolvendo crimes cibernéticos, há um problema conceitual significativo: o furto mediante fraude, conforme tipificado, pressupõe que o meio utilizado diminua a vigilância da vítima, facilitando a subtração patrimonial.

Nos crimes informáticos, contudo, as fraudes são frequentemente direcionadas a sistemas computacionais, e a subtração patrimonial ocorre de forma indireta, sem a necessidade de redução da vigilância pela vítima. No caso da "fraude eletrônica", prevista no Código Penal, artigo 171, § 2º-A, identificam-se diversos problemas técnicos na redação da qualificadora. Entre eles, destaca-se a ausência de uma descrição clara de ação criminosa e a formulação imprecisa que menciona "redes sociais" e "contatos telefônicos" no plural, o que pode gerar dificuldades interpretativas perante o princípio da taxatividade. Idealmente, essa redação deveria ser revisada para ter maior clareza ou, alternativamente, esse tipo de conduta deveria ser tratado como um crime autônomo, em vez de ser uma qualificadora.

Em relação ao art. 9º da Convenção ("Pornografia infantil"), a legislação brasileira atende à exigência da Convenção quando legislou sobre pornografia infantil e condutas relacionadas. A reforma legislativa de 2008 no Estatuto da Criança e do Adolescente (ECA) representou um marco importante no combate à pornografia infantil no Brasil. Com a promulgação da Lei nº 11.829/2008, foram introduzidas alterações significativas nos artigos 240 a 241-E do ECA, ampliando o escopo das condutas criminosas relacionadas à produção, reprodução, distribuição e posse de material pornográfico envolvendo crianças e adolescentes. A nova redação passou a criminalizar também o simples armazenamento e o compartilhamento pela internet, reconhecendo o impacto das tecnologias digitais na disseminação desse tipo de conteúdo.

Essa atualização reforçou a proteção integral prevista no ECA e alinhou a legislação brasileira aos tratados internacionais de enfrentamento à exploração sexual infantil. A reforma legislativa ocorrida em 2018 complementou de forma significativa as disposições do ECA sobre pornografia infantil, reforçando o combate à exploração sexual de crianças e adolescentes por meio de alterações no Código Penal, especialmente nos artigos 216-B, 217-A, 218, 218-A, 218-B e 218-C.

Essas mudanças ampliaram a proteção penal, tipificando condutas como a importunação sexual (artigo 216-B), o estupro de vulnerável (artigo 217-A)

e a mediação ou induzimento de menores à prática sexual (artigos 218 a 218-C), incluindo situações de aliciamento pela internet e produção de conteúdo sexual. Em conjunto com as previsões do ECA, essas normas formam um arcabouço jurídico mais abrangente e coerente, que abrange desde a prevenção até a punição das diversas formas de violência e exploração sexual contra menores, adaptando-se às novas dinâmicas tecnológicas e sociais.

Por fim, no que concerne ao artigo 10º da Convenção ("violação de direitos autorais"), o ordenamento brasileiro igualmente atende à exigência de criminalização. O ordenamento jurídico brasileiro, no artigo 184 do Código Penal, tipifica a violação de direitos autorais, prevendo sanções para quem reproduz, distribui ou utiliza obra intelectual sem autorização, inclusive por meios eletrônicos. No campo específico do software, a Lei nº 9.609/1998 (Lei do Software), em seu artigo 12, prevê sanções para a reprodução não autorizada de programas de computador, equiparando tal conduta à violação de direitos autorais.

Assim, o conjunto normativo brasileiro busca assegurar a proteção da criação intelectual frente às novas formas de pirataria digital e garantir o respeito aos direitos morais e patrimoniais dos autores no ambiente tecnológico. Da mesma forma, o artigo 184 do CP abrange violações sobre direitos autorais por qualquer meio, cumprindo as exigências do artigo 10 da Convenção.

Neste contexto, a internalização da Convenção de Budapeste representa um avanço importante, pois demanda que o legislador brasileiro adote medidas para tipificar condutas que configuram cibercrimes, protegendo novos bens jurídicos. Isso inclui a necessidade de legislar sobre crimes como o uso indevido de aparelhagem e a obtenção indevida de credenciais de acesso[60], bem como o aprimoramento de dispositivos relacionados à fraude eletrônica e falsificação informática.

A Convenção também previu a instituição mínima de medidas cautelares pelos países signatários, considerando que a prova em meios informáticos exige celeridade. Os artigos 16 a 21 da Convenção de Budapeste sobre Cibercrime estabelecem normas que asseguram a rápida preservação

60 O Brasil precisa adequar melhor a tipificação penal para esta conduta, considerando que o Art. 154-A do Código Penal abarca satisfatoriamente apenas o uso indevido de aparelhagem. No caso da obtenção de credenciais, a redação do Código Penal não criminaliza o uso de ardil como técnica de phishing para obter senhas e dados de acesso de usuários senão quando concretizado em uma invasão de dispositivo informático.

e o acesso a informações em casos envolvendo infrações cibernéticas. Diferentemente dos crimes, as medidas processuais possuem aplicação direta a partir da promulgação do Decreto internalizador,[61] tornando-se ferramentais com técnicas especiais para a investigação e persecução criminal pelas autoridades competentes.[62]

A necessidade de adaptação da legislação diz respeito à compatibilização de alguns textos anteriores que podem dificultar a aplicação das medidas processuais previstas na Convenção. Por ser aplicável diretamente, na esfera dos cibercrimes, ela deve ser lida e harmonizada com a Lei de Interceptações em matéria criminal (Lei nº 9.296/96), em especial pela necessidade de definição de quem seriam as autoridades competentes para ordens das cautelares previstas na Convenção, e com o Marco Civil da Internet (Lei nº 12.965/2014), especificamente nas disposições sobre guarda

61 Por exemplo, diversos casos em que o STF já admitiu a aplicação da transferência de processos, embasados exclusivamente nas Convenções de Viena, de Palermo e de Mérida (Cavalcante, 2024).

62 Sobre as disposições trazidas pela Convenção de Budapeste, o Artigo 16 dispõe sobre a obrigação de preservação expedita de dados informáticos armazenados. Esse procedimento deve ser adotado em casos específicos onde há risco de perda ou modificação dos dados necessários para investigações criminais. É um pedido para que eles sejam mantidos na forma como eles estão. A preservação deve ocorrer independentemente do armazenamento estar localizado em um único país ou em múltiplas jurisdições. O Artigo 17 complementa o artigo anterior ao focar na preservação de dados relativos ao tráfego, especialmente quando esses dados estão ligados a uma investigação em curso. Além de preservar, as autoridades competentes podem solicitar a divulgação parcial de informações sobre o tráfego, limitando-se aos dados que possibilitam a identificação da fonte, destino, data, hora e duração de uma comunicação. Este artigo visa facilitar a rastreabilidade das comunicações envolvidas em atividades criminosas. Tais mecanismos possuem um marco temporal limite de 90 dias, prorrogáveis por mais 90 dias. O Artigo 18 estabelece o poder de autoridades competentes ordenarem a exibição de dados específicos por parte de prestadores de serviços e indivíduos. Esses dados podem incluir informações sobre assinantes e outros dados relacionados a comunicações e transações, inclusive dados de fatura, como número de cartão de crédito, sendo essenciais para a identificação de indivíduos e a reconstrução de eventos ligados ao cibercrime. O Artigo 19 trata da busca e apreensão de dados informáticos, permitindo que as autoridades investigativas acessem e copiem dados relevantes armazenados em sistemas informáticos. Este artigo assegura que, durante uma investigação, as autoridades possam realizar buscas tanto físicas quanto eletrônicas para apreender informações necessárias para a elucidação de crimes cibernéticos. Trata-se de disposição bem-vinda, pois os órgãos de persecução hoje no Brasil utilizam-se do art. 240, 'f' e 'h' do CPP. O artigo 20 traz a medida de interceptação em tempo real dos dados de tráfego. As autoridades de persecução então ordenam ao provedor de serviço que, dentro das suas capacidades técnicas, faça essa interceptação dos dados de tráfego, podendo obrigar a que a interceptação e gravação sejam confidenciais no interesse da investigação criminal. E, por fim, o artigo 21 traz a interceptação do conteúdo propriamente dito, medida prevista no nosso ordenamento na lei nº 9296/96 e no artigo 7º, inciso III do MCI *a contrario sensu*.

de registros e requisições, tendo em vista que possuem algumas definições distintas, como dados cadastrais e prazos. Devido a estas diferenças, o ideal é que a matéria fosse reformada em conjunto, para uniformizar o entendimento e evitar posteriores nulidades.

Por fim, a Convenção de Budapeste traz um capítulo dedicado à cooperação internacional, o que dialoga diretamente com o terceiro eixo da E-Ciber (GSI, 2025a, art. 7º e 8º). Entre as medidas de cooperação internacional destacadas no texto, algumas são comuns a outros tratados, mas voltadas especificamente para cibercrimes, enquanto outras são inovadoras e exclusivas da Convenção de Budapeste. Um exemplo de inovação é o mecanismo dito de "informações espontâneas". Conforme previsto no artigo 26, é permitido que um país envie, por iniciativa própria, informações sobre crimes cibernéticos a outro país, mesmo que esse outro país não tenha solicitado tais informações ou iniciado uma investigação. Essa medida é particularmente inovadora porque permite uma cooperação mais ágil e proativa entre os Estados, facilitando investigações antes que os criminosos possam destruir ou ocultar provas.

A Convenção também exige a criação de um "sistema de plantão 24h por 7 dias" (artigo 35), um mecanismo operacional que permite que os países signatários se comuniquem rapidamente em emergências, especialmente durante investigações de cibercrimes que requerem ação imediata. Este mecanismo é crucial para garantir uma resposta ágil e eficaz em casos que envolvem cibercrime. A rede "24/7" facilita o intercâmbio de informações em tempo real, aumentando a probabilidade de sucesso nas operações de combate ao cibercrime. Embora a rede "24/7" seja uma ferramenta poderosa, sua eficácia depende da capacidade dos Estados de manter pontos de contato operacionais, adequadamente treinados e devidamente suportados.

Outra medida importante diz respeito à preservação expedita de dados (artigo 29). Esse artigo permite que as autoridades de um país solicitem a outro país a preservação rápida de dados armazenados em um sistema de computador. Esses dados devem ser mantidos intactos enquanto um pedido formal de cooperação, como a produção de provas, é processado. A preservação expedita é crucial em investigações de cibercrime devido à volatilidade dos dados em formato digital, que podem ser facilmente alterados ou deletados. A rapidez na preservação garante que as provas estejam disponíveis quando necessárias.

Além disso, o artigo 32 traz uma autorização para que um país obtenha provas digitais em outro país sem a necessidade de autorização prévia, nos casos em que as provas estejam publicamente disponíveis ou no caso de consentimento "da pessoa que tenha autoridade legal para revelar os dados" (Council of Europe, 2001, art. 32). Este é um dos aspectos mais inovadores da Convenção, pois facilita a obtenção de provas que são essenciais em investigações de crimes cibernéticos, onde os dados podem estar espalhados em servidores de diversos países. Apesar de ser um avanço significativo, a aplicação desse artigo é limitada e levanta questões sobre a soberania dos Estados e a proteção de direitos fundamentais, como a privacidade. Assim, neste sentido existem preocupações de que a falta de autorização prévia possa levar a abusos ou a violações de direitos em jurisdições mais protetivas.

Em conclusão, a Convenção de Budapeste estabelece um marco internacional com vocação global[63] no enfrentamento ao cibercrime, buscando harmonização legislativa e a cooperação para responder aos desafios impostos pela criminalidade cibernética. Porém, como foi abordado nesta subseção, ainda existem lacunas no ordenamento jurídico brasileiro, apesar dos notáveis avanços. A existência de tais lacunas mostra a importância de tipificar condutas específicas e regulamentar medidas processuais para garantir celeridade e eficácia na persecução penal. Na próxima subseção, será explorada a relevância da incorporação dessas diretrizes na Estratégia Nacional de Cibersegurança, destacando o alcance e a contribuição que essas medidas podem oferecer no fortalecimento do combate ao cibercrime no Brasil.

2.4.3 Contribuições que a Política Nacional de Cibersegurança (PNCiber) pode fornecer para o enfrentamento do cibercrime

A Política Nacional de Cibersegurança (PNCiber) e a Estratégia Nacional de Cibersegurança (E-Ciber) representam um marco estratégico na

63 Tal vocação é compartilhada pela Convenção da ONU contra o Cibercrime, adotada com Resolução 79/243 pela Assembleia Geral das Nações Unidas. Porém, no momento desta publicação, este tratado ainda não foi assinado nem ratificado por nenhum membro da ONU. Disponível em: https://www.unodc.org/unodc/en/cybercrime/convention/home.html.

proteção de ativos digitais em face de riscos cibernéticos, consolidando diretrizes voltadas para a prevenção, detecção e resposta a incidentes cibernéticos. No contexto do enfrentamento ao cibercrime, sua implementação assume papel crucial ao estabelecer bases que reforçam a capacidade do Estado de mitigar, investigar e punir atividades ilícitas no ciberespaço.

No âmbito da prevenção, a PNCiber e E-Ciber enfatizam a importância da educação digital e da conscientização pública. Ao promover campanhas educativas, busca-se capacitar a população para reconhecer e evitar práticas maliciosas, como golpes cibernéticos e fraudes eletrônicas, reduzindo assim as vulnerabilidades associadas ao fator humano. Além disso, ambos os documentos incentivam a formação e a especialização de profissionais em segurança cibernética, garantindo que tanto agentes públicos quanto privados estejam preparados para lidar com ameaças emergentes. A padronização de protocolos de segurança entre diferentes setores também é destacada, visando uma abordagem coesa na proteção das infraestruturas críticas do país.

Para a detecção eficaz de ameaças, a PNCiber e E-Ciber promovem o desenvolvimento de capacidades avançadas de monitoramento e inteligência cibernética. Isso inclui a implementação de sistemas de coleta e análise de dados que utilizam tecnologias, como *Big Data* e *Machine Learning*, permitindo a identificação proativa de padrões suspeitos e a antecipação de possíveis ataques.[64] A cooperação entre equipes de Resposta a Incidentes (CSIRTs) e *Information Sharing and Analysis Center* (Centro de Compartilhamento e Análise de Informações) é incentivada para assegurar uma comunicação ágil e eficiente diante de incidentes complexos.

Na esfera da resposta a incidentes, a E-Ciber estabelece como importantes ações para a promoção do intercâmbio de informações e a criação de equipes de resposta, centros de análise e plataformas de notificação de incidentes. Essa arquitetura facilita a colaboração entre os atores operacionais e cria condições para a padronização de procedimentos de compartilhamento de informações e evidências digitais, inclusive por meio de bases e repositórios integrados de inteligência (art. 8º, I–III). Estas diretrizes vi-

64 Por exemplo, o monitoramento de tráfego malicioso contra *honeypots* pelo CERT.br. Disponível em: https://stats.cert.br/honeypots.

sam otimizar as operações das autoridades e aprimorar a análise forense em casos de cibercrimes.

No plano externo, a PNCiber e a E-Ciber/2025 alinham-se às normativas internacionais, como a Convenção de Budapeste sobre Cibercrime, reforçando o compromisso do Brasil com a cooperação internacional no combate aos crimes cibernéticos. A E-Ciber, ademais, determina a divulgação da Convenção e de instrumentos congêneres e incentiva mecanismos e canais para notificação e cooperação em matéria de cibercrime (GSI, 2025a, art. 4º XI e 8º, II–V).

Esse alinhamento é essencial para a celeridade e a segurança jurídica das investigações transnacionais, pois a Convenção de Budapeste disciplina, entre outros pontos, os princípios gerais de cooperação e auxílio mútuo (arts. 23 e 25-26) e instrumentos probatórios voltados ao ambiente digital (arts. 29-35).

Desse modo, a PNCiber e a E-Ciber conformam uma estrutura que integra atores públicos e privados na prevenção, detecção e resposta coordenada a incidentes, fortalecida pela cooperação nacional e internacional e amparada por instrumentos de cooperação internacional que viabilizam o compartilhamento tempestivo e padronizado de informações e evidências digitais.

Como destacaremos na seção seguinte, um dos elementos mais relevantes para prevenir crimes e riscos cibernéticos e se preparar devidamente para o acontecimento de tais ameaças é a literacia digital, que deve ser considerada como elemento fundamental de qualquer estratégia ou política de cibersegurança e luta contra o cibercrime.

2.5 Literacia digital: alicerce da cibersegurança e da soberania digital

Enquanto abordagens sistêmicas direcionadas à governança tendem a variar entre países, a educação aparece como uma temática constante em diferentes políticas públicas e índices internacionais de cibersegurança (Cabinet Office, 2023; CISCO, 2025; GSI, 2023; The State Council Information Office of the People's Republic of China, 2022; Voo; Hemani; Cassidy, 2022; White House, 2023).

A literacia digital, promovida por meio de educação, formação e capacitação, é considerada como um pilar fundamental da cibersegurança. Sua re-

levância se intensifica à medida que avanços tecnológicos, como inteligência artificial e computação quântica, redefinem o cenário de ameaças, tornando a educação e a capacitação elementos centrais para mitigar riscos cibernéticos em um contexto de crescente digitalização. Estima-se que 92% dos incidentes cibernéticos envolvem erros humanos, desde cliques em links maliciosos até configurações inadequadas de sistemas. Nesse sentido, a adoção destas novas tecnologias, sem os devidos cuidados e treinamento, pode contribuir para o agravamento do cenário de ciber(in)-segurança (Hoepers, 2024).

Entretanto, o ser humano não deve ser visto apenas como o "elo fraco" da cibersegurança; ele também exerce o papel de principal agente de defesa e fator fundamental na segurança cibernética (Hoepers, 2024). Para mitigar eventuais falhas humanas e potencializar este recurso a favor da cibersegurança, a Política Nacional de Cibersegurança (Decreto nº 11.856/2023) estabeleceu, entre os seus objetivos principais, "desenvolver a educação e a capacitação técnico-profissional em segurança cibernética na sociedade", além de "fomentar as atividades de pesquisa científica, de desenvolvimento tecnológico e de inovação relacionadas à segurança cibernética" (GSI, 2023).

Em sequência, a Estratégia Nacional de Cibersegurança estabeleceu como objetivo criar condições seguras para o uso de serviços digitais, meta que somente será possível mediante ações voltadas à proteção e à conscientização do cidadão e da sociedade (artigo 3º da E-Ciber/2025).

Uma dificuldade inerente às tecnologias digitais decorre da velocidade da evolução das ameaças cibernéticas, que exige constante atualização dos profissionais e usuários. O treinamento contínuo permite que esses agentes não apenas respondam a incidentes, mas também desenvolvam estratégias proativas, como a criação de campanhas internas de conscientização adaptadas ao perfil psicológico dos usuários. Dessa forma, a combinação de conhecimento técnico com habilidades comportamentais revela-se essencial para identificar vulnerabilidades internas, assim como padrões de ataques de engenharia social.

Para transformar comportamentos, no entanto, é necessário ir além de treinamentos pontuais e adotar abordagens multidisciplinares que integrem psicologia cognitiva, design de interfaces e pedagogia crítica (Cabinet Office, 2023; GSI, 2023; Hoepers, 2024). Iniciativas como o programa *Cyber*

Essentials[65] do Reino Unido exemplificam essa perspectiva ao combinar simulações de ataques de *phishing* com workshops voltados à compreensão das heurísticas de decisão, ensinando usuários a identificar padrões de manipulação emocional em e-mails fraudulentos. Essa abordagem holística reconhece que a segurança não se limita à dimensão tecnológica, mas envolve também transformações culturais, nas quais o indivíduo passa a ser visto como um ativo estratégico, e não como uma fraqueza a ser controlada.

Dada a transversalidade das ameaças cibernéticas, a conscientização em larga escala é essencial para compor a primeira linha de defesa, mas sua eficácia depende de estratégias adaptadas a diferentes públicos. Há mais de uma década, vários especialistas destacam a necessidade de uma "linguagem comum" para conseguir engajar os interlocutores mais heterogêneos, desde líderes políticos até comunidades rurais (Pawlak; European Union Institute for Security Studies, 2014). Sob essa ótica, é necessário traduzir conceitos técnicos (como *ransomware*) para linguagens acessíveis em vários contextos culturais, recorrendo a analogias para facilitar a compreensão.

Na Índia, por exemplo, a rede de 150 *Cyber Shakti Centres*, promovida pelo Ministério da Eletrônica e das TICs, capacita mulheres em áreas rurais, combinando cursos online com mentorias de especialistas.[66] De modo semelhante, o programa *Safe Online* da UNICEF adapta materiais educativos para idosos, crianças e populações com baixa alfabetização digital, priorizando grupos vulneráveis.[67] Essas iniciativas evidenciam que a capacitação técnica não deve se restringir às elites (econômicas ou técnicas), mas ser democratizada para incluir grupos historicamente marginalizados, a fim de promover uma mudança efetiva.

Porém, para que educação e capacitação sejam efetivas, é necessário colmatar as lacunas entre currículos acadêmicos e demandas do setor, como habilidades em resposta a incidentes e análise de ameaças, inclusive no que diz respeito a tecnologias mais avançadas como sistemas de IA (Belli, 2025b). Sob uma ótica pedagógica, integrar cibersegurança ao currículo obrigatório do ensino básico e usar módulos gamificados sobre segurança da informa-

65 Ver o site dedicado do programa. Disponível em: https://www.ncsc.gov.uk/cyberessentials.

66 Ver o site do programa. Disponível em: https://isea.app/cybershakti/.

67 Ver o site dedicado ao programa. Disponível em: https://www.unicef.org.au/unicef-youth/staying-safe-online.

ção, cibercrimes e proteção de dados pessoais podem ser soluções efetivas para sensibilizar as gerações mais jovens em idade escolar (Souza; Silva, 2023). Não obstante o desafio educacional dos mais jovens, há também a necessidade de educar e capacitar gerações que estejam fora do ensino fundamental.

Nesse âmbito, esforços nacionais como o Programa Hackers do Bem, capitaneado pela Rede Nacional de Ensino e Pesquisa (RNP), com fomento do Ministério da Ciência, Tecnologia e Inovação (MCTI), criaram cursos gratuitos em cibersegurança, além de tomar parte em discussões acerca da atualização curricular de escolas e cursos universitários direcionados para a cibersegurança (RNP, 2024).

Também no âmbito da educação e capacitação, cabe frisar o papel central da cooperação multissetorial como chave para alcançar resultados sólidos e robustos de longo prazo. Particularmente, a capacitação deve ser tratada como um processo em constante evolução, capaz de conectar os diferentes atores que estão à frente de iniciativas frequentemente fragmentadas entre atores acadêmicos, privados, governo federal, estadual e municipal.

Modelos inspiradores, neste sentido, incluem a iniciativa *Cyber Capacity Building – Cybil* (2023) que estabeleceu uma plataforma continental africana para compartilhar recursos educacionais e métricas de capacitação entre 54 países, demonstrando que a cooperação internacional pode acelerar o desenvolvimento de capacidades locais e regionais.[68]

A cibersegurança efetiva depende de um equilíbrio entre tecnologia segura, monitoramento, mitigação de riscos contínua e capital humano preparado. A capacitação deve ser enxergada como um investimento sistêmico direcionado não somente à mitigação de vulnerabilidades sociais, mas também como uma iniciativa que potencializa e equipa indivíduos em uma área na qual existe uma enorme escassez de profissionais. A falta de profissionais de cibersegurança é um desafio enfrentado por empresas e entidades públicas de todo o mundo. Somente no Brasil, em 2024, a demanda alcançava 750.000 profissionais.[69]

---

68 Ver o site dedicado à plataforma. Disponível em: https://cybilportal.org/projects/african-cyber-programme/.

69 GONÇALVES, A. L. Brasil tem escassez de 750 mil profissionais de cibersegurança, diz estudo. Techmundo. (9 julho 2024). Disponível em: https://www.tecmundo.com.br/mercado/286789-brasil-tem-escassez-750-mil-profissionais-ciberseguranca-diz-estudo.htm.

Em última instância, cidadãos digitalmente capacitados são essenciais para transformar usuários comuns em aliados conscientes, antecipar ameaças com análise crítica de cenários e garantir a sustentabilidade de políticas de segurança a longo prazo e fortalecer a soberania digital nacional, como será explicado na seção seguinte.

2.5.1 A educação como força motriz para a construção da soberania digital[70]

A educação mediante a formação inicial e continuada em cibersegurança, para além de ferramentas técnicas, representa um instrumento de empoderamento coletivo, essencial para alcançar o conhecimento, as competências e habilidades de entender, desenvolver e regular efetivamente as tecnologias digitais. A literacia digital, portanto, precisa ser assimilada como elemento fundamental da educação, contribuindo para a criação e o fortalecimento da soberania digital.

Nessa trilha, identificam-se ao menos quatro dimensões nas quais a soberania digital e a educação se justapõem: *i)* conectividade significativa; *ii)* acesso a *software*; *iii)* acesso a conteúdo educacional; e *iv)* a necessidade de se considerar os riscos das tecnologias digitais.

Primeiro, destaca-se a conectividade significativa, mediante o acesso não discriminatório e universal à Internet e a possibilidade de usar dispositivos apropriados para finalidades específicas, como aquelas profissionais. Tal tipo de conectividade é essencial para trabalhar e desenvolver tecnologia digital. Neste sentido, necessitamos frisar que, no Brasil, a esmagadora maioria dos internautas – 78% segundo os dados do Cetic[71]– se encontram ainda sem conectividade significativa, sendo de fato meros usuários de redes sociais, sobretudo daquelas plataformas que estão entre os pouquíssimos aplicativos subsidiados nas franquias dos planos de Internet móvel (*zero rating*).

---

70 Esta seção é uma expansão das considerações incluídas na seção sobre "A necessária modernização da política educacional para um país digitalmente soberano" incluída em (Belli et al., 2023b, p. 60–63) e elaborada principalmente por Bruna Franqueira.

71 CETIC. Conectividade Significativa: Propostas para medição e o retrato da população no Brasil. (2024). Disponível em: https://cetic.br/pt/publicacao/conectividade-significativa-propostas-para-medicao-e-o-retrato-da-populacao-no-brasil/.

As desigualdades materiais relativas à conexão e ao acesso aos dispositivos físicos e tecnologias digitais, especialmente considerando a enorme difusão entre as camadas mais pobres da sociedade dos planos de *zero rating* como principal medida de democratização do acesso (Instituto Locomotiva, 2021), reforçam outros processos discriminatórios e de dependência tecnológica em curso no país. Tais dinâmicas prejudicam a soberania digital individual e nacional (Belli; Jiang, 2024) e dificultam enormemente a possibilidade de cada indivíduo tornar-se um usuário ativo de Internet ao invés de mero consumidor de um número limitado de redes sociais.

Em segundo lugar, cita-se o acesso significativo a software. Isso abrange a educação digital com enfoque na programação, no uso seguro e desenvolvimento de software livre, bem como na capacitação embasada no uso de modelos algorítmicos abertos. Neste sentido, a possibilidade de ser educado ao uso e ao desenvolvimento de software em código aberto, inclusive no que diz respeito aos mais recentes modelos de IA, configura uma dimensão emergente e já essencial para literacia digital.

Como terceiro ponto de interseção entre educação e soberania digital, elenca-se o acesso significativo a conteúdo educacional. O que implica definir licenças apropriadas para regular direitos autorais na perspectiva de permitir o acesso legítimo e uso de material educacional produzido com fundos públicos e a criação de repositórios públicos de conteúdo educacional aberto facilmente acessíveis para qualquer indivíduo.

Por fim, consideram-se os riscos da ausência ou insuficiência das auditorias realizadas sobre as tecnologias digitais (como plataformas educacionais), sobretudo relativas às medidas implementadas para garantir a proteção de dados pessoais, sejam de menores de idade ou de seus responsáveis legais, eventualmente obrigados a instalar aplicativos com baixo nível de segurança da informação para acompanhamento das atividades escolares (Chacon; Bawden Silverio de Castro; Xavier Morales, 2022). Isto sem olvidar, por óbvio, dados e impactos sobre demais titulares, como os do corpo discente, administrativo e técnico.

Iniciativas em nível federal no Brasil direcionadas à promoção e integração do uso de tecnologias na educação remontam aos anos 1980. Todavia, a primeira política pública nacional somente foi promulgada em 1997. Tratava-se do Programa Nacional de Informática Educacional (Proinfo), reformulado em 2007, dando origem ao Programa Nacional de Tecnologia

Educacional (ProInfo Integrado) (Martins; Flores, 2015). Esse programa serviu de base para o surgimento de diversas outras iniciativas normativas voltadas à integração da tecnologia na educação.

Atualmente, o Brasil coleciona três políticas principais que, em âmbito federal, refletem a interseção das tecnologias digitais com as práticas educacionais (em níveis básico e superior). São elas: a Política de Garantia de Acesso à Internet para Fins Educacionais (Lei nº 14.172/2021), a Política de Inovação e Educação Conectada – PIEC (Lei nº 14.180/2021) e a Política Nacional de Educação Digital – PNED (Lei nº 14.533/2023) (Presidência da República, 2021a, 2021a, 2023a). Conquanto sejam marcos relevantes, as políticas demandam complementação para que se viabilizem avanços em prol da consolidação da soberania digital do país. Na sequência, exploram-se brevemente tais políticas.

A Lei nº 14.172/2021 dispõe sobre a garantia de acesso à Internet, com fins educacionais, a alunos e a professores da educação básica pública. Esta deverá ser viabilizada por meio da assistência da União aos estados e ao Distrito Federal (art. 1º). Conforme previsto em Lei (art. 3º), compreende-se como finalidades educacionais: a contratação de soluções de conectividade móvel para execução e acompanhamento de atividades pedagógicas à distância relacionadas aos conteúdos curriculares, por meio do uso de tecnologias da informação e da comunicação; a aquisição de equipamentos, dispositivos eletrônicos e terminais portáteis para acesso a rede de dados móveis ou a rede sem fio nos estabelecimentos públicos de ensino ou fora deles; bem como a contratação de serviços de acesso à Internet em banda larga e de conexão de espaços dos estabelecimentos públicos de ensino a uma rede sem fio, todos endereçados aos beneficiários legais (alunos e professores do ensino médio e fundamental, com a respectiva ordem de priorização).

A Política de Inovação e Educação Conectada (PIEC), oriunda do programa anterior (ProIEC),[72] apresenta-se como uma iniciativa de natureza complementar e tem como objetivos promover a equidade no uso pedagógico dos recursos digitais, ampliar o acesso à inovação, fortalecer a cooperação entre os entes federativos, incentivar a autonomia docente e o

72 O Programa Inovação Educação Conectada (ProIEC), promulgado pelo Decreto nº 9.204/2017, cujo objetivo era, além de fomentar o uso pedagógico dessas tecnologias digitais na educação básica, apoiar a universalização do acesso à internet de alta velocidade.

protagonismo de educadores e estudantes, garantir conectividade de alta velocidade, disponibilizar recursos educacionais digitais e fomentar a formação continuada de professores e gestores voltada a práticas pedagógicas mediadas por tecnologias. Baseada em um modelo importado da Holanda (Centro de Inovação para a Educação Brasileira, 2021), a política se alinha às recentes reformas educacionais, como a uniformização curricular (Leis nº 9.394/1996, nº 13.415/2017 e nº 14.945/2024) (Presidência da República, 1996, 2017, 2024).

Não obstante a existência destas leis e políticas públicas, além de estarem em consonância com a estratégia do Banco Mundial que sublinha a relevância da inclusão de novas tecnologias para o enfrentamento dos problemas atrelados à aprendizagem, a revisão bibliográfica realizada por Souza e Silva denuncia haver "mais discursos nas ações e propostas governamentais do que um real alcance de práticas concretas para o uso pedagógico de tecnologias nas escolas" (Souza; Silva, 2023, p. 7).

Os autores destacam que a vagueza textual da política permite interpretações destoantes: por um lado, potencializando a tecnologia por uma visão determinista e, portanto, como a grande salvadora dos problemas da educação; por outro, uma visão neutra, na qual a tecnologia figura como mero instrumento a ser moldado pelo usuário. Apesar da preocupação com o acesso à Internet e às novas tecnologias, a PIEC não inova ao mirar nas parcerias público-privadas para a formação mais técnica dos indivíduos. Carece de instruções para escolas-membros docentes e administrativos – acerca da necessidade de apropriação educacional das tecnologias e de reestruturação de projetos pedagógicos e curriculares. Nesse sentido, contraria o aprendizado crítico e o fortalecimento da soberania digital.

Similarmente, em 2023 promulgou-se a Política Nacional de Educação Digital (Presidência da República, 2023a) que estabelece como objetivos (art. 2º) a "inclusão digital", a "educação digital escolar", a "capacitação e especialização digital" e a pesquisa e desenvolvimento em Tecnologias Digitais da Informação e Comunicação (TDICs). A política apresenta elementos importantes, como (i) a separação entre educação e capacitação (de habilidades e competências digitais), que são frentes distintas e não devem ser confundidas; e (ii) ressalta o componente multigeracional, já que a educação escolarizada (em nível básico) é apenas um dos eixos pelos quais as ações da política devem permear, mas não o único, considerando o amplo

despreparo acerca do entendimento do funcionamento de tecnologias digitais e dos seus respectivos efeitos.

Para estimular o aprimoramento e atualização constante das políticas educacionais, é necessário avançar em relação ao diálogo multissetorial capaz de enfrentar as múltiplas preocupações e desafios relativos à cibersegurança, junto com mecanismos adequados para a garantia das outras dimensões da soberania digital, como a autodeterminação informativa e a autonomia tecnológica, alcançável sobretudo por meio do desenvolvimento de sistemas e tecnologias digitais nacionais.

O papel da participação pública multinível e multissetorial na identificação dos principais pressupostos da educação digital em segurança cibernética deverá ser valorizado e compreendido na sua centralidade para que as propostas não sejam desconectadas da realidade local – pressuposto para formação da necessária conscientização digital (sem a qual não há soberania), bem como nos seus mais variados campos de alcance, haja vista sua transversalidade.

Como exemplo de iniciativa promovida por perspectivas plurais, destaca-se o Comitê Nacional de Cibersegurança, que reúne representantes relacionados à área de cibersegurança de órgãos do Governo Federal, de entidades da sociedade civil, de instituições científicas e do setor empresarial (Presidência da República, 2023b). O grupo, perante a relevância temática e as evidências já mencionadas, elaborou a nova Estratégia Nacional de Cibersegurança (E-Ciber) e firmou a "proteção e a conscientização do cidadão e da sociedade" como um de seus pilares fundamentais ("Eixo 1"), conforme disposto no artigo. 1º, inciso I, do Decreto nº 12.573/25 (GSI, 2025b).

Pela E-Ciber, objetiva-se criar condições seguras para o uso dos serviços digitais, enfocando em indivíduos vulneráveis como, por exemplo, crianças, adolescentes, idosos e pessoas neurodivergentes (art. 3º). Dentre as ações mínimas voltadas à proteção e à conscientização de cidadãos e da sociedade, no artigo 4º elencaram-se atividades dedicadas *i)* à capacitação de professores e gestores em cibersegurança, incentivo à participação em eventos sobre o tema e à inclusão de conteúdos correlatos nos currículos formativos nacionais em todos os níveis; *ii)* ao robustecimento de órgãos de atendimento e proteção de vítimas de abusos e crimes cibernéticos, fomento à formação continuada de profissionais engajados com entidades de persecução penal de combate de tais condutas criminosas e aprimoramen-

to normativo e estrutural dos canais de denúncia; *iii)* às ações preventivas de combate ao cibercrime, às fraudes digitais e demais ações maliciosas no espaço cibernético, combinadas com a divulgação de conteúdo normativo nacional e internacional sobre os tipos penais com previsões correlatas; *iv)* ao incentivo ao desenvolvimento de planos de contingência institucionais para verificação do grau de cibersegurança de instituições públicas e privadas, bem como à avaliação de modelos flexíveis para garantia da cibersegurança em entidades públicas e, no caso de micro e pequenas empresas e startups, à orientação de ações voltados à gestão de riscos e recuperação das atividades após a ocorrência de incidentes cibernéticos; *v)* a identificação e autenticação de usuários de acordo com a complexidade ou necessidade de proteção, sempre respeitando o direito à privacidade; e, enfim, *vi)* incentivo à atuação segura no espaço cibernético pelo usuário.

Diante do exposto, e convencidos da existência de um enorme capital de criatividade e talento no país, acredita-se que a adoção de iniciativas capazes de promover a soberania digital – como a E-Ciber – possa permitir que o Brasil não somente mitigue suas falésias sociais, mas se torne uma liderança mundial da soberania digital, potencializada pela criação de tecnologias nacionais. Nesta perspectiva, é necessário enxergar brasileiras e brasileiros não somente como consumidores, mas como criadores da tecnologia do futuro.

Para que se alcancem esses resultados, é cogente traduzir as aspirações colocadas nas políticas supracitadas em ações concretas, capazes de estimular e fomentar a educação, a inclusão e a colaboração multissetorial e multigeracional, reconhecendo que, para construir a cibersegurança e a soberania digital do país, as pessoas são a primeira e a última linha de defesa.

2.5.2 Ciber-higiene e educação multigeracional em cibersegurança

A ciber-higiene pode ser definida como o conjunto de práticas preventivas destinadas a garantir a segurança no ambiente digital, sendo comparável à higiene pessoal no que diz respeito à sua relevância, à maneira na qual pode ser integrada – necessariamente por meio de educação – e aos benefícios individuais e coletivos que desencadeia (ENISA, 2024c; Vishwa-

nath *et al.*, 2020). Particularmente, nossa crescente dependência da tecnologia e o avanço em termos de conectividade tornam imprescindível que as práticas de ciber-higiene sejam ensinadas desde a infância, integrando-se ao processo educacional básico.

Assim, a ciber-higiene deve ser entendida de forma análoga à higiene pessoal. Isto é, quando devidamente integrada a uma organização, a ciber-higiene consistirá em rotinas diárias simples, bons comportamentos e verificações ocasionais que fomentam a segurança da organização e/ou do indivíduo em questão (European Union Agency for Network and Information Security, 2016). Contudo, cabe reiterar a relevância do desafio de educar toda a população em cibersegurança, que exige uma abordagem multigeracional e diferenciada, considerando as especificidades de cada faixa etária e os níveis de preparação técnica.

Esta subseção destaca alguns aspectos da educação em cibersegurança, oferecendo algumas pistas para abordar este assunto crucial com crianças, adolescentes, pais, educadores, idosos e técnicos (Belli *et al.*, 2023b; Neigel *et al.*, 2020). O intuito desta subseção é destacar como cada grupo possui necessidades distintas que devem ser entendidas e atendidas para a comunicação efetiva das práticas de ciber-higiene e a construção de uma cultura abrangente de cibersegurança. Como destacado anteriormente, a educação em cibersegurança deve ser inclusiva e adaptada às necessidades específicas dos diferentes grupos populacionais. Desde ensinar crianças sobre os fundamentos da navegação segura até capacitar técnicos para proteger infraestruturas críticas contra ataques sofisticados, todos os segmentos têm um papel essencial na construção de um ambiente digital mais seguro.

A promoção de uma cultura multigeracional orientada pela ciber-higiene requer esforços contínuos no âmbito educacional e comunitário, haja vista que, embora as práticas de ciber-higiene já sejam conhecidas e consolidadas, sua comunicação e integração na população permanecem um desafio. Isto é, há uma resistência social à adoção de medidas de segurança básicas que por vezes vão de encontro a conveniências e facilidades de medidas mais simples de segurança. Nesse sentido, a resistência à adoção de medidas de autenticação de dois fatores ou mesmo senhas complexas surge como exemplo ilustrativo (Nygard *et al.*, 2021). A conscientização coletiva sobre os riscos digitais deve ser acompanhada pela implementação

sistemática de estratégias preventivas que envolvam indivíduos, famílias, escolas e organizações públicas ou privadas.

O esforço da higiene cibernética envolve mudanças culturais e sociais, configurando um esforço realmente hercúleo. Mas somente por meio dessa abordagem integrada será possível enfrentar os desafios crescentes com eficácia. Cabe destacar que este esforço não precisa começar do zero. Ao nível brasileiro, os trabalhos do Cetic.br, ANATEL e RNP, por exemplo, fornecem uma ampla gama de excelentes materiais que podem ser usados para organizar atividades educacionais, e até lúdicas, com o intuito de ensinar a ciber-higiene (CERT.br, 2022).

Porém, apesar da existência de tal material há diversos anos, a população ainda está longe de aproveitá-lo, sendo a divulgação maciça um dos principais gargalos a serem superados para conseguir incrementar os níveis de literacia digital da população brasileira. Como passo fundamental e basilar nessa direção estão as iniciativas direcionadas a diferentes grupos geracionais que precisam ser educados para parar de ser o elo fraco e se tornar o elo forte da cibersegurança.

2.5.2.1 Crianças e adolescentes

As crianças constituem um grupo especialmente vulnerável, uma vez que interagem desde cedo, frequentemente sem a devida supervisão adulta, com o ambiente digital por meio de jogos, redes sociais e plataformas educacionais (CERT.br, 2022). Essa exposição inicial, embora repleta de oportunidades educacionais e recreativas, também as coloca em risco frente a ameaças como cyberbullying, exposição a conteúdos impróprios e golpes online. É fundamental tanto que sejam ensinadas práticas básicas de segurança digital desde cedo, como evitar interações com desconhecidos na Internet, proteger informações pessoais e criar senhas fortes, mediante a utilização de uma linguagem contextualizada e positiva para comunicar de maneira efetiva (Gcaza; Thomson, 2025).

Ademais, cabe aos responsáveis estabelecerem mecanismos de supervisão parental que garantam um uso seguro da tecnologia por parte das crianças e, ao mesmo tempo, exigir que os sites e plataformas acessíveis para crianças disponibilizem tais mecanismos. Assim, como destacaremos na seção seguinte, pais e educadores desempenham um papel fundamen-

tal, porém enfrentam um desafio duplo, ao passo que eles mesmos precisam de treinamento e capacitação em ciber-higiene.

Os adolescentes, por sua vez, possuem maior autonomia no uso da Internet e menor inclinação a escutar recomendações de pais e educadores, o que amplifica os riscos aos quais estão expostos e pode dificultar enormemente a educação em ciber-higiene (NIC.br, 2025). Neste caso, é imprescindível que sejam orientados sobre a importância de configurar adequadamente as opções de privacidade nas redes sociais, identificar mensagens fraudulentas ou links suspeitos e gerenciar o tempo dedicado às atividades online. Paralelamente, deveria ser responsabilidade dos próprios provedores de aplicativos a definição de contas e modalidades para adolescentes, com parâmetros de proteção aprimorada por padrão.

Além disso, é essencial que pais e educadores ensinem uma cultura de respeito no ambiente digital, tal como no ambiente analógico, incentivando comportamentos respeitosos e responsáveis nas interações virtuais e alertando sobre as consequências nefastas que pessoas mais vulneráveis, como crianças e adolescentes, podem sofrer.

2.5.2.2. Pais e educadores

Pais e educadores desempenham uma função crucial na formação das práticas de ciber-higiene e educação das crianças e adolescentes. Enquanto supervisores diretos do uso da tecnologia por parte dos jovens, são também responsáveis por modelar comportamentos seguros no ambiente digital. Para tanto, é necessário que eles mesmos, em primeiro lugar, se eduquem sobre os riscos mais comuns associados à Internet e as ferramentas disponíveis para mitigá-los.

Entretanto, vide a velocidade de permeabilidade e adoção de novas tecnologias, a capacitação de pais e educadores foi tipicamente negligenciada por escolas, faculdades e instituições de ensino[73]. Além disso, pais e

73 Para uma seleção de materiais, cartilhas e cursos de formação para pais e educadores, disponível em: https://internetsegura.br/pais-educadores/. Para uma seleção de cursos on-line gratuitos sobre diversos temas que envolvem o comportamento social e responsável no ambiente digital, ver o Programa de Formação Docente em Direitos Humanos Digitais, desenvolvido em parceria entre FGV e NIC.br. Disponível em: https://cursoseventos.nic.br/curso/programa-formacao-docente-em-direitos-humanos-digitais-fgv-nicbr/.

educadores representam o elemento essencial do estabelecimento de regras claras sobre como a tecnologia pode ser usada no ambiente doméstico ou escolar, incluindo limites para o tempo de tela e critérios para escolha de aplicativos ou plataformas permitidas (CERT.br, 2022).

O diálogo aberto entre pais, educadores e os jovens é igualmente relevante para construir confiança que, exatamente como em qualquer outro setor da cibersegurança, é a peça fundamental para conseguir resolver um problema. Tal abordagem permite que crianças e adolescentes compartilhem suas experiências online sem receio de represálias ou julgamentos severos e, consequentemente, possam ser ajudados a resolver seus problemas antes que se tornem danosos. Paralelamente, o uso de ferramentas tecnológicas como filtros de conteúdo ou softwares de controle parental pode ser empregado para bloquear conteúdos inadequados ou monitorar atividades suspeitas.

A conscientização e a disseminação de informações desempenham um papel fundamental, que pode ser enfrentado usando uma metodologia de ensino baseada em narrativas e resolução de problemas (Karimi *et al.*, 2024). Além disso, cabe frisar que é responsabilidade dos adultos ensinar pelo exemplo ao adotar práticas seguras em suas próprias interações digitais. Tal responsabilidade não deve ser considerada como um ulterior ônus para pais e educadores, mas, ao contrário, como um estímulo à aprendizagem na perspectiva de melhorar, ao mesmo tempo, seu próprio comportamento e sua capacidade de educar seus filhos, preparando-os para enfrentar os desafios e aproveitar os benefícios da tecnologia digital.

2.5.2.3 Idosos

Entre todos os grupos demográficos, os idosos constituem um grupo particularmente vulnerável às ameaças digitais devido à menor familiaridade com tecnologias digitais, conjugada com uma recente digitalização de serviços públicos e privados cada dia mais essenciais para as próprias atividades cotidianas (Medeiros *et al.*, 2020). Essa vulnerabilidade é frequentemente explorada por agentes mal-intencionados, especialmente por meio de golpes online ou fraudes eletrônicas.

Cabe ressaltar que a educação de idosos pode representar um desafio adicional porque pode implicar dificuldades na comunicação e a necessi-

dade de estimular a motivação dos usuários da terceira idade a adquirir habilidades de cibersegurança (Blackwood-Brown; Levy; D'Arcy, 2021). Portanto, a educação em ciber-higiene para essa faixa etária deve ser acessível e prática, priorizando orientações claras sobre como reconhecer mensagens fraudulentas (*phishing*) e engenharia social, evitar compartilhar informações pessoais nas redes sociais e manter dispositivos atualizados com as últimas atualizações de segurança.[74]

Além disso, é recomendável que os idosos busquem apoio técnico confiável quando enfrentarem problemas tecnológicos ou dúvidas relacionadas ao uso da Internet. Oficinas comunitárias voltadas à alfabetização digital podem ser promovidas como forma de inclusão tecnológica desse grupo populacional. A criação de manuais simples com instruções básicas sobre navegação segura também pode contribuir significativamente para aumentar sua confiança no uso da tecnologia.

2.5.2.4 Profissionais técnicos

Os profissionais técnicos ocupam uma posição estratégica na proteção das infraestruturas digitais que suportam empresas e organizações. Sua formação em cibersegurança deve ser aprofundada e contínua, considerando a complexidade crescente e a evolução dinâmica e permanente das ameaças digitais. Entre suas responsabilidades estão a definição e implementação de políticas robustas para gerenciamento seguro de senhas, realização periódica de backups e atualização automática dos sistemas utilizados pelas organizações e sensibilização aos inúmeros riscos de cibersegurança.

Além disso, esses profissionais devem estar aptos a utilizar ferramentas avançadas, como IA defensiva (Belli, 2025c; Malatji; Tolah, 2025), capazes de detectar atividades suspeitas em tempo real e responder rapidamente a incidentes cibernéticos por meio de planos detalhados previamente elaborados. O treinamento contínuo dos colaboradores das empresas sobre ciber-higiene básica também é uma atribuição relevante dos técnicos na mitigação de riscos internos.

74 Ver o Guia Internet com responsa 60+ elaborado pelo Cetic.br. Disponível em: https://nic.br/media/docs/publicacoes/13/internet_com_responsa_60+.pdf.

A atualização constante dos conhecimentos desses profissionais é indispensável diante da evolução acelerada das tecnologias digitais e das ameaças associadas. Participação em cursos especializados e acompanhamento regular das publicações técnicas mais recentes são práticas recomendáveis para garantir sua preparação frente aos desafios contemporâneos.[75]

Exemplo emblemático da transversalidade das medidas de cibersegurança, a capacitação, o treinamento e a educação também podem ser compreendidos de forma holística como instrumentos de política industrial, especialmente quando direcionados ao fortalecimento da capacidade produtiva nacional e à promoção da autonomia tecnológica, como ocorre no caso das tecnologias digitais, tema da próxima seção.

2.6 O papel e as modalidades da política industrial

O Brasil passa, nas últimas três décadas, por um processo de desindustrialização precoce que se manifesta por meio de especialização regressiva de sua base industrial. A especialização regressiva é um processo por meio do qual a indústria de transformação nacional perde relevância e participação no conjunto da economia (Lacerda; Severian, 2023, p. 8). Neste processo, os segmentos que passam a ganhar proeminência na composição da produção nacional são aqueles ligados à exportação de bens de menor conteúdo tecnológico. A desindustrialização precoce, então, é refletida na elevação da participação de produtos importados tanto no consumo aparente nacional quanto nos insumos utilizados pela indústria nacional.

75 Vejam-se, por exemplo, as boas práticas de cibersegurança consolidadas no Programa Internet Segura, desenvolvido pelo NIC.br. Disponíveis em: https://bcp.nic.br/i+seg/.

Figura 4 - Coeficiente de importações da indústria de transformação

Fonte: CNI e FUNCEX (2022).

Este diagnóstico da indústria brasileira já é conhecido, tendo sido abordado a partir de diversas perspectivas. A questão, por exemplo, é muito debatida no campo da saúde, onde a organização do Complexo Econômico-Industrial da Saúde (CEIS) serve como linha-guia para esforços de industrialização com o interesse de criação de capacidade tecnológica, inovativa e produtiva nacional, com casos de sucesso na formação de estruturas de ciência, tecnologia e inovação (CT&I) e da institucionalidade necessária para a coordenação dos atores do sistema.

O exemplo da área da saúde é eloquente porque ilustra um risco já conhecido, mas tornado agudo durante o período da pandemia de COVID-19. Trata-se do risco da dependência tecnológica e produtiva externa, que se traduz em prejuízos relacionados ao desabastecimento, à vulnerabilidade em tomada de preços e a tecnologias desenvolvidas e testadas em contextos estranhos ao local. Assim, as "consequências perversas da desindustrialização, a saber, a perda de empregos de qualidade, a vulnerabilização das contas externas, a queda de arrecadação tributária, […] um fator adicional se mostra mais evidente: a questão da segurança no fornecimento" (Lacerda; Severian, 2023, p. 18).

Se na saúde o problema do desabastecimento é um componente acrescido à problemática da desindustrialização precoce brasileira, no caso da defesa, da segurança e, em específico, da cibersegurança e da ciberdefesa a dependência exterior deságua em considerações a respeito da capacidade

de proteção de interesses nacionais e de ativos altamente valiosos e estratégicos, como dados (pessoais e não pessoais), sistemas, redes, bem como de toda infraestrutura física e digital.

Tanto em um quanto em outro exemplo, movimentos geopolíticos recentes têm ilustrado a relevância do tema. Discussões a respeito do *re-shoring* ou *near-shoring* – essencialmente, a transferência da produção de volta para dentro da jurisdição nacional ou para a área de influência de um país (Szapiro; Cassiolato, 2021, p. 17) – se intensificam diante da constatação das fragilidades decorrentes da dependência tecnológica e produtiva externa. Ademais, a disputa comercial-tecnológica entre Estados Unidos e China, com sucessivos bloqueios comerciais não apenas de produtos, mas de ferramentas e insumos necessários para a inovação e a aplicação de tecnologias inovadoras, como a inteligência artificial (Guzman, 2025), retrata a percepção de que o controle sobre certas capacidades tecnológicas requer uma postura proativa do Estado no direcionamento do setor produtivo e das atividades de CT&I (Ciência, Tecnologia e Inovação). Em certa medida, mesmo intervenções em áreas tecnológicas de aplicação civil podem se espraiar para aplicações militares, e vice-versa, dado que certas tecnologias têm caráter dual.

No caso brasileiro, trabalha-se com o conceito de Base Industrial de Defesa, definido pela Política Nacional da Indústria de Defesa (PNID) como "o conjunto das empresas estatais e privadas, bem como organizações civis e militares, que participem de uma ou mais das etapas de pesquisa, desenvolvimento, produção, distribuição e manutenção de produtos estratégicos de defesa" (BRASIL, 2005, art. 2º, I). A este conceito acrescem-se os de Produto de Defesa (PRODE) – aquele utilizado em atividades finalísticas de defesa –, Produto Estratégico de Defesa (PED) – aquele que é de interesse estratégico para a Defesa Nacional – e suas correspondentes Empresas de Defesa (ED) e Empresas Estratégicas de Defesa.

A conjunção entre a questão da dependência tecnológica decorrente de desindustrialização e especialização regressiva e considerações a respeito da economia de defesa no Brasil, especialmente em relação à cibersegurança e ciberdefesa, delineia a necessidade de integração entre política de cibersegurança e ciberdefesa, política industrial e estratégia de desenvolvimento nacional. Isto passa por se adotar uma visão sistêmica em relação à inovação, estimulando processos de aprendizado dinâmico que sejam conducentes à inovação incremental e radical, e estabelecer as condições ins-

titucionais necessárias em termos de regulação e governança – por exemplo, para facilitar a aplicação industrial do conhecimento científico e das inovações, as aproximações entre atores do sistema (firmas, instituições de pesquisa públicas e privadas), a retroalimentação entre produtores e usuários e o enriquecimento do cenário de financiamento público e privado de pesquisa, desenvolvimento e inovação.

Em relação especificamente às tecnologias digitais, que têm maior interpenetração de considerações relativas a cibersegurança e ciberdefesa, isso significa estimular o fortalecimento da indústria nacional em tecnologias estratégicas de modo a aliviar a dependência tecnológica e identificar franjas de mercado e serviços tecnológicos de alto retorno para a inserção do país em mercados globais de tecnologia, perseguindo estratégias de *catch-up* e *leapfrogging* (Lee; Lim, 2001; Lee; Malerba, 2017). Ou seja, adotar estratégias que visem alcançar o estágio de desenvolvimento tecnológico já atingido por incumbentes, seja por uma trajetória linear de desenvolvimento, seja por processos que "pulam" etapas em trajetórias tecnológicas.

Como já observamos anteriormente, a capacidade de estimular o desenvolvimento tecnológico é essencial para alcançar o objetivo constitucional da autonomia tecnológica e, em última análise, a situação de soberania digital. Neste sentido, Di Césare (In: Niss, 2023, p. 49–75) descreve alguns dos componentes do conceito de "ciberespaço" que apresentam sobreposição ao de "soberania", elaborando considerações a respeito de como a dependência tecnológica nestes campos implica perda de algumas capacidades essenciais da soberania – a democracia traduzida na capacidade de eleição livre de representantes e a "normatividade", ou seja, a capacidade de definição de normas no ciberespaço (Niss 2023, p. 52).

Esta abordagem aponta para elementos da definição provida por Belli (2023d) ao tratar de "boa soberania digital" (*good digital sovereignty*), "que se baseia na ideia de que qualquer entidade (não apenas o Estado) pode ser digitalmente soberana quando é capaz de entender a tecnologia e usá-la em seu próprio benefício" (*id.*). Assim, a ideia de soberania aplicada a tecnologias digitais estaria enraizada nas capacidades de compreender, desenvolver e regular determinadas tecnologias, de modo que o conceito se espraia em manifestações específicas, como a soberania de dados ou a soberania de IA (Belli; Gaspar, 2023b; Belli; Gaspar; Singh Jaswant, 2024). Sob esta perspectiva, a soberania se conecta e é diretamente impactada

pela dependência tecnológica em campos como sistemas/capacidade de computação, redes, cabos submarinos de fibra ótica, criptografia, software, armazenamento e análise massiva de dados (incluindo dados usados para treinamento de inteligência artificial) (Belli, 2025b; Belli e Gaspar, 2023a).

Particularmente, sobre este último aspecto, a consideração da soberania compreende não somente a relação direta entre Estados, mas também apresenta uma visão expandida do sistema internacional em que atores privados têm papel relevante. A dependência demasiada se traduz em processos de extração de valor – em dados pessoais e não pessoais, treinamento de IA, "fuga de cérebros", concentração de patenteamento de tecnologias em países onde estão sediadas as empresas *Big Tech* etc. – que são reforçados pela formação de sistemas corporativos de inovação centrados em companhias transnacionais sediadas em outras jurisdições (Rikap, 2022, 2023a, 2023b; Rikap; Lundvall, 2021).

2.6.1 Tipos de políticas industriais

Em termos concretos, a política industrial sob uma ótica que compreende a intervenção estatal como componente necessário para o estímulo à incorporação do progresso técnico na base produtiva nacional se integra à política tecnológica, tomando a forma de política de inovação. Essa intervenção se dá pelo lado da oferta, com instrumentos de construção de capacidade tecnológica, e pelo lado da demanda, com mecanismos de subsídio à difusão de novas tecnologias. Seus instrumentos podem ser genéricos, mirando o conjunto dos agentes econômicos, ou seletivos, focados em certos grupos de empresas, e incluem, por exemplo:

> subvenção a projetos de alta densidade tecnológica, incentivos fiscais à pesquisa e desenvolvimento, financiamento em condições preferenciais para a inovação, compras do setor público, e a disponibilidade de capital de risco para novos empreendimentos, além de medidas orientadas a garantir a apropriabilidade privada do investimento tecnológico (patentes) e manter padrões técnicos (metrologia, padronização e qualidade) (Ferraz; Paula; Kupfer, 2016, p. 319).

Tais mecanismos poderiam ser aplicados, em conjunto ou separadamente, para estimular a produção de produtos e serviços de ciberseguran-

ça. Tal visão é instrumental para transformar a percepção de cibersegurança como custo em uma oportunidade de desenvolvimento da indústria nacional, com intuito de construir a autonomia tecnológica. Além destes mecanismos de intervenção, ações de fortalecimento do sistema de inovação, como o fortalecimento de instituições científicas e tecnológicas, a formação de recursos humanos especializados, inclusive para conseguir regular o setor eficientemente, como será destacado na próxima subseção, são fundamentais, na perspectiva de estimular o mercado enquanto se controle a soberania nacional.

Outra classificação das alternativas de política industrial que esclarece as ferramentas disponíveis é aquela que as divide em horizontais, ou seja, políticas voltadas para a totalidade da economia, e verticais, ou seja, aquelas com um enfoque setorial específico. As políticas horizontais apresentam um rol de ferramentas de política amplo, incluindo fatores tão variados como a defesa da concorrência, investimentos e controle de infraestrutura, política de comércio exterior e política de propriedade intelectual.

Este tipo de política movimenta incentivos de caráter geral relacionados à inovação (incentivo e fomento à pesquisa e difusão de novas tecnologias), à disponibilidade de capital (crédito e financiamento, estímulos à exportação e importação), incentivos fiscais e compras governamentais. Também lança mão de políticas genéricas, como as de infraestrutura, recursos humanos e ciência e tecnologia (Ferraz; Paula; Kupfer, 2016). Por sua vez, as políticas verticais seriam aquelas em que o Estado "mobiliza parte dos instrumentos anteriormente descritos, focalizando e privilegiando um conjunto de empresas, indústrias ou cadeias produtivas" (*idem*, p. 320).

Pode-se classificar estas políticas, ainda, de acordo com a sua natureza, entre aquelas que atuam sobre o regime de regulação – "a arbitragem do processo concorrencial, englobando a política antitruste e a comercial, assim como regulações referidas à propriedade intelectual, consumidor e meio ambiente" (*ib.*) – visando intensificar a concorrência e aquelas que atuam sobre o regime de incentivos, como medidas fiscais e financeiras com objetivo de estimular pesquisa e desenvolvimento e exportação. Assim, o estabelecimento de autoridades regulatórias ou outros arranjos de governança dotados de recursos intelectuais e econômicos necessários para conseguir fiscalizar e facilitar a implementação de tais políticas é ele-

mento instrumental para o sucesso da política industrial, como destacaremos na próxima subseção.

Todo esse rol de ferramentas de política pública presume uma atuação do Estado não apenas como garantidor de condições de mercado, mas como promotor, direcionador e criador de mercados e da economia, em conformidade com o supramencionado art. 219 da Constituição Federal. Isso está relacionado a um debate sobre a função do Estado na organização de sistemas de inovação e no estímulo ao desenvolvimento econômico. Esse papel pode variar desde a garantia de "condições de mercado" via correção de falhas de mercado até a ideia de um Estado empreendedor, que direciona a inovação e atua na criação de novos mercados.

Mazzucato define esse "Estado empreendedor" como aquele que "investe em áreas de extrema incerteza, buscando influenciar tanto a taxa quanto a direção da mudança" (Penna; Mazzucato, 2016, p. 16). A necessidade de sua atuação, especialmente em etapas iniciais de trajetórias tecnológicas, deve-se justamente ao caráter de incerteza da inovação, que requer investimento paciente e de longo prazo para a realização de seu potencial. Este tipo de investimento, em regra, é provido pelo Estado, como tomador dos riscos da inovação tecnológica, comprador inicial, financiador de atividades de ciência e tecnologia, investidor e credor sob condições especiais para novos empreendimentos, enfim, por meio das ferramentas de política supracitadas.

Esse papel crucial do Estado é comentado por Mazzucato (2018) a partir dos exemplos do nascimento da Internet como projeto com amplo investimento público do departamento de defesa estadunidense, inclusive por meio da criação de uma agência dedicada, a *Advanced Research Project Agency* (ARPA); do setor de biotecnologia com apoio do *National Institutes of Health*; da exploração espacial e aeronáutica a partir do estabelecimento de uma agência governamental dedicada, a *National Aeronautics and Space Administration* (NASA); entre outros.

Sob essa perspectiva, o incentivo estatal é componente central de uma política industrial pautada pela ideia do desenvolvimento via inovação, em perspectiva neoschumpeteriana. Esta é a perspectiva que informa, por exemplo, propostas de políticas orientadas por missões – missões promotoras, concomitantemente, do progresso técnico autóctone e da consecução de objetivos de "bem público" (Mazzucato, 2018; Mazzucato; Ryan-Collins,

2022). Também está na raiz de análises a respeito do *catch-up* e *leapfrogging*[76] de países em desenvolvimento, a partir do reconhecimento de que mudanças no padrão produtivo de um país são necessárias para que ele se desvencilhe de processos estruturais que reproduzem uma relação desigual entre países. De particular interesse, sob esta perspectiva, são os investimentos em indústrias mais dinâmicas, como as indústrias nascentes, de alta tecnologia e associadas a revoluções tecnológicas que desencadeiam mudanças de paradigma tecnológico ou tecno-econômico (Perez; Soete, 1988).

Muitas experiências internacionais ilustram e corroboram a necessidade de atuação estatal concentrada no direcionamento a indústrias de maior conteúdo tecnológico e promotoras de inovação autóctone. Um exemplo eloquente é a trajetória chinesa, conquistando posição de liderança em campos tecnológicos e indústria sofisticados, como as tecnologias quânticas e diversas aplicações de inteligência artificial (Gaida *et al.*, 2023), além de posição relevante em setores como a produção de chips e a produção de componentes da indústria fotovoltaica (Diegues; Roselino, 2021; Luo; Lovely; Popp, 2017). Tais sucessos são resultados diretos de políticas industriais setoriais planejadas e executadas de maneira extremamente bem organizada, criando uma sinergia entre os vários *stakeholders* setoriais por meio de mecanismos de governança capazes de proporcionar uma comunicação, coordenação e cooperação altamente eficientes.

2.6.2 Exemplos de sucesso brasileiro em política industrial

É interessante notar no cenário brasileiro alguns exemplos de esforços no sentido de transição para um modelo de desenvolvimento baseado na inovação por meio de políticas industriais direcionadas. O setor de agronegócio, por exemplo, se posiciona como importante exportador global a partir de aprimoramentos produtivos derivados do sistema de inovação, com relevante integração sistêmica entre os agentes econômicos,

76 Lim *et al*. (2021) definem *leapfrogging* como o desenvolvimento tecnológico que salta fases em uma trajetória linear. Esse desenvolvimento pode ser competitivo ou alternativo, ou seja, pode ocorrer através da criação de um produto que concorre diretamente no mesmo mercado com os produtos das empresas estabelecidas ou através da introdução de um novo produto em um mercado novo.

especialmente "fornecedores de máquinas e equipamentos e de insumos e fertilizantes com institutos de pesquisa e com unidades produtivas agrícolas" (Cassiolato, 2015, p. 276, tradução nossa). Destaca-se a importância da Empresa Brasileira de Pesquisa Agropecuária (EMBRAPA) como ponto fulcral do componente de pesquisa e desenvolvimento do sistema nacional de inovação neste setor (Penna; Mazzucato, 2016).

Na saúde, formou-se no Brasil um sistema de inovação densamente integrado em torno do Complexo Econômico-Industrial da Saúde (CEIS). Este sistema apresenta capacidade científico-tecnológica, na figura de universidades, institutos de pesquisa e um papel particularmente importante da Fiocruz como instituição de pesquisa e desenvolvimento. A capacidade de demanda no sistema é fortalecida pela existência do SUS como comprador de serviços, produtos e equipamentos. A capacidade produtiva vem se fortalecendo, especialmente com a presença e crescimento da indústria nacional de medicamentos genéricos e o aperfeiçoamento produtivo via apoio provido pelo programa BNDES Profarma.[77]

A capacidade estatal está consubstanciada em instituições públicas e burocracia estatal especializada presente no Ministério da Saúde, Fiocruz, Anvisa, BNDES e universidades públicas. A capacidade de política pública se manifesta em uma ampla gama de ferramentas de apoio já mencionadas, como o uso do poder de compra do Estado e incentivos fiscais, bem como a definição de padrões técnicos e a formação de redes de pesquisa via PDPs e outros mecanismos. Finalmente, a capacidade de planejamento, via integração de interesses mais amplos de política de saúde ao desenho

77 O BNDES Profarma é um programa criado pelo Banco Nacional de Desenvolvimento Econômico e Social (BNDES) para apoiar o desenvolvimento da cadeia produtiva farmacêutica no Brasil. Com foco no fortalecimento da indústria nacional, o programa incentiva investimentos em pesquisa e desenvolvimento, aumento da capacidade produtiva e consolidação de empresas de controle nacional. Estruturado em três subprogramas – Investimentos Associados à Produção, Investimentos em Pesquisa e Desenvolvimento e Fortalecimento das Empresas de Controle Nacional –, o Profarma busca reduzir a dependência de insumos importados, melhorar a qualidade dos medicamentos conforme exigências da Anvisa e estimular a inovação, inclusive com o aproveitamento da biodiversidade brasileira. O financiamento pode cobrir até 90% dos investimentos em produção e P&D e até 75% em processos de fusão ou aquisição, com prazos de amortização de até 10 anos, contribuindo para a competitividade e sustentabilidade do setor.

das ferramentas de política industrial sob o marco conceitual do CEIS[78] (Penna; Mazzucato, 2016).

Mazzucato e Penna (2016) destacam, ainda, o caso da EMBRAER como retrato da importância do esforço estatal no direcionamento do progresso técnico:

> A Embraer foi fundada em 1969 a partir de uma visão concebida pelo Estado brasileiro para criar uma indústria aeroespacial do zero (que, portanto, se tornou uma política orientada por missão). O sucesso da Embraer após sua privatização em 1994 é frequentemente reconhecido como um exemplo paradigmático da superioridade das empresas sobre o governo. É verdade que as finanças da empresa estavam em apuros no início dos anos 1990 e melhoraram sob gestão privada. Mas as principais competências tecnológicas da Embraer, que foram a chave para o sucesso nos mercados globalizados com seus jatos regionais, foram adquiridas muito antes, no final da década de 1970, quando era controlada pelo Estado e garantiu acordos de cooperação com outros países como a Itália. Além disso, quando a Embraer assinou um de seus primeiros grandes contratos de venda, com a American Airlines (AA), a operação foi financiada não por bancos privados, que se esquivaram de seu perfil de risco e longo prazo, mas pelo BNDES, que forneceu o financiamento paciente e comprometido de longo prazo. Foi esse acordo com a AA que colocou a Embraer em evidência no mercado global e a ajudou a se tornar uma das líderes mundiais no mercado de jatos regionais (Penna; Mazzucato, 2016, p. 39, tradução nossa).

Os setores de agronegócio, saúde e aviação brasileiros proveem exemplos da importância de organizações de conhecimento (*knowledge organisations*), como a EMBRAPA, EMBRAER e Fiocruz, como instituições de

78 O Complexo Econômico-Industrial da Saúde (CEIS) é um conceito que abrange o conjunto de atividades produtivas, tecnológicas e de serviços relacionados à saúde no Brasil, incluindo a indústria farmacêutica, de equipamentos médicos, biotecnologia e serviços hospitalares. No contexto brasileiro, o CEIS é estratégico para a soberania sanitária e o desenvolvimento nacional, pois busca reduzir a dependência externa de insumos e tecnologias essenciais, fortalecer a capacidade produtiva interna e fomentar a inovação no setor. Ele envolve políticas públicas voltadas para a integração entre o Sistema Único de Saúde (SUS) e a indústria, estimulando parcerias, investimentos em pesquisa e a produção nacional de medicamentos, vacinas e equipamentos médicos, alinhados às demandas da saúde pública (Gadelha; Temporão, 2018).

ancoragem das relações entre os agentes de um sistema de inovação (Assimakopoulos *et al.*, 2022; Penna; Mazzucato, 2016). Também demonstram o papel crucial do Estado como direcionador e provedor de financiamento paciente e de longo prazo, especialmente para as etapas mais imprevisíveis da inovação tecnológica, em uma política industrial voltada ao desenvolvimento via inovação.

Documentos de política pública como o Plano Nacional de IoT (2019) (MGI, 2019) e a Estratégia Nacional de Transformação Digital (2018) (MCTI, [S.d.]) se inserem nos esforços do Brasil frente aos avanços de novas tecnologias digitais. Esta última foi atualizada por uma nova Estratégia de Transformação Digital para o período de 2022 a 2026, que inclui investimentos no desenvolvimento de IA e fomento da capacidade nacional em ciência, tecnologia e inovação. Além do financiamento público não reembolsável, também são aplicadas ferramentas como o uso do poder de compra do Estado via Encomendas Tecnológicas.[79] Porém, essas iniciativas nos parecem ainda extremamente embrionárias, apresentando um nível de organização e sofisticação extremamente limitado, comparado com os exemplos de sucesso analisados anteriormente.

Cumpre destacar a inclusão, dentre as missões da nova política industrial do atual governo, a "Nova Indústria Brasil: Plano de ação para a neoindustrialização 2024-2026", a preocupação com a perspectiva da soberania e da defesa condicionadas pelo controle de determinadas tecnologias (CNDI, 2024, destaque nosso):

> Missão 1: Cadeias agroindustriais sustentáveis e digitais para a segurança alimentar, nutricional e energética
> Missão 2: Complexo econômico industrial de saúde resiliente para reduzir as vulnerabilidades do SUS e ampliar o acesso à saúde
> Missão 3: Infraestrutura sustentável, saneamento, habitação e mobilidade para integração produtiva e bem-estar nas cidades
> Missão 4: Transformação digital da indústria para aumentar a produtividade

79 "Encomendas Tecnológicas" são uma modalidade de "contratação de pesquisa e desenvolvimento para a criação e aplicação de solução tecnológica inovadora não disponível no mercado, a ser utilizada ou apropriada pelo Estado, na presença de risco tecnológico, que pode incluir a aquisição subsequente em larga escala do produto final gerado, para atender a uma demanda pública específica" (AGU, 2021, p. 3).

Missão 5: Bioeconomia, descarbonização e transição e segurança energéticas para garantir recursos para as gerações futuras
Missão 6: Tecnologias de interesse para a soberania e defesa nacionais

O Nova Indústria Brasil representa um esforço do atual governo de recuperação da industrialização e das capacidades tecnológicas do país após período de estagnação (Lacerda; Severian, 2023; "Orlando Silva", 2024), o que, como já comentado, está conectado a considerações de soberania e dependência tecnológica. Este tipo de dependência, por sua vez, resulta em um espaço de política pública[80] reduzido para o país por meio da submissão a regras estabelecidas por atores estrangeiros, sejam Estados ou corporações transnacionais monopolistas intelectuais.[81]

Por fim, como destacaremos na próxima subseção, a criação de arranjos de governança capazes de monitorar o setor e facilitar a implementação da política industrial, proporcionando a comunicação, coordenação e cooperação multissetorial, pode ser considerada em si como um elemento da política industrial.

2.6.3 A governança da cibersegurança como elemento de política industrial

A construção de uma estrutura de governança dotada de recursos suficientes e capacidade técnica adequada configura-se como força motriz institucional para a eficácia das políticas industriais contemporâneas, conforme demonstrado pela literatura especializada em economia regulatória e governança setorial.[82] Essa premissa fundamenta-se em algumas dimen-

80 Ver Ardissone (2017) sobre a ideia de "espaço de política pública" na formulação da política industrial brasileira no contexto das negociações do Acordo TRIPS. Veja Jackson (2021) para uma revisão da literatura sobre o conceito de espaço político.

81 O conceito de "monopólios intelectuais" desenvolvido por Rikap e Lundvall (2022) refere-se à capacidade das grandes empresas de tecnologia de dominar a criação de valor por meio da formação de sistemas de inovação corporativa em escala global. Ao fazê-lo, essas empresas determinam as regras de produção e circulação de ativos intangíveis, sejam dados, informações ou conhecimento. O conceito fala de como essas empresas empregam várias estratégias para garantir o fluxo de valor a seu favor, reduzindo a autonomia de outros atores (estatais e não estatais) no processo.

82 O papel da regulação e das autoridades reguladoras é particularmente relevante no que diz respeito às políticas industriais orientadas ao desenvolvimento tecnológico. Ver Kuo, C., Shyu, J.,

sões interligadas, analisadas à luz de marcos teóricos e estudos empíricos que envolvem desde agentes públicos no nível ministerial até executores públicos e privados.

Em primeiro lugar, uma perspectiva institucionalista de economia política reconhece que instituições — incluindo autoridades regulatórias — não apenas corrigem falhas de mercado, mas constituem a ação humana, inclusive no Estado ou em mercados, definindo direitos, obrigações e formas legítimas de participação. Nesse sentido, o Estado atua como arquiteto institucional do funcionamento e da evolução dos mercados por meio de instrumentos como planejamento estratégico e incentivos à inovação (Chang, 2002). Essa abordagem, no contexto de políticas industriais modernas, permite fomentar empresas que se tornem competitivas globalmente ("campeãs nacionais") promovendo uma abordagem híbrida que combine política desenvolvimentista (Wade, 2012) em setores identificados como estratégicos com mecanismos de mercado e padrões de governança regulatória compatíveis com diretrizes internacionais como as da OCDE (OECD, 2012, 2015).

Em seguida, a independência regulatória, longe de constituir mera delegação técnica, assume caráter democrático ao assegurar transparência, prestação de contas e equilíbrio entre interesses públicos e privados (Estache; Martimort, 1999; Rodrik, 2004). Estudos de caso em setores como energia e telecomunicações demonstram que arranjos institucionais claros – incluindo procedimentos decisórios públicos, mecanismos de *stakeholder engagement* e controle judicial – elevam a legitimidade social (Jacobi, 2015; Belli, 2015) das políticas industriais além de incrementar a qualidade regulatória (Belli, 2015).

Como alerta North (1991), instituições fracas geram custos transacionais incompatíveis com o desenvolvimento industrial sustentável. Tal consideração é essencial ao se pensar qual tipo de configuração administrativa deverá ter a futura Autoridade Nacional de Cibersegurança. Neste sentido, o "custo" de uma autoridade deve ser enxergado, em realidade, como um investimento necessário.

& Ding, K. (2019). Industrial revitalization via industry 4.0 – A comparative policy analysis among China, Germany and the USA. Global Transitions. Disponível em: https://doi.org/10.1016/J.GLT.2018.12.001.

Por fim, setores industriais baseados em tecnologias emergentes (IA, computação quântica, biotecnologias, energia limpa etc.) demandam modelos regulatórios ágeis, aptos a gerir riscos sistêmicos e fomentar ecossistemas inovadores. Como argumentam Baldwin, Cave e Lodge (2012), autoridades técnicas capacitadas permitem transitar entre regulação *ex ante*, corregulação setorial e mecanismos de autorregulação assistida, garantindo segurança jurídica sem asfixiar a criatividade empresarial. Essa flexibilidade institucional é particularmente relevante em políticas industriais orientadas à transformação digital do país e à promoção de um setor brasileiro de produtos e serviços em cibersegurança, nas quais a coordenação público-privada torna-se condição para a competitividade global.

Nessa perspectiva, cabe ressaltar que a literatura mencionada (Levi-Faur, 2011; Majone, 1997; North, 1991; Rodrik, 2004) converge ao afirmar que a capacidade regulatória constitui pilar estruturante de capacidade de atuação estatal, transcendendo visões reducionistas que a limitam à correção de falhas de mercado. Isto pode tomar diferentes formas, desde órgãos de governo até autoridades independentes, sendo necessário priorizar, como indica Rodrik (2004), o aproveitamento de "bolsões de excelência burocrática […] [concentrando] atividades nessas agências, em vez de criar novas agências do zero ou usar as existentes com histórico ruim" (id., 2004, p. 23). O autor destaca, ainda, a necessidade de mecanismos claros de controle político dessas estruturas de governança, que devem "ser monitoradas de perto por um agente com interesse claro nos resultados e que tenha autoridade política no mais alto nível" (id., 2004, p. 24). Como sintetiza Stiglitz (2018), em economias cada vez mais baseadas em conhecimento e redes globais de valor, a qualidade das instituições reguladoras determina a capacidade das nações de converter investimentos em crescimento inclusivo e sustentável.

Apesar das diferentes visões e abordagens, esse entendimento converge com a literatura neoschumpeteriana e a abordagem sistêmica da inovação na consideração do Estado como ator chave no desenvolvimento socioeconômico e tecnológico por meio de uma postura ativa consubstanciada em instituições e políticas públicas. Tratando-se de um tema como a cibersegurança, que, como comentado, apresenta interpenetrações significativas com questões de governança, esse papel é ainda mais fortemente enraizado no Estado. Porém, como destacamos na seção 2.1.3, a governança e eventual

construção de uma Agência Nacional de Cibersegurança exige arcabouço jurídico claro, dotação orçamentária adequada e mecanismos permanentes de capacitação técnica – desafios que permanecem centrais e, no momento da publicação deste trabalho, ainda não resolvidos no Brasil.

2.7 Tecnologias disruptivas e os desafios da inteligência artificial (IA)

Dada a amplitude e a transversalidade dos processos de digitalização e da cibersegurança, é notável o destaque que o debate sobre os impactos da IA vem assumindo, seja do ponto de vista ofensivo ou defensivo. A adoção da IA, embora traga vantagens em termos de capacidade técnica e operacional, também transforma o cenário competitivo, nos âmbitos econômico e político, configurando o que pode se definir como inovação disruptiva (Pfaff, 2020; Sontan; Samuel, 2024). Contudo, como aferido anteriormente, os ganhos decorrentes dessa inovação podem ser utilizados na exploração de vulnerabilidades inerentes a outras tecnologias digitais que compõem o ciberespaço.

No Brasil, a ausência de um marco regulatório específico para a IA, bem como de uma lei geral de cibersegurança, resulta em uma governança dispersa, com a regulação desses temas compartilhada entre múltiplos atores. Nesse cenário, órgãos públicos e empresas privadas enfrentam o desafio de implementar medidas eficazes sem o respaldo de uma política nacional definida e implementada. As autoridades com competência regulatória sobre os impactos da IA na cibersegurança estão distribuídas entre diversos atores, incluindo órgãos governamentais, instituições militares e empresas privadas, que desempenham uma importante função de autorregulação e exercem um papel fundamental na proteção da infraestrutura crítica e na garantia da segurança da informação.

Cabe frisar que a relação entre IA e cibersegurança depende do modo como a primeira é usada para impactar a segunda, seja por meio de aplicações defensivas, ofensivas ou adversariais. Embora já exista um corpo considerável de pesquisa sobre os aspectos técnicos de I.E. cibersegurança, separadamente, ainda são escassos os estudos que abordam interações entre

IA e cibersegurança sob a perspectiva da governança e regulação (Jiang; Belli, 2024; Malatji; Tolah, 2024).

Nesse sentido, é importante distinguir, inicialmente, IA defensiva e IA ofensiva. A IA defensiva geralmente utiliza aprendizado de máquina e outras técnicas de IA para melhorar a cibersegurança e aumentar a resiliência de sistemas, redes e bancos de dados, além de proteger indivíduos contra ameaças cibernéticas. Nesse contexto, sistemas baseados em IA podem aumentar a eficácia de controles de segurança destinados à proteção de ativos específicos, como por meio de análise automatizada de *malware*, firewalls ativos, operações automatizadas de inteligência de ameaças cibernéticas, além de apoio em processos de tomadas de decisão (Geluvaraj; Satwik; Kumar, 2018; Malatji; Tolah, 2024; Sontan; Samuel, 2024).

Em contraste, a IA ofensiva, também conhecida como ataques cibernéticos com IA, envolve o uso de IA para lançar atividades maliciosas, como desenvolver novos tipos e estratégias de ataques ou automatizar a exploração de vulnerabilidades existentes. Destaca-se que a IA adversarial é uma subcategoria da IA ofensiva e se refere à manipulação de sistemas de IA para causar previsões incorretas. Isso pode ocorrer por meio da alteração de dados de entrada ou do envenenamento dos dados de treinamento utilizados na construção do sistema (ENISA, 2023; Sontan *et al.*, 2024).

Assim, a integração de capacidades de IA tem o potencial para ampliar a eficácia, o escopo, a escala e a precisão de operações maliciosas. Essa evolução representa uma mudança de paradigma no panorama da cibersegurança, alterando fundamentalmente a natureza tanto das estratégias ofensivas quanto defensivas (Belli, 2024a; Sontan; Samuel, 2024).

Além disso, o uso da IA impacta o ecossistema da cibersegurança de múltiplas formas. A primeira, e mais abrangente, decorre da democratização e do aumento da sofisticação das ferramentas disponíveis, permitindo que criminosos automatizem e aprimorem ataques, tornando-os mais eficazes, impactantes, dinâmicos e difíceis de detectar. Algoritmos de aprendizado de máquina, por exemplo, podem analisar grandes volumes de dados para identificar vulnerabilidades em sistemas e redes, permitindo que os atacantes explorem essas fraquezas com maior precisão. Campanhas de *phishing* automatizadas podem ser adaptadas a indivíduos específicos com base em dados obtidos em mídias sociais e outras fontes. Essa personali-

zação aumenta a probabilidade de sucesso, já que as mensagens parecem mais convincentes e relevantes para o destinatário.

Em segundo lugar, a IA é capaz de expandir o alcance das ameaças cibernéticas, permitindo que os atacantes gerenciem e executem operações em grande escala com mínima intervenção humana. *Botnets* baseadas em IA podem ser usadas para lançar ataques de negação de serviço (DDoS) em massa, sobrecarregando e desabilitando redes. Ataques de *ransomware* também estão se tornando mais sofisticados, com *malware* impulsionado por IA capaz de se espalhar autonomamente por redes, criptografando dados e exigindo resgates. Ademais, a IA pode facilitar ameaças internas, pois os atores maliciosos podem usar modelos de aprendizado de máquina para prever, emular e manipular o comportamento dos funcionários (Belli *et al.*, 2023b).

Em terceiro lugar, os sistemas de IA podem aumentar significativamente a capacidade dos atacantes de analisar conjuntos de dados complexos e reconhecer padrões, permitindo executar ataques altamente direcionados e precisos. Por exemplo, a IA pode ser usada para identificar alvos de alto valor em organizações e adaptar ataques às suas funções e responsabilidades específicas. A tecnologia também possibilita a criação de falsificações realistas de áudio e vídeo, conhecidas como "*deepfakes*", que podem ser usadas em ataques de engenharia social para manipular indivíduos a divulgar informações sensíveis ou autorizar transações fraudulentas (Malatji; Tolah, 2024).

A criação de mídias sintéticas altamente convincentes que podem ser empregadas para orquestrar campanhas de desinformação com fins financeiros e políticos. Como frisado na seção 1.4, essas tecnologias representam uma nova ameaça à cibersegurança de processos democráticos, permitindo que atores maliciosos manipulem informações em uma escala e complexidade sem precedentes.

Por fim, embora a integração da IA tenha capacitado atores maliciosos a conduzir ataques mais eficazes, abrangentes e precisos, ela também ressalta a importância de estratégias de cibersegurança proativas e adaptativas. Isso inclui investir em inteligência avançada contra ameaças, sistemas de detecção de anomalias e ferramentas de monitoramento contínuo que aproveitam o aprendizado de máquina para identificar efeitos incomuns. Neste contexto, a literacia digital adquire uma relevância ainda maior, considerando que os programas de capacitação em cibersegurança devem ser atualizados para

sensibilizar e preparar os usuários sobre as táticas em evolução dos ataques, impulsionados ou não por IA, enfatizando a importância de uma postura vigilante, pensamento crítico e adoção de boas práticas.

Ainda que o presente trabalho se concentre na cibersegurança, é importante ressaltar que, ao fomentar a colaboração entre entidades governamentais, organizações do setor privado e instituições de pesquisa, o Brasil pode abordar de forma proativa os desafios apresentados pela IA nesse domínio. Essa abordagem multissetorial será essencial para desenvolver regulamentações efetivas, implementar medidas robustas de cibersegurança e promover inovação em tecnologias defensivas baseadas em IA para proteger a infraestrutura crítica da nação e proteger seus cidadãos de ataques cibernéticos, impulsionados ou não por IA.

3 Os Caminhos Sinérgicos da Soberania Digital e Cibersegurança

É importante reiterar que a soberania digital é um objetivo que pode ser almejado e alcançado não somente por Estados. Dependendo da política ou iniciativa em questão, o "soberano digital" pode ser um indivíduo, uma comunidade, uma corporação, um Estado ou até uma entidade supranacional capaz de compreender o funcionamento das tecnologias usadas, definir autonomamente seu desenvolvimento digital e exercer controle sobre os ativos digitais usados (Belli; Jiang, 2024). Tal situação, definidora da soberania digital, permite entender os riscos e benefícios das tecnologias digitais e, portanto, incrementar sua cibersegurança (Belli *et al*., 2023a). Assim, para se tornar soberanos digitalmente, é necessária a adoção de uma abordagem sistêmica e integrada, capaz de entender as interconexões entre as diferentes camadas que compõem a "pilha" das tecnologias digitais, e que implicam a pesquisa e desenvolvimento, a governança e a regulação não somente de *i)* dados; *ii)* software; e *iii)* hardwares; mas também da *iv)* conectividade entre esses ativos; *v)* da educação necessária para entender como funcionam; e da *vi)* cibersegurança de tais ativos (Belli, 2023d).

As dimensões mencionadas são fundamentalmente interconectadas e o fato de que as estratégias e arcabouços regulatórios considerem esses "setores" de maneira separada e fragmentada representa em si uma enorme vulnerabilidade sistêmica. O exemplo brasileiro não poderia ser mais eloquente: como analisamos nesse volume, já existem várias regulações setoriais de cibersegurança no país, mas para nenhum setor regulado a cibersegurança é uma prioridade, sendo somente uma preocupação secundária, à qual pouquíssimos reguladores dedicam recursos específicos. A necessidade de se adotar políticas e mecanismos de governança aptos a entender e gerenciar as interdependências e as potenciais vulnerabilidades existentes entre essas camadas torna-se cada vez mais relevante, à medida que a tecnologia avança e um número crescente de atividades críticas para nossas sociedades, economias e democracias são conduzidas online,

se tornando dependentes do bom funcionamento das tecnologias digitais (Belli *et al.*, 2022).

Portanto, a construção da soberania digital almeja evitar a dependência digital e incrementar a cibersegurança por meio da promoção da autonomia tecnológica e do desenvolvimento socioeconômico. No entanto, cabe reiterar que limitar ou evitar a dependência tecnológica não significa se isolar e instaurar uma autarquia digital. Ao contrário, significa ter uma visão desenvolvimentista, capaz de reconhecer o papel positivo da política industrial, e cooperativa, capaz de promover não somente o desenvolvimento, mas também o uso de um amplo leque de tecnologias inclusive importadas, à condição de que os riscos que tais tecnologias implicam sejam conhecidos e que a regulação pátria seja devidamente respeitada.

De um lado, a soberania digital requer a promoção de um maior número de iniciativas voltadas à pesquisa, desenvolvimento, capacitação e inovação e organizar tais iniciativas de maneira sistêmica. De outro lado, precisa aumentar as opções tecnológicas utilizáveis para reduzir eventuais dependências, promovendo não somente parcerias e cooperações internacionais, mas também a interoperabilidade técnica e legislativa de tais iniciativas (Belli; Zingales, 2023). Assim, uma abordagem voltada à criação e ao fortalecimento de sistemas integrados é essencial para evitar que esforços enormes sejam desperdiçados e que a adoção de novas tecnologias signifique inevitavelmente se submeter ao uso de sistemas controlados por terceiros e cujos potenciais riscos não são entendidos.

Infelizmente, a ausência de pensamento estratégico sobre transformação digital soberana leva inevitavelmente a uma situação de colonização digital, na qual indivíduos, entidades, organizações ou até nações se tornam meros consumidores de tecnologias cujo uso e desenvolvimento não é definido de forma autônoma, mas sim regulado por terceiros, frequentemente guiados por lógicas extrativistas e de concentração (Belli, 2023d; Couldry; Mejias, 2024; Pinto, 2018; Zuboff, 2019b). Portanto, para alcançar a soberania digital, é essencial promover uma abordagem crítica da transformação digital e das próprias tecnologias digitais, fundamentada na capacidade de entender e conseguir controlar as tecnologias adotadas. Cada tecnologia digital é vulnerável a ataques, que ocorrem com frequência diária, tanto no Brasil quanto no resto do mundo. Portanto, o

entendimento do funcionamento e o controle das tecnologias são elementos essenciais e instrumentais à garantia da cibersegurança.

No âmbito da transformação digital, setores inteiros da economia e da sociedade (como educação, finanças, justiça e saúde), incluindo infraestruturas críticas brasileiras, estão sendo digitalizados e automatizados na tentativa de reduzir custos e aprimorar eficiência. Entretanto, como demonstra o crescimento exponencial de ciberataques sofridos pelo Brasil (Fortinet, 2022), a transformação digital frequentemente ocorre sem a devida consideração dos riscos decorrentes da falta de cibersegurança (Solar, 2020). Isto é, o aumento do número de dispositivos e de conexões corresponde a uma superfície de ataque maior e mais difusa, comumente não tratada por esforços sistêmicos de cibersegurança. Para promover o desenvolvimento seguro e utilizar ativos digitais protegendo-os contra ciberataques e outras ameaças digitais, é essencial estabelecer uma gama de medidas que fortaleçam ao mesmo tempo a cibersegurança e a soberania digital.

Essas medidas precisam ser organizadas com base em duas vertentes regulatórias combinadas por meio de uma governança capaz de proporcionar uma organização sistêmica (Belli *et al.*, 2023b). Uma vertente regulatória que pode ser definida como "clássica" precisa definir mecanismos de avaliação e mitigação de riscos, por meio de regulamentações setoriais, padrões mínimos de segurança, normas técnicas e sistemas de monitoramento. De outro lado, uma vertente regulatória que pode ser definida como "regulação facilitadora" e precisa ser embasada numa política industrial digital organicamente estruturada precisa proporcionar o desenvolvimento de tecnologia cibersegura, junto com a formação e capacitação de indivíduos aptos a entender e enfrentar riscos cibernéticos, explorando os elementos definidos na seção 1.7. Com intuito de promover a pesquisa e desenvolvimento e, sobretudo, a capacidade de traduzir a inovação em produtos e serviços que possam ser adotados nacionalmente e, idealmente, exportados internacionalmente.

Para que essas medidas sejam concebidas e implementadas de forma correta e efetiva, é fundamental estudar as estratégias regulatórias e de desenvolvimento já existentes, com particular atenção às experiências de outros países em desenvolvimento, a fim de identificar as melhores práticas e opções mais adequadas e eficientes que podem ser aplicadas ao caso brasileiro (Belli, 2021a; Belli; Galdino de Magalhães Santos, 2024; Belli; Jiang,

2024). Como destacamos na seção 2.6, tais práticas incluem a realização de investimentos estratégicos por meio de uma política industrial bem estruturada, que fortaleça o desenvolvimento de capacidades, pesquisa, criação e manutenção de infraestruturas digitais robustas, para garantir atualização contínua não somente de hardware e software, mas também da força de trabalho. No Brasil, apesar de 84% da população afirmar se conectar à Internet com regularidade, menos da metade possui habilidades básicas como copiar e colar textos ou ativar configurações de segurança e privacidade (Hoepers, 2024). Essa situação pode – e deve – ser revertida somente por meio da capacitação, graças à qual o ser humano pode se tornar o elo mais forte ao invés de ser o mais fraco da cadeia da cibersegurança, como destacamos na seção 2.5.

Cabe reiterar que, para plena realização de soberania digital e o consequente aprimoramento da cibersegurança, é essencial uma forte ação de capacitação e treinamento multigeracional, direcionada não somente as novas gerações, mas também àquelas que, embora já tenham concluído a educação básica (sobretudo considerando as negações ao direito à educação que caracterizam a realidade brasileira), nunca foram preparadas para os desafios da tecnologia digital (Belli *et al.*, 2023b). O cenário é ainda mais preocupante, considerando que a grande maioria da população desconhece a lógica de funcionamento das tecnologias digitais usadas cotidianamente. Sendo mera consumidora de tais tecnologias, atuando de forma inconsciente, a população brasileira inviabiliza sua habilidade de contribuir para o aprimoramento da cibersegurança nacional e, ainda menos, a criação de ferramentas nacionais para enfrentar as ciberameaças de maneira efetiva.

Tal falta de preparo e conhecimento crítico da população cria uma das maiores vulnerabilidades sistêmicas em termos de cibersegurança e impossibilita a construção de uma nação digitalmente soberana. Neste sentido, o Brasil precisa de uma estratégia de soberania digital que tenha a cibersegurança, a capacitação individual e o desenvolvimento tecnológico na perspectiva da autonomia, como pilares centrais da soberania nacional. Isso implica estimular investimentos estratégicos por meio de uma política industrial digital, fortalecer o arcabouço institucional e regulatório por meio de uma Lei Geral de Cibersegurança e uma Agência Nacional de Cibersegurança e, acima de tudo, fortalecer os recursos humanos, com políticas educacionais transgeracionais (Belli *et al.*, 2023b).

Embora o Brasil ainda não possua uma estratégia explícita de soberania digital, o país oferece exemplos interessantes de como esta concepção pode ser construída, seja por meio de uma abordagem *top-down* (de cima para baixo) ou *bottom-up* (de baixo para cima). Nesse sentido, infraestruturas públicas digitais podem ser importantes vetores de soberania digital, (Belli, 2023d; Belli; Jiang, 2024) ainda que tipicamente criadas e gerenciadas de maneira *top-down* pelo Estado. A título de exemplo, o sistema de pagamento Pix, criado pelo Banco Central do Brasil, permitiu ao Brasil reduzir a dependência de atores estrangeiros, como as empresas Visa e MasterCard, no que se refere aos pagamentos, reduzindo custos e proporcionando um ecossistema inovativo (Belli, 2023b).

A soberania digital também pode ser alcançada por meio de iniciativas *bottom-up*, como ilustram os inúmeros exemplos de redes comunitárias,[83] que permitem a comunidades locais construir e gerenciar sua própria infraestrutura de acesso à Internet como um bem comum (Belli; Hadzic, 2023). Outra abordagem que pode ser mencionada é o cooperativismo de plataforma, que possibilita a grupos de trabalhadores e desenvolvedores se associarem para fornecer serviços digitais de forma colaborativa, inclusive por meio de software em código aberto (Grohmann, 2022).

O Brasil, portanto, não está fadado a ser uma colônia digital. Na verdade, pode-se até afirmar que o país foi um precursor da soberania digital, especialmente considerando as políticas da primeira administração Lula que, já em 2003, promoviam a adoção e o uso de software livre, com intuito de direcionar o país rumo à autonomia tecnológica. Porém, cabe frisar que

83 As redes comunitárias são iniciativas colaborativas e descentralizadas, construídas e operadas pelas comunidades locais como bens comuns digitais para superar as divisões digitais e alcançar a "autodeterminação" (Belli, 2018), provando que a conectividade à Internet pode ser construída pelas próprias comunidades locais, para benefício delas mesmas. Essas estratégias alternativas e complementares para a expansão da conectividade são a essência da autodeterminação e da autonomia, demonstrando que as comunidades locais podem se tornar protagonistas de seus futuros digitais, desenvolvendo suas próprias infraestruturas digitais, serviços e conteúdo. Mulheres quilombolas brasileiras, comunidades rurais e cidadãos marginalizados tornaram-se protagonistas de seus futuros digitais ao construírem suas próprias redes comunitárias, aprendendo a criar literalmente novas partes da Internet que atendem às necessidades das comunidades locais, com base nas características das próprias comunidades locais. Em outras palavras, até mesmo comunidades locais de indivíduos anteriormente não conectados podem ser digitalmente soberanas, compreendendo e desenvolvendo tecnologia, e promovendo seu desenvolvimento econômico, social e cultural.

a experiência brasileira de software em código aberto fracassou, apesar do pioneirismo e das boas intenções, justamente porque não conseguiu proporcionar uma visão sistêmica, voltada não somente a encorajar a adoção de tecnologia *open source* mas também a facilitar a produção de soluções que possam ser usadas de maneira segura, econômica e facilmente acessível. Uma política pública voltada à promoção do *open source* como ferramenta de soberania digital e de fortalecimento da cibersegurança não pode deixar de considerar que raramente tecnologias se tornaram difundidas sendo caras e/ou complexas de usar.

Ao contrário, ao longo das últimas décadas, ferramentas de *open source* foram apoiadas e até integradas por grandes empresas de tecnologias – como a integração do Linux pela IBM ou a produção de Large Language Models (LLMs) em acesso livre ou código aberto como o modelo Llama da Meta ou os modelos R1 e V3 da Deepseek – quando foram enxergadas como oportunidades não somente para reduzir custos, mas também para incrementar sua capacidade de influenciar o desenvolvimento e eventual regulação do mercado por meio da tecnologia *open source* (Belli *et al.*, 2023b).

Assim, parece necessário ressaltar que o Brasil, como qualquer país, precisa enxergar as tecnologias digitais que compõem o ciberespaço como sistemas que, precisam de uma abordagem sistêmica para serem entendidos, regulados e protegidos. Nesta perspectiva, a jornada rumo à soberania digital e à cibersegurança deve ser enxergada como uma oportunidade para estruturar seu desenvolvimento de maneira a explorar a transformação digital cibersegura como uma oportunidade de fortalecimento da economia, da sociedade e da democracia brasileira.

Nessa perspectiva, esta seção enfatiza que somente uma abordagem voltada a alcançar o objetivo constitucional da autonomia tecnológica pode permitir ao país construir uma cibersegurança efetiva e inclusiva, se tornando protagonista do próprio futuro digital. A promoção de uma boa soberania digital, baseada no desenvolvimento tecnológico seguro e sustentável, pode permitir ao país retomar seu papel de liderança nas políticas digitais, não somente em nível regional, mas também em âmbito global (Belli, 2024a; Belli; Jiang, 2024).

4 Conclusão: Rumo a uma Nova Governança da Cibersegurança no Brasil

Conforme evidenciado ao longo deste trabalho, bem como em estudos anteriores (Belli *et al.*, 2023b; Belli; Gaspar, 2023b; Goldoni; Rodrigues; Medeiros, 2024), a cibersegurança constitui um tema multifacetado que ganhou centralidade a partir do discurso de securitização do ciberespaço e dos ativos digitais. Tal relevância decorre da crescente interdependência dos sistemas digitais e do valor estratégico que estes representam para o país, inserindo a questão no centro do debate sobre formulação de políticas públicas.

Na primeira parte desta obra, demonstrou-se como a noção de segurança, tradicionalmente associada ao domínio político-militar, passou a abranger também as dimensões econômica e social, por meio do processo de securitização. Essa evolução permitiu a consolidação da cibersegurança como um campo específico dentro dos estudos de segurança (Hansen; Nissenbaum, 2009). Observou-se que não há consenso acadêmico quanto à sua definição, embora a conceituação mais holística proposta pela União Internacional de Telecomunicações (ITU-T) seja amplamente adotada.

Para os fins deste estudo, cibersegurança foi compreendida como o conjunto de iniciativas voltadas à proteção de objetos de referência, inclusive pessoas, contra riscos cibernéticos. Neste sentido, a proteção e empoderamento individual passam a ser um objeto de referência fundamental da cibersegurança, como demonstra a escolha de considerar a "Proteção e Conscientização do Cidadão e da Sociedade" como primeiro eixo estruturante da recém-adotada E-Ciber (GSI, 2025a).

Foi igualmente realizada a distinção entre ciberdefesa e cibersegurança, com exame do papel das infraestruturas críticas (ICs) e dos serviços essenciais, fundamentais para o funcionamento da sociedade. Verificou-se que, em determinados contextos, esses elementos podem ser objeto simultaneamente da regulação em cibersegurança e de ações de ciberdefesa, o que reforça a necessidade de coordenação e cooperação entre os múltiplos atores que atuam nesse ecossistema.

A análise contemplou ainda uma taxonomia das ameaças e vulnerabilidades exploradas por ataques cibernéticos, incluindo aquelas derivadas da ausência de medidas básicas de segurança. Nesse sentido, defendeu-se a adoção de uma abordagem baseada em direitos fundamentais, que coloque o ser humano no centro das ações de cibersegurança, de modo a viabilizar a construção de um ambiente digital seguro e democrático.

Encerrando a primeira parte, discutiu-se a relação entre cibersegurança e soberania digital. Destacou-se que a interdependência entre ambas requer políticas industriais e mecanismos de governança capazes de fomentar investimentos estratégicos voltados a incrementar a autonomia tecnológica do país e fortalecer a literacia digital, por meio da capacitação, educação e formação contínua da força de trabalho.

Na segunda parte, foram apresentados seis pilares essenciais à consolidação da cibersegurança: *i)* governança; *ii)* mecanismos de segurança da informação; *iii)* combate ao cibercrime; *iv)* literacia digital; *v)* política industrial; e *vi)* tecnologias disruptivas, com ênfase na inteligência artificial (IA). A análise de cada pilar considerou a integração de medidas previstas na Estratégia Nacional de Cibersegurança (E-Ciber/2025), promulgada em 5 de agosto de 2025, no contexto da política instituída pela PNCiber (Decreto nº 11.856/2023).

No que tange à governança, defendeu-se que a atuação multissetorial seja articulada por um arranjo institucional centralizado em um Sistema Brasileiro de Cibersegurança, inspirado em modelos existentes, como o Sistema Militar de Defesa Cibernética e o Sistema Nacional de Defesa do Consumidor. Idealmente, tal sistema deveria contar com uma Rede Nacional de Cibersegurança, promovendo a participação ampla dos *stakeholders* e facilitando a coordenação e cooperação entre os atores da cibersegurança no país (Belli, 2025b; Jiang; Belli, 2024). Reconhecendo os desafios políticos, práticos e gerenciais, propôs-se uma abordagem "minimalista", na qual a definição dos detalhes operacionais seja fruto de debate público, coordenado pelo CNCiber, com participação social inclusiva e democrática.

O segundo pilar, segurança da informação, foi identificado como elo central da proteção de ativos digitais, sejam infraestruturas críticas, bens de consumo ou sistemas operacionais integrados a redes e fluxos de dados. Discutiram-se, nesse contexto, a regulação dos dados (pessoais e não pessoais), as boas práticas de governança da informação e a necessidade de

se combinar estas boas práticas com um apoio institucional que fomente a efetiva implementação de controles e obrigações claras, para garantir a segurança da informação.

O combate ao cibercrime, terceiro pilar, foi considerado dada a inserção do Brasil no epicentro de uma onda global de crimes cibernéticos. Embora não exista no país uma lei geral sobre crimes cibernéticos, a adesão à Convenção de Budapeste (2022) e sua internalização pelo Decreto nº 11.491/2023 representaram avanço significativo. Ressaltou-se, contudo, a necessidade de medidas complementares e de uma abordagem integrada, não restrita ao âmbito penal. A adoção de tais medidas pode ser instrumental para facilitar também a integração das futuras obrigações, decorrentes da assinatura da nova Convenção da ONU contra o Cibercrime.

O quarto pilar, literacia digital, foi apresentado como componente essencial para a efetivação da cibersegurança, uma vez que a construção de um ambiente digital saudável exige não apenas medidas técnicas, mas também a formação de uma consciência coletiva sobre segurança e a resiliência cibernética. A literacia digital, nesse contexto, compreende a educação, a capacitação e a formação contínua dos usuários de tecnologias digitais, devendo ser concebida como oportunidade estratégica para reduzir desigualdades sociais, ampliar o acesso seguro às tecnologias e construir a soberania digital do país. Entre as prioridades desse processo, destacam-se a atenção a grupos vulneráveis, como crianças, adolescentes e idosos, e a capacitação de professores para que possam atuar como multiplicadores de conhecimento e práticas seguras desde as fases iniciais da educação.

O quinto pilar, política industrial, está intrinsecamente relacionado à noção de soberania digital e à mitigação dos riscos decorrentes da dependência tecnológica e da desindustrialização. Argumentou-se que a capacidade de fomentar o desenvolvimento tecnológico interno é condição indispensável para alcançar o objetivo constitucional de autonomia tecnológica e, consequentemente, assegurar uma "boa soberania digital" (Belli, 2023a), aquela em que qualquer entidade, e não apenas o Estado, é capaz de compreender o funcionamento das tecnologias digitais, desenvolvê-las e utilizá-las em seu próprio benefício e para fortalecer a soberania nacional. Nesse sentido, destacou-se que a política industrial deve ser robusta e alinhada às estratégias nacionais de transformação digital e cibersegu-

rança, promovendo investimentos, inovação e o fortalecimento de cadeias produtivas estratégicas.

Por fim, o sexto pilar refere-se às tecnologias disruptivas, com especial ênfase na inteligência artificial (IA), cuja relação com a cibersegurança é determinada pelo modo como é utilizada, seja para finalidades defensivas, ofensivas ou adversariais. A integração de capacidades de IA pode ampliar significativamente a eficácia, o alcance, a escala e a precisão de operações cibernéticas maliciosas, representando uma mudança de paradigma tanto para estratégias ofensivas quanto defensivas. Apesar dos riscos, essa evolução também oferece oportunidades para o fortalecimento de mecanismos de defesa. Para que isso ocorra, porém, é imprescindível uma abordagem multissetorial capaz de congregar entidades governamentais, setor privado e instituições de pesquisa, a fim de desenvolver regulações adequadas, implementar medidas robustas de cibersegurança e incentivar inovações em tecnologias defensivas baseadas em IA, voltadas à proteção das infraestruturas críticas e dos cidadãos.

Considerando a necessidade de proteger a soberania nacional, os interesses do Estado e os direitos fundamentais dos cidadãos, este estudo conclui reiterando (Belli *et al*., 2023a) a sugestão de se adotar com urgência uma nova Lei Geral de Cibersegurança e de se criar uma Agência Nacional de Cibersegurança capaz de implementar efetivamente tal marco regulatório. Propostas detalhadas com tais objetivos já foram elaboradas pelos grupos de trabalho do CNCiber ao longo de 2024 e, na opinião dos autores, representam excelentes propostas que deveriam ser usadas para construir os novos pilares da cibersegurança no Brasil.

A adoção de uma Lei Geral de Cibersegurança e a criação de uma autoridade competente para fiscalizar tal representa, na visão dos autores, um passo decisivo para o estabelecimento de uma nova governança da cibersegurança no Brasil. A pretensão dos autores é que a enorme relevância e complexidade da cibersegurança tenham se tornado mais acessíveis por meio das análises apresentadas neste volume.

5 Glossário

5.1 Ameaça Persistente Avançada (Advanced Persistent Threat – APT)

Inicialmente introduzido pela Força Aérea dos Estados Unidos (USAF – *United States Air Forces*) em 2006, o conceito de Ameaça Persistente Avançada – ou APT, na sigla em inglês para *Advanced Persistent Threat* –, se refere a um adversário altamente especializado e com recursos substanciais capaz de empregar uma variedade de ferramentas de ataque, como ataques cibernéticos ou físicos, a fim de criar oportunidades para atingir seus objetivos. Esses objetivos geralmente estão relacionados ao estabelecimento e à expansão de sua presença nas infraestruturas de tecnologia da informação de organizações, visando vazamentos contínuos de informações, minando aspectos críticos de operações, missões, programas ou negócios, ou preparando-se para fazê-lo no futuro. Além disso, a APT é caracterizada por sua persistência ao buscar esses objetivos, prolongando-se no tempo e adaptando-se de forma contínua às tentativas dos defensores de resisti-la (Rocha, 2023).

A APT possui como diferencial os seus aspectos estratégicos e furtivos: os invasores iniciam o processo por meio de métodos convencionais, como *phishing* ou cavalos de Tróia, mas buscando ocultar suas pegadas ou rastros digitais, enquanto se movem silenciosamente pela rede ou ambiente de dados da vítima e implementam seu software de ataque de forma abrangente. Ao estabelecer um ponto de apoio, os invasores buscam alcançar seu objetivo principal, que geralmente envolve a extração contínua e persistente de dados ao longo de meses ou até anos. A execução de APTs segue uma abordagem sequencial e padronizada, envolvendo etapas como o desenvolvimento de uma estratégia específica para a nuvem, obtenção de acesso por meio de técnicas de engenharia social, estabelecimento de um ponto de apoio na rede, investigação para planejar o ataque, organização

dos dados desejados para exfiltração e, finalmente, assumir o controle dos dados, permitindo a movimentação furtiva pelo mundo sem ser detectado por longos períodos, até que eventualmente seja identificado ("What is an Advanced Persistent Threats (APT)", *[S.d.]*).

5.2 Análise de Risco e Risco Cibernético

Risco é um conceito atrelado à noção da ocorrência hipotética de determinado evento futuro, capaz de afetar, de alguma forma, o alvo em análise (por exemplo, uma organização, um sistema etc.). Em outras palavras, fala-se na possibilidade de ocorrência de um evento (incerto), no futuro (elemento temporal), com potencial de impactar um determinado cenário, positivamente ou negativamente, o que, no contexto da segurança da informação, é nocivo, haja vista o potencial lesivo. Para desvelar um risco, a partir de uma proposição abstrata, transcreve-se a seguinte fórmula (Fernandes, 2009, p. 13): "Risco de Segurança = Chance de ocorrência * Impacto negativo estimado * Incerteza relacionada com as medidas".

A importância de mapear e analisar os riscos perfaz-se em razão da possibilidade de refletir acerca das medidas necessárias para a respectiva mitigação (redução). Entretanto, é importante destacar que inexiste "risco zero". Nessa linha, entende-se que, pela gestão desses riscos por meio da implementação de controles de segurança, produz-se um novo tipo de risco, o "risco residual". Um último aspecto relevante é que este mapeamento e monitoramento devem ser realizados em fluxo contínuo, em razão da celeridade das novas tecnologias, golpes e, consequentemente, vulnerabilidades.

O risco cibernético abarca uma amplitude terminológica profundamente associada ao conceito de ameaças cibernéticas que envolvem diferentes níveis, fontes de risco e alvos em potencial. Adicionalmente, o risco cibernético especificamente abrange elementos inerentes ao ciberespaço. Incluindo, mas não limitado à desterritorialidade cibernética que apresenta desafios práticos aos conceitos de território e jurisdição, dentre outros, bem como incidentes cibernéticos, desde o vazamento de dados até crimes e sabotagem cibernética (Eling; Schnell, 2016). Não obstante sua amplitude, definições de ciberrisco que abarquem o conceito de forma holística

são relativamente escassas. Para reverter este quadro, Strupczewski (2021) define risco cibernético da seguinte forma:

> O risco cibernético é um risco operacional associado à realização de atividades no ciberespaço, ameaçando ativos de informação, recursos de TIC e ativos tecnológicos, o que pode causar danos materiais a ativos tangíveis e intangíveis de uma organização, interrupção dos negócios ou prejuízo à reputação. O termo "risco cibernético" também inclui ameaças físicas aos recursos de TIC dentro da organização (Strupczewski, 2021, p. 6, tradução nossa).

Em sua definição, Strupczewski abarca uma dimensão operacional de risco, que complementa a de Cebula e Young (2010) que definem o risco cibernético como "riscos operacionais para ativos de informação e tecnologia que têm consequências afetando a confidencialidade, disponibilidade ou integridade de informações ou sistemas de informação" (Cebula; Young, 2010, p. 1, tradução nossa). Neste sentido e considerando o imperativo da resiliência cibernética em negócios, empresas e governos na atualidade, o Bank for International Settlements propõe a seguinte definição de risco cibernético: "A combinação da probabilidade de um evento ocorrer no âmbito dos ativos de informação, recursos de computação e comunicação de uma organização e as consequências desse evento para a organização" (Bank for International Settlements, 2016, p. 24, tradução nossa).

Trata-se, portanto, de uma realidade inerente à interconectividade e globalização hodierna, a ser mitigada por conceitos como a segurança cibernética acompanhada de medidas de resiliência cibernética em diferentes empreendimentos.

5.3 Ativo/Ciberativo

Um Ativo é algo – um objeto, uma propriedade, um recurso – a que se pode atribuir valor (ISACA, *[S.d.]*). Outra forma de se definir um ativo é como tudo aquilo que tem utilidade para a realização de um fim (NICCS, 2023). De modo geral, um ativo tem valor atribuído pelos *stakeholders* relacionados a ele, sejam a organização que o detém, competidores ou atacantes. Um ativo pode ser tangível (tem forma física) ou intangível (não tem

forma física). Ativos intangíveis incluem propriedade intelectual, dados e informação, software e outros elementos que se encaixam na definição. Sendo assim, ativos cibernéticos ou ciberativos são aqueles cuja existência se concretiza no ambiente cibernético. De fato, a definição pode ser significativamente elástica, incluindo, a depender do contexto:

> Contratos, instalações, propriedade, registros, saldos não obrigatórios ou não gastos de dotações e outros fundos ou recursos, pessoal, inteligência, tecnologia ou infraestrutura física, ou qualquer coisa útil que contribua para o sucesso de algo, como uma missão organizacional; ativos são coisas de valor ou propriedades às quais o valor pode ser atribuído; Do ponto de vista da inteligência, inclui qualquer recurso – pessoa, grupo, relacionamento, instrumento, instalação ou suprimento – à disposição de uma organização de inteligência para uso em uma função operacional ou de suporte (Management Directorate, DHS, 2017, p. 42, tradução nossa).

Alguns ativos podem ser classificados como críticos por serem absolutamente indispensáveis para a realização de uma determinada finalidade. A depender do ponto de vista adotado, pessoas e o conhecimento nelas incorporado, capacidades e atividades poderão ser considerados ativos (CSRC, *[S.d.]*).

5.4 Atribuição

Atribuição, como o nome sugere, é a indicação de autoria de um ataque cibernético. Ou seja, trata-se da atribuição de um determinado incidente a um determinado grupo, que pode ser independente ou estatal. Fala-se, geralmente, em atribuição de ataques a infraestruturas críticas e a órgãos ou serviços governamentais, de modo que o termo é comumente utilizado no contexto das relações entre Estados. A atribuição é cercada de complexidades estratégicas e técnicas que fazem com que a indicação com total certeza da autoria de um ataque, especialmente um ataque incentivado, provocado ou realizado diretamente por outro Estado, seja infrequente.

Por um lado, a natureza descentralizada e transnacional da Internet, aliada a ferramentas de anonimização, dificulta o processo de identificação da origem de ataques. Por outro lado, mesmo quando se sabe com al-

gum grau de certeza qual é a origem, a decisão por divulgá-la não deve ser tomada de forma leviana, especialmente considerando-se as relações geopolíticas envolvidas. Ainda, o grau de dano causado pelo incidente é levado em consideração em decisões de atribuição e nos esforços necessários para tanto: vale a pena perseguir esclarecimentos a respeito da origem de um ataque que não tenha causado impactos significativos? Basta reforçar as defesas relevantes, ou conhecer a origem do ataque trará algum benefício ulterior? Estas são perguntas que organizações precisam enfrentar ao tratar da atribuição (Rid; Buchanan, 2015). No marco analítico construído por Rid e Buchanan, decisões a respeito da atribuição são atravessadas pelas seguintes dimensões:

> O objetivo tático é entender o incidente principalmente em seus aspectos técnicos, o como. O objetivo operacional é entender a arquitetura de alto nível do ataque e o perfil do atacante – o quê. O objetivo estratégico é entender quem é o responsável pelo ataque, avaliar a lógica do ataque, o significado, a resposta apropriada a quem e por quê. Finalmente, a comunicação também é um objetivo por si só: comunicar o resultado de uma investigação forense trabalhosa é parte integrante do processo de atribuição e não deve ser tratada como de baixa prioridade. De fato, a própria atribuição pública pode ter efeitos significativos: os agressores podem abortar uma operação, mudar de tática ou reagir publicamente às alegações, moldando assim a resposta mais ampla da vítima (Rid; Buchanan, 2015, p. 7–8).

A decisão por tornar pública a atribuição de um ataque cibernético deve, ainda, levar em consideração elementos estratégicos relacionados à capacidade de resposta, à proporcionalidade da mesma e à credibilidade. Edwards *et al.* comentam o caso do ataque à empresa Sony atribuído ao governo norte-coreano pelos Estados Unidos. No caso, a atribuição inicial à Coreia do Norte foi encarada com ceticismo até que evidências suficientes fossem apresentadas; além disso, o escopo de respostas possíveis era limitado, visto que um contra-ataque no mesmo campo poderia legitimar ações de interferência cibernética malvistas, enquanto uma resposta em outro campo poderia desencadear um processo de escalada de agressões (Edwards *et al.*, 2017).

Por fim, um ponto importante a se considerar é o cenário regulatório que cerca a atuação de determinada organização. Em se tratando de

empresas listadas em bolsa, bem como organizações que realizam processamento de dados pessoais, há, em diversas jurisdições, obrigações regulatórias de transparência. A ANPD brasileira, por exemplo, sugere um prazo de dois dias úteis para a divulgação à Autoridade e aos titulares afetados de incidentes de segurança que possam provocar danos significativos (ANPD, 2024a). De forma semelhante, a *Securities and Exchange Commission* estadunidense requer a comunicação de fato relevante relacionado a incidentes de cibersegurança em até quatro dias úteis, com informações a respeito da "ocorrência de um incidente material de segurança cibernética e […] os aspectos materiais da natureza, escopo e momento do incidente, bem como o impacto material ou impacto material razoavelmente provável do incidente sobre a empresa" (Gerding, 2023).

Assim, ainda que seja salutar que uma organização pública ou privada esteja preparada para reconhecer ataques – desde o modo como foram realizados até de onde se originam – e responder a eles, a decisão de atribuição pública de um ataque não é trivial e deve ser analisada caso a caso, com atenção aos aspectos estratégicos, operacionais e regulatórios.

5.5 Autenticação Multifator (*Multi-Factor Authentication* – MFA)

MFA, ou Autenticação Multifator (*Multi-Factor Authentication*, em inglês), é um mecanismo de segurança que exige que os usuários forneçam múltiplas formas de autenticação de sua identidade antes de obter acesso a um sistema ou conta. O objetivo do MFA é aumentar a segurança adicionando uma camada extra de proteção além de apenas um nome de usuário e senha. Geralmente, o MFA envolve uma combinação de algo que o usuário sabe (como uma senha) e algo que o usuário possui (como um dispositivo móvel ou um token de segurança). Por exemplo, podemos citar o login por meio de e-mail e senha com uma etapa adicional de validação de identidade por meio do envio de um código ao e-mail cadastrado, ou a um token registrado em algum aplicativo de autenticação, ou até mesmo uma etapa adicional de validação por biometria digital ou facial (Pretesh Biswas, 2023; Souppaya; Scarfone, 2016).

5.6 *Backdoors*

O termo *Backdoor* refere-se a uma vulnerabilidade ou funcionalidade oculta inserida intencionalmente em um sistema de software (e.g. aplicativo, programa, etc.) ou hardware (dispositivo, equipamento, etc.) para permitir acesso não autorizado ou controle sobre o sistema, muitas vezes sem o conhecimento dos usuários legítimos (Francillon *et al*., 2018).

As *backdoors* podem assumir várias formas, desde portas de comunicação não documentadas até códigos maliciosos inseridos em software durante o desenvolvimento. Independentemente da forma que assumem, as *backdoors* são projetadas para evadir detecção e fornecer acesso não autorizado ao sistema, contornando os mecanismos de segurança convencionais.

Portanto, presença de uma *backdoor* em um sistema representa uma séria ameaça à cibersegurança, pois pode ser explorada por atores maliciosos para uma série de atividades prejudiciais, tais como acesso não autorizado a sistemas e dados, comprometendo a confidencialidade e integridade das informações armazenadas; espionagem e vigilância, monitorando atividades dos usuários ou coletando informações corporativas; execução de ataques, como instalação de *malware*, ataques de negação de serviço (DDoS) ou roubo de informações; e manipulação de sistemas, podendo resultar em danos operacionais, financeiros ou reputacionais para organizações afetadas.

5.7 Centro de dados (Data center)

É uma infraestrutura física concentrada que abriga os sistemas computacionais de uma organização, incluindo redes, dispositivos de armazenamento, roteadores, *switches*, *firewalls*, sistemas de armazenamento, servidores e controladores de disponibilização de aplicativos e outros componentes tecnológicos essenciais para a execução de atividades. Essa infraestrutura é que possibilita a ocorrência da computação em nuvem, pois essa abriga os servidores que, em variados níveis de organização e técnicas de virtualização, oferecem os serviços em nuvem. Portanto, os data centers são a manifestação física da computação em nuvem (Verdi; Rothenberg; Pasquini, 2010).

Essas instalações são projetadas para fornecer uma infraestrutura confiável, segura e eficiente para operações de TI (tecnologia da informação), garantindo a continuidade dos serviços e a proteção dos dados. Essa

abordagem reduz significativamente a necessidade de equipamentos físicos, consumo de energia e espaço ocupado.

Um data center serve a várias finalidades distintas. Eles servem para armazenamento de dados, processamento de dados, hospedagem e aplicações, suporte à computação em nuvem, conectividade e distribuição de conteúdo, *backup* e recuperação de dados, segurança, além de apoiar a pesquisa e desenvolvimento de uma organização. Pode-se unificar essas funções em três grupos: *i)* funções relacionadas à infraestrutura de rede, pois conectam vários servidores (virtuais e físicos), serviços e conectividade externa aos usuários; *ii)* funções ligadas à infraestrutura de armazenamento, já que armazenam os dados, que são os principais elementos de um centro de dados moderno; e, *iii)* funções que oferecem recursos de computação, vez que são eles que fornecem o processamento, a memória, o armazenamento local e conectividade necessária para que os usuários acessem diversos aplicativos (Verdi; Rothenberg; Pasquini, 2010).

Para comportar o hardware e software de um grande data center é preciso de uma infraestrutura significativa, o que inclui sistemas de energia potentes e interruptos (UPSs – *Uninterruptible Power Supplies*), fontes de resfriamento e ventilação, sistema de segurança forte e supressão de incêndio, geradores de *backup* e conexão de redes externas com estruturas de balanceamento (isto é, balanceamento de carga entre servidores ou conexões de rede para distribuir o tráfego uniformemente e manter a disponibilidade do serviço).

Deve-se considerar, ainda, que toda essa infraestrutura deve ser redundante, ou seja, existem componentes ou sistemas extras que são mantidos em reserva para garantir a continuidade das operações em caso de falha de um componente ativo. Essa redundância é projetada para aumentar a confiabilidade e disponibilidade de um sistema, minimizando os pontos únicos de falha e assegurando que os serviços permaneçam operacionais mesmo diante de um problema técnico.

5.8 Ciberameaça

O termo "Ameaça Cibernética" é usado de forma holística para se referir à miríade de atores e potenciais riscos e vulnerabilidades no cibe-

respaço. Nesse sentido, pode ser genericamente compreendido como "uma pessoa ou organização que intenciona causar mal" (FRYE, Jason *et al*, 2012, p. 10, tradução nossa). No ciberespaço ou através dele. Tal amplitude conceitual acarreta uma taxonomia própria de ameaças. Especificamente quanto à fonte destas ameaças, o National Institute of Standards and Technology (NIST) promulga a seguinte definição de ameaça cibernética:

> Uma ameaça é qualquer circunstância ou evento com potencial de impactar adversamente as operações e ativos organizacionais, indivíduos, outras organizações ou a Nação por meio de um sistema de informação via acesso não autorizado, destruição, divulgação ou modificação de informações e/ou negação de serviço. Os eventos de ameaça são causados por fontes de ameaça. Uma fonte de ameaça é caracterizada como: (i) a intenção e o método direcionados à exploração de uma vulnerabilidade; ou (ii) uma situação e um método que podem explorar acidentalmente uma vulnerabilidade. Em geral, os tipos de fontes de ameaça incluem: (i) ataques cibernéticos ou físicos hostis; (ii) erros humanos de omissão ou comissão; (iii) falhas estruturais de recursos controlados pela organização (por exemplo, hardware, software, controles ambientais); e (iv) desastres, acidentes e falhas naturais e provocados pelo homem, além do controle da organização. Várias taxonomias de fontes de ameaça foram desenvolvidas. Algumas taxonomias de fontes de ameaça usam o tipo de impactos adversos como princípio organizador. Múltiplas fontes de ameaça podem iniciar ou causar o mesmo evento de ameaça - por exemplo, um servidor de provisionamento pode ser tirado do ar por um ataque de negação de serviço, um ato deliberado de um administrador de sistema malicioso, um erro administrativo, uma falha de hardware ou uma falha de energia (National Institute of Standards and Technology; Joint Task Force Interagency Working Group, 2020, p. 8, tradução nossa).

Trata-se, portanto, de um termo de grande amplitude que abarca também uma taxonomia de ameaças de mais variada origem, intenção, tipo e dimensão. Tamanha amplitude suscita profunda incerteza e pode afetar a percepção de ameaças por diferentes atores cibernéticos (Walt, 2018; Solar, 2020). Adicionalmente, a rápida adoção e ímpeto por soluções de TI, sem as devidas medidas de proteção, aumentam a superfície de ataque para es-

tas ameaças cibernéticas, caracterizadas pelo seu dinamismo e persistência, com progressivos custos a Estados, nações e indivíduos (Atwell, 2021).

5.9 Ciberdefesa

Ciberdefesa é o conjunto de estratégias, políticas e práticas implementadas por organizações, indivíduos e governos para proteger sistemas de informação, redes e infraestruturas críticas contra ameaças cibernéticas (NordVPN, [S.d.]). A ciberdefesa é crucial para preservar a integridade, confidencialidade e disponibilidade dos ativos digitais de uma organização, sendo vital tanto para o setor privado quanto para o setor público. Uma estratégia de ciberdefesa, especialmente sob uma perspectiva de ciberdefesa "ativa", objetiva a detecção, interrupção e mitigação dos efeitos de incidentes (CIO-DoD, 2013; DoD, 2011).

No Brasil, a crescente digitalização de processos empresariais e governamentais, acelerada em virtude do período pandêmico e consequente isolamento social, aumentou a relevância da ciberdefesa. No contexto do Estado brasileiro, o conceito de defesa cibernética assume definição especificamente relacionada à defesa nacional, conforme a Doutrina Militar de Defesa Cibernética:

> Defesa Cibernética - ações realizadas no espaço cibernético, no contexto de um planejamento nacional de nível estratégico, coordenado e integrado pelo Ministério da Defesa, com as finalidades de proteger os ativos de informação de interesse da defesa nacional, obter dados para a produção de conhecimento de inteligência e buscar superioridade sobre os sistemas de informação do oponente (EMCFA, 2023, p. 17).

Os desafios enfrentados na ciberdefesa incluem a sofisticação crescente de ataques cibernéticos e a necessidade de atualização contínua de medidas de segurança. Tendências como inteligência artificial, análise de dados em tempo real e colaboração entre setores público e privado têm se destacado como estratégias promissoras. O Brasil testemunhou uma série de incidentes significativos recentemente, mirando desde empresas até órgãos de todas as esferas do poder público (Security Report, 2021, 2022,

2023). A variedade e o impacto destes incidentes ressaltam a importância de se manter o foco em estratégias robustas de ciberdefesa.

5.10 Ciberespaço

O Ciberespaço é compreendido como um domínio inédito e artificial, com características que o diferenciam dos demais domínios naturais, como terra, mar, ar ou mesmo espaço. Em função de seu ineditismo e amplitude, o ciberespaço possui uma miríade de definições, inferidas a partir do uso que atores fazem deste novo domínio.

Apesar de abarcar diversas definições, o ciberespaço pode ser compreendido genericamente como "um conjunto de sistemas de informação interconectados dependentes do tempo e dos usuários humanos que interagem com esses sistemas" (Ottis; Lorents, 2010, s.p., tradução nossa). Contudo, a "característica definidora desses sistemas está na sua interconectividade em um espaço que é em si uma rede de usuários que habitam e experienciam essa rede" (Cohen, 2007, p. 255, tradução nossa). Ainda, a rede que o ciberespaço representa possui uma dimensionalidade física além dos usuários que o utilizam. Como proposto por Rattray, "o ciberespaço é, na verdade, um ambiente físico; ele é criado pela conexão de sistemas físicos e redes, gerenciados por regras estabelecidas em software e protocolos de comunicação" (Rattray, 2009, p. 254, tradução nossa).

Para melhor definir o ciberespaço, é fortuito analisar sua composição. Nesse sentido, Kuehl (2009) e Libicki (2009a) entendem o ciberespaço como um domínio composto por camadas. A primeira camada são os componentes e dispositivos físicos que ancoram o ciberespaço; a segunda, a camada informacional, é representada pelos programas, dados e informações intangíveis que estão presentes em computadores individuais e circulando pelas redes do ciberespaço. Por último, a camada de usuários representa os operadores que controlam e interagem com o ciberespaço. A compreensão do ciberespaço como um domínio em camadas, por sua vez, possibilita a definição proposta por Medeiros e Goldoni, como

> [u]m domínio único de interação humana artificial, parcialmente desassociado de elementos físicos, que permeia os domínios tradicionais. Ele existe por meio da conexão de diferentes camadas:

> tecnológica, técnica e pessoal. Possui peculiaridades distintas, viabilizadas por sua imaterialidade parcial e interconectividade expansiva. O ciberespaço está em constante evolução à medida que a tecnologia avança e muda continuamente conforme diferentes atores o utilizam, moldando-o para atender às mais diversas necessidades (Medeiros; Goldoni, 2020, p. 37, tradução nossa).

Tem-se, portanto, uma definição do ciberespaço holística, que o compreende como um domínio artificial, composto por diferentes camadas, interconectadas tecnicamente e interrelacionadas por diferentes usuários. O inter-relacionamento e operacionalização destas camadas, por sua vez, suscitam peculiaridades únicas ao ciberespaço, sendo elas a desterritorialidade, a difusão de poder e a incerteza cibernética (Medeiros; Goldoni, 2020). Estas peculiaridades, por sua vez, são exploradas por diversos atores que perseguem seus interesses no e através do ciberespaço, no que é chamado de poder cibernético (Nye, 2010).

5.11 Ciber-Guerra

O conceito da Guerra Cibernética pode ser entendido holisticamente como "Ações realizadas por um Estado-nação para penetrar os computadores ou redes de outra nação com o objetivo de causar danos ou interrupções" (Richard A. Clarke; Clarke; Knake, 2010, p. 11, tradução nossa). Perpetrada para fins estratégicos, a guerra cibernética resulta de "[u]ma campanha de ciberataques lançada por uma entidade contra um estado e sua sociedade, principalmente, mas não exclusivamente, com o objetivo de influenciar o comportamento do estado-alvo […]" (Libicki, 2009b, p. 117, tradução nossa). Contudo, o conceito de guerra cibernética não possui uma definição de comum acordo e abarca uma ampla discussão acadêmica, normativa e política (Ashraf, 2021).

No âmbito acadêmico, Thomas Rid recorre ao estudo de Carl Von Clausewitz – um dos principais teóricos das Ciências Militares – para determinar que a guerra em si é caracterizada pela violência, aplicada de forma instrumental para fins políticos. Nesse sentido, Rid argui que a guerra cibernética, vislumbrada por ataques entre redes, realizados através de *softwares,* não caracteriza o uso da violência. Este ponto, somado à busca

de atores cibernéticos pelo anonimato e exploração da dificuldade de atribuição no ciberespaço, também esvazia a concepção da instrumentalidade política da guerra cibernética. Neste sentido, segundo Rid, a guerra cibernética na prática diz respeito a uma nova terminologia para se referir a práticas antigas de subversão, sabotagem e espionagem, sendo realizadas no ciberespaço (Rid, 2012).

John Stone, por sua vez, contraria a argumentação de Rid, ao enxergar "violência" como um elemento associado, mas não exclusivo de "força" e "letalidade". Nesse sentido, Stone defende que atos de guerra envolvem a aplicação de força para gerar efeitos violentos, os quais não necessariamente precisam ser letais, podendo causar danos materiais. Além disso, a mediação da tecnologia permite que pequenas ações, como operar um teclado, resultem em impactos significativos de violência, independentemente de serem letais ou não (Stone, 2013).

Na esfera normativa, e em função da não letalidade, a guerra cibernética ganha uma nova dimensão. Ao passo que a incerteza cibernética contribui para uma nebulosidade acerca dos limiares entre paz e guerra, mesmo em vista de incidentes e ataques cibernéticos perpetrados por atores estatais e não estatais, não há um consenso acerca do que acarretaria a guerra cibernética (Hathaway *et al*., 2012; Libicki, 2012a). Sob uma lente normativa, a discussão sobre a definição de guerra cibernética foca na prática dos Estados no ciberespaço e sua adequação ao direito internacional. Sob esta lente, ataques no ciberespaço podem configurar o uso da força, permitindo que um Estado aja em legítima defesa, em conformidade com o conceito jurídico de *jus ad bellum*, que trata da justificativa para a autodefesa de um Estado. Uma vez iniciada a guerra cibernética, os ciberataques seriam regulados pelo *jus in bello*, as regras que governam a conduta da guerra (Ashraf, 2021).

Contudo, a falta de clareza conceitual e normativa do conceito de guerra cibernética contribuem para o que alguns atores chamam de *gray zone* ou "zona cinzenta". Nesta, atores estatais e não estatais deliberadamente calibram e conduzem suas ações no ciberespaço, evitando consequências ou mesmo a escalada que suas ações provocariam nos demais domínios (Wirtz, 2017).

5.12 Cibersegurança

Cibersegurança é o conjunto de normas, práticas e processos que permitem proteger indivíduos conectados, sistemas críticos, informações particularmente importantes de potenciais riscos e ameaças cibernéticas. A única definição consensual existente foi elaborada pelo Setor de Normatização das Telecomunicações da União Internacional de Telecomunicações da ONU, conhecido pelo acrônimo inglês ITU-T, segundo a qual:

> Cibersegurança é o conjunto de ferramentas, políticas, conceitos de segurança, diretrizes, abordagens de gestão de risco, ações, treinamentos, melhores práticas, garantias e tecnologias que podem ser utilizadas para proteger os ativos do ambiente cibernético, da organização e dos usuários. […] A cibersegurança busca garantir o cumprimento e a manutenção das propriedades de segurança dos ativos da organização e dos usuários contra riscos relevantes à segurança encontrados no ambiente cibernético (ITU-T - International Telecommunication Union, 2008).

Como sugere a leitura desta definição particularmente extensiva, a cibersegurança é um assunto necessariamente multidimensional, multissetorial e, frequentemente, transnacional (Belli *et al.*, 2023b). Tal natureza é evidente, considerando que a elaboração e implementação das ferramentas, conceitos, diretrizes etc. mencionados anteriormente dependem de atores de natureza extremamente diferente – pública, privada, associativa etc. – que não são necessariamente localizados na mesma jurisdição.

Vários autores exploraram como diferentes abordagens à cibersegurança são construídas, destacando a existência de perspectivas complementares, mas frequentemente divergentes, e enfatizando que as definições de cibersegurança muitas vezes se cristalizam em torno de questões, ameaças, atividades e aspectos específicos. Apesar de não existir uma taxonomia oficial das dimensões nas quais se estrutura a cibersegurança, vários autores convergem na identificação de pelo menos quatro camadas, incluindo a segurança de dados pessoais, de informações e sistemas financeiros, de infraestruturas críticas e de infraestruturas democráticas.

5.13 Computação em Nuvem (Cloud Computing)

A Computação Em Nuvem, conhecida também como *cloud computing*, representa um paradigma de provisão e consumo de recursos computacionais baseado na entrega sob demanda de recursos em redes públicas ou privadas com alcance global, infraestrutura em grande escala, preços reduzidos e a experiência de capacidade aparentemente infinita. O conceito de *cloud computing* surgiu no ano de 1950 com a implementação de computadores *mainframe*, acessíveis remotamente, com a popularização do conceito de compartilhamento de recursos através de redes. Desde então, a computação em nuvem evoluiu e, a partir dos anos 2010, o termo ganhou notoriedade, impulsionado pelo avanço tecnológico e pela necessidade crescente de escalabilidade e flexibilidade nos ambientes computacionais (De Filippi; Belli, 2012; Antonopoulos; Gillam, 2017).

A infraestrutura de computação em nuvem é composta por diversos elementos interligados que possibilitam o fornecimento eficiente de serviços. Estes elementos incluem servidores, *data centers*, redes, software e serviços, todos acessíveis remotamente por meio da Internet. Os *data centers* desempenham um papel particularmente relevante, sendo o conjunto de servidores onde está alojado o serviço (aplicativo) que você acessa. Praticamente, o *data center* pode ser tanto uma grande sala no seu prédio corporativo quanto um galpão cheio de servidores do outro lado do mundo que você acessa pela Internet. Uma tendência crescente é a virtualização de servidores, ou seja, um software pode ser instalado permitindo a utilização de múltiplas instâncias de servidores virtuais. Desta forma, você pode ter múltiplos servidores virtuais rodando em um servidor físico. Cabe ressaltar que, no âmbito da computação em nuvem, os servidores são tipicamente distribuídos, ou seja, não precisam estar todos hospedados no mesmo local. Frequentemente, os servidores estão em locais geograficamente díspares, mas para o usuário os servidores agem como se estivessem funcionando um ao lado do outro. Isso dá ao provedor de serviços mais flexibilidade em opções e segurança, considerando que, se algum acidente ou falha de funcionamento acontecer em um servidor, o serviço ainda seria acessível através de outro servidor (Buyya; Broberg; Goscinski, 2011).

Assim, a virtualização desempenha um papel crucial para permitir a computação em nuvem, baseada na criação de recursos virtuais que po-

dem ser alocados dinamicamente conforme a demanda, otimizando a utilização dos recursos disponíveis. A computação em nuvem apresenta três modelos principais: Infraestrutura como Serviço (IaaS), Plataforma como Serviço (PaaS) e Software como Serviço (SaaS). O IaaS fornece recursos básicos, como armazenamento. O PaaS oferece uma plataforma completa para o desenvolvimento e execução de aplicações, enquanto o SaaS disponibiliza aplicativos prontos para uso (Antonopoulos; Gillam, 2017).

Apesar dos benefícios, a computação em nuvem apresenta desafios significativos em termos de cibersegurança. Questões como a falta de controle direto sobre a infraestrutura física, compartilhamento de recursos e dependência de fornecedores terceirizados aumentam a exposição a ameaças. Vulnerabilidades, como a falta de criptografia adequada, falhas na autenticação e autorização, bem como o vazamento de dados, representam riscos significativos para organizações que adotam essa tecnologia. Exemplos de incidentes cibernéticos particularmente frequentes no âmbito da computação em nuvem incluem (Belli *et al*., 2023b).

1. **Ataques de Negação de Serviço (DoS/DDoS):** Sobrecarregar servidores em nuvem com tráfego malicioso, tornando os serviços inacessíveis.
2. **Injeção de Código:** Explorar vulnerabilidades em aplicações na nuvem para injetar código malicioso e comprometer dados.
3. **Vazamento de Dados:** Acesso não autorizado a dados sensíveis armazenados na nuvem, seja por meio de falhas de configuração ou ataques direcionados.
4. **Ataques de Homem no Meio (MitM):** Interceptação de comunicações entre usuários e servidores na nuvem para obter informações confidenciais.
5. **Sequestro de Conta:** Comprometimento de credenciais para obter acesso indevido a serviços em nuvem, podendo resultar em perda de controle sobre recursos.

Para mitigar os riscos associados à computação em nuvem, diversas boas práticas têm sido estabelecidas. A implementação rigorosa de protocolos de segurança, o uso de criptografia robusta para proteger dados

em trânsito e em repouso, a autenticação multifatorial e a monitorização constante são essenciais. Além disso, a seleção criteriosa de provedores de serviços em nuvem, a implementação de políticas de governança eficazes e a educação contínua dos usuários são componentes cruciais de uma abordagem abrangente de segurança na nuvem.

5.14 Cópia de Segurança (*Backup*)

Backup é um termo inglês que se refere à geração de cópias de segurança de dados provenientes de dispositivos ou sistemas. Esse procedimento é relevante na medida em que permite a troca ou migração desses aparelhos ou *softwares* de forma facilitada e automatizada e, primordialmente, para garantir que face eventual incidente de segurança da informação que afete a integridade e/ou a disponibilidade da informação, os seus proprietários ou possuidores tenham os riscos de perdas totais ou parciais, temporárias ou permanentes, minorados. Essas cópias poderão ser armazenadas em mídia física – por exemplo, discos rígidos (HDs) externos e pendrives – ou digital, pelo armazenamento em nuvem.

Existem três principais tipos de *backup* (Maymí; Harris, *[S.d.]*):

1. *Full Backups*, dos quais há o armazenamento de uma cópia completa dos dados contidos em determinado dispositivo ou sistema protegido. São ideais para aquelas atividades que demandam rápida recuperação de arquivos, entretanto, são custosos e de implementação morosa;
2. *Backups* Incrementais, em que são armazenados somente os arquivos que foram modificados desde o último *backup* completo ou incremental mais recente. Esse modelo precisa ser acionado em períodos regulares e são utilizados com frequência em empresas que detém grande volume de dados; e,
3. *Backups* Diferenciais, que, assim como os incrementais, armazenam os dados modificados pela última vez desde o *backup* completo mais recente, entretanto, com o diferencial mais recente. São aqueles que permitem a restauração de arquivos mais rapidamente, ainda que de implementação mais lenta que o incremental.

Conforme anunciado, todos apresentam aspectos positivos e negativos. São as necessidades do negócio que determinarão qual o melhor modelo a ser utilizado (inclusive, eventualmente de forma híbrida). O que não se deve olvidar é documentar o tipo eleito e a periodicidade aplicada, seja na própria política de *backup*, seja no Plano de Recuperação de Desastres.

5.15 Criptografia

A criptografia é um elemento basilar da segurança cibernética e tem como propósito garantir a autenticidade, segurança e confiabilidade das informações sendo armazenadas e/ou compartilhadas. Tecnicamente, a criptografia emprega métodos matemáticos e algorítmicos para converter dados e impedir sua leitura ou manipulação por partes não autorizadas. Ao cifrar mensagens com algoritmos e chaves conhecidas apenas pelo remetente e pelo destinatário, a criptografia assegura que apenas as partes autorizadas possam acessar o conteúdo.

O Padrão de Criptografia de Dados (DES) foi estabelecido originalmente pelo *National Institute of Standards and Technology* (NIST) em 1977 (National Institute of Standards and Technology (NIST), 2016). Desde então, com o avançar das tecnologias computacionais, as metodologias e técnicas matemáticas ficaram progressivamente mais complexas, tornando a tecnologia de criptografia mais eficiente. Técnicas modernas de criptografia incluem algoritmos e cifras que possibilitam a criptografia e a decriptografia de informações, como chaves de criptografia de 128 bits e 256 bits, de forma que cifras modernas, como o Padrão de Criptografia Avançada (AES), são consideradas virtualmente inquebráveis (Fortinet, 2024).

De forma aplicada, o uso da criptografia no cotidiano suscita novas oportunidades e mercados, possibilitando transações online e assinaturas digitais que de outra forma não seriam viáveis (ENISA, 2024a). Indivíduos e organizações recorrem à criptografia para preservar a privacidade e a confidencialidade de suas comunicações e dados. Um exemplo são aplicativos de mensagens instantâneas, que empregam criptografia para proteger as conversas contra hackers e interceptações. Além disso, a criptografia é fundamental para a segurança da navegação online, como em redes virtuais privadas (VPNs), que estabelecem túneis criptografados e utilizam chaves públicas e privadas para garantir a integridade das informações

transmitidas. Ademais, a criptografia também surge como um contraponto às práticas de vigilância e monitoramento em massa (McGowan, 2022).

5.16 Dado anonimizado

A Lei Geral de Proteção de Dados Pessoais (LGPD), no artigo 5º, inciso I, estabelece que dados pessoais são definidos como quaisquer informações que possam ser usadas para identificar uma pessoa física, seja diretamente (identificada) ou indiretamente (identificável). Portanto, se um dado ou um conjunto de dados permite reconhecer a identidade de uma pessoa física, esse dado é considerado pessoal.

Isso significa que a anonimização consiste "na remoção ou na ofuscação de toda a informação pessoal de uma base de dados, com o objetivo de impedir a identificação dos indivíduos". Aplicam-se técnicas que pretendem dificultar, no sentido de tornar impossível ou quase impossível, a reidentificação, inclusive pelo próprio técnico que realizou a operação inicial.

A lei, seguindo padrões internacionais, incentiva a anonimização dos dados, que consiste em processá-los de forma que não se identifique a quem pertencem. Isso é uma estratégia fundamental para a proteção da privacidade e segurança dos dados.

Existem vários métodos reconhecidos internacionalmente para anonimizar dados, incluindo: *i)* remoção de informações imediatamente identificáveis, como CPF, nome e endereço; *ii)* generalização, que torna os dados menos específicos, como indicar uma faixa etária ao invés da idade exata; e *iii)* randomização, que desorganiza os dados de maneira que sua correlação se torne imprecisa, seja por meio da adição de dados inexatos ou pela alteração da ordem dos dados em uma tabela (Ribeiro, 2017).

A anonimização não é um processo simples nem totalmente à prova de riscos de reidentificação dos indivíduos. Há riscos de identificação isolada de alguns ou todos os dados que identificam uma pessoa e de capacidade de vinculação de registros sobre a mesma pessoa em diferentes bases de dados, bem como existe a possibilidade de inferência de atributos a partir de outros dados (Ehrhardt Jr.; Modesto, 2022).

A LGPD, em seu artigo 12, estabelece que dados anonimizados não são considerados dados pessoais, a menos que o processo de anonimização seja reversível com meios próprios ou com esforços razoáveis. Assim, um dado

ainda pode ser considerado pessoal se, ao ser combinado com outros dados, permitir a identificação de seu titular com um esforço considerado razoável.

A definição do que constitui um "esforço razoável" depende do contexto específico do dado, seu potencial interesse para terceiros, a relevância do dado, os benefícios de sua utilização e o nível tecnológico disponível para seu tratamento. Este critério busca equilibrar a expansão na definição de dados pessoais com a exclusão de dados anonimizados da aplicação da lei, conforme o artigo 12 da LGPD. Neste ponto, a Agência Nacional de Proteção de Dados poderá contribuir determinando o que será entendido como "esforço razoável", vez que essa possui competência para estabelecer regulamentos e procedimentos para a proteção de dados pessoais e privacidade, além de orientar sobre as melhores práticas para cada setor, conforme o artigo 52 da LGPD.

5.17 Dado pessoal/sensível

O artigo 5, inciso I, da Lei Geral de Proteção de Dados (LGPD) define o Dado pessoal como "informação relacionada a pessoa natural identificada ou identificável". Isso inclui uma ampla gama de informações, desde elementos de identificação direta, como nome, endereço ou CPF, até elementos indiretos, como características físicas, preferências pessoais e dados de localização. A definição abrangente de dado pessoal é fundamental para garantir a proteção dos direitos do titular de dados, particularmente no contexto da era digital.

A identificação de uma pessoa física pode ser direta, quando os dados permitem identificar uma pessoa sem a necessidade de informações adicionais, ou indireta, quando os dados podem ser combinados com outras informações para identificar uma pessoa específica. O tratamento de dados pessoais é regulamentado por leis em mais de 160 países no mundo. Essas leis, como a Lei Geral de Proteção de Dados (LGPD) no Brasil e o Regulamento Geral de Proteção de Dados (GDPR) na União Europeia, estabelecem princípios, direitos e obrigações para o tratamento adequado de dados pessoais, incluindo a obtenção de consentimento, a transparência nas práticas de coleta e o fornecimento de mecanismos para que os indivíduos exerçam

seus direitos, e a fiscalização de tais elementos por autoridades reguladores, como a Autoridade Nacional de Proteção de Dados no Brasil.

Dados pessoais podem ser dados sensíveis. O artigo 5, inciso II, da LGPD define dado pessoal sensível como "dado pessoal sobre origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou à organização de caráter religioso, filosófico ou político, dado referente à saúde ou à vida sexual, dado genético ou biométrico, quando vinculado a uma pessoa natural". Essa categoria específica de dados pessoais merece proteção especial devido ao seu potencial de causar danos significativos, discriminação ou violações dos direitos fundamentais das pessoas.

A sensibilidade desses dados decorre de sua capacidade de revelar aspectos íntimos e privados da vida das pessoas, tornando-os especialmente vulneráveis a abusos, discriminação ou uso indevido. Como resultado, a coleta, processamento e armazenamento de dados sensíveis são geralmente sujeitos a restrições mais rigorosas e exigem consentimento explícito dos titulares dos dados, além de medidas adicionais de segurança e proteção.

A proteção de dados sensíveis é uma preocupação central em legislações de proteção de dados em todo o mundo, que tipicamente incluem obrigações de estabelecer proteções aprimoradas dessas informações, como a necessidade de consentimento específico para coletar tais dados.

5.18 Desterritorialidade

Naturalmente, o conceito de Desterritorialidade está profundamente associado ao conceito de "territorialidade". Este diz respeito à "tentativa de um indivíduo ou um grupo de atingir, influenciar ou controlar pessoas, fenômenos e relacionamentos, através de delimitação e afirmação do controle sobre uma área geográfica" (Haesbaert, 2002, p. 119). Isto é, trata-se de um processo de territorialização quando diferentes grupos manifestam o poder em uma área precisa, delimitando-a e tendo os limites reconhecidos pelos demais (Raffestin, 1993). O instrumento para essa territorialização se dá mediante a construção de fronteiras, reconhecidas como limiares entre os espaços destes diferentes grupos.

Embora este processo de territorialização seja expressivo e reconhecido nos demais domínios naturais, na forma de espaços aéreos, zonas ma-

rítimas ou territórios físicos, o ciberespaço é marcado pela peculiaridade da desterritorialidade. Isso ocorre porque noções zonais de território tradicionalmente aplicadas aos domínios terrestre, marítimo e aéreo não se aplicam ao ciberespaço. A compreensão do ciberespaço como um domínio em camadas é o que suscita o conceito de desterritorialidade. Isto é, o ciberespaço é composto por uma camada física de dispositivos tecnológicos que abarcam desde computadores e smartphones até satélites e cabos submarinos. Há também uma camada informacional que, destilada em sua essência, corresponde ao código binário que compõe os dados, informações, softwares e todo tipo de informação transmitida entre dispositivos. Por último, há a camada dos usuários que operam o ciberespaço, interagindo fisicamente com os dispositivos e virtualmente com a camada informacional. Essa composição em camadas caracteriza o ciberespaço como um domínio parcialmente imaterial.

Essa imaterialidade se manifesta especificamente na camada informacional, onde os dados e informações, a priori contidos nos dispositivos físicos, são enviados de um dispositivo para outro, se dá a desterritorialidade do ciberespaço, que ocorre em oposição a um fluxo informacional de dados sendo transmitidos pelo espectro eletromagnético. Dessa forma, enquanto dispositivos físicos e seus usuários estão inseridos em territórios, os fluxos informacionais que interconectam estes dispositivos transpõem os limites fronteiriços construídos pelo processo de territorialização, configurando assim, a desterritorialidade do ciberespaço, que ocorre em oposição a territorialidade tradicional dos outros domínios naturais.

Como mencionado anteriormente, a gestão dos fluxos nas fronteiras, aliada à sua delimitação, constitui os principais elementos que definem o processo de territorialização (Haesbaert, 2007). Contudo, na era da globalização, quando os fluxos de informação no ciberespaço conseguem transcender o controle nas fronteiras, adquirem uma natureza desterritorializadora. Assim, a estrutura interconectada do ciberespaço leva a um esvaziamento, ainda que parcial, da física tradicional do território, pois se trata de um espaço de poder desprovido de fronteiras físicas que não segue os princípios fundamentais da territorialidade. O esvaziamento conceitual do território como uma zona de poder é a expressão do caráter desterritorializante do espaço cibernético. Ainda, ao passo que a globalização está fundamentada nas redes de Tecnologias de Informação e Telecomunica-

ções, a desterritorialidade do ciberespaço atinge uma escala global (Medeiros; Goldoni, 2020).

5.19 Difusão de Poder

O conceito de Difusão de Poder, em conjunto com as peculiaridades de "desterritorialidade" e "incerteza cibernética", define o ciberespaço (Medeiros; Goldoni, 2020). A difusão de poder em si também é dependente do ciberespaço. O termo foi cunhado por Joseph Nye que o define: "A difusão de poder no domínio cibernético é representada pelo vasto número de atores envolvidos e pela relativa redução dos diferenciais de poder entre eles. Qualquer um, desde um hacker adolescente até um importante governo moderno, pode causar danos no espaço cibernético (Nye, 2012, p. 173).

A definição de Nye, contudo, deve ser contextualizada com outro conceito do autor: o poder cibernético. Este é brevemente definido como a perseguição de interesses no e/ou através do ciberespaço (Nye, 2010). O poder cibernético, portanto, diz respeito a uma instrumentalização do ciberespaço como um domínio em si ou como uma alternativa para afetar os demais domínios. Nesse novo ambiente, diferentes atores irão perseguir seus interesses e dentre estes atores, o ciberespaço comporta desde indivíduos até grupos, sociedades e governos.

A difusão de poder ocorre quando elementos de poder, provenientes de recursos militares, econômicos, técnicos ou científicos, tradicionalmente concentrados na figura do Estado, são redistribuídos para os demais atores. Embora os governos ainda detenham a maior parte dos recursos financeiros, tecnológicos e os elementos físicos fundamentais do ciberespaço, a diminuição das disparidades de capacidade entre o Estado e outros atores nesse ambiente permite que toda sorte de atores – sejam eles Estados mais fracos, ou grupos de dissidentes, separatistas, terroristas, ativistas e militares – possam operar no espaço cibernético, afetando os demais atores. Isso se torna uma forma viável de compensar eventuais deficiências em armamentos, recursos financeiros e/ou capacidades de poder convencionais (Medeiros; Goldoni, 2020).

Ainda, é pertinente notar que Estados que detêm maior capacidade militar e econômica – tradicionais elementos de poder – comumente são

as nações mais avançadas tecnologicamente e têm sua infraestrutura crítica, econômica e militar profundamente dependente de Tecnologias de Informação e interconectadas pelo ciberespaço, configurando uma chamada "dependência cibernética" ilustrada pela vasta superfície de ataques destas nações. Essa dependência, por sua vez, se manifesta como um atrativo para demais atores que, em função da difusão de poder proporcionada pelo ciberespaço, podem explorar a dependência cibernética de atores mais poderosos. A história recente está povoada com exemplos de ocorrências cibernéticas onde grupos de cibercriminosos conseguiram causar bilhões de dólares em danos, explorando a dependência internacional de determinados softwares (Solar, 2020); ou de Estados militares e/ou economicamente mais fracos que recorrem ao ciberespaço como uma forma de compensar disparidades capacitativas (Kim, 2022; Swallow, 2023).

5.20 Diplomacia Cibernética

Como conceito, a Diplomacia Cibernética diz respeito à atualização do instrumento diplomático estatal para a realidade hodierna, perpassada pelas redes informacionais e inserida no ciberespaço. Neste sentido, holisticamente a diplomacia cibernética pode ser entendida como uma mera transposição de esforços diplomáticos para temáticas referentes ao ciberespaço. Como Barrinha e Renard postulam, "ciberdiplomacia pode ser definida como a diplomacia no domínio cibernético, ou seja, o uso de recursos diplomáticos e o desempenho de funções diplomáticas para garantir interesses nacionais no que diz respeito ao ciberespaço" (Barrinha; Renard, 2017, p. 355, tradução nossa).

Contudo, dada a realidade globalizada e a ubiquidade do ciberespaço para as sociedades e economias globalizadas, a diplomacia cibernética não está limitada às vias tradicionais da diplomacia. Como Barrinha e Renard argumentam, a diplomacia cibernética vai além do diálogo diplomático entre atores estatais e abarca também empresas, grupos e indivíduos. Ainda segundo os autores, essa expansão para envolver outros atores não estatais faz parte de um esforço mais amplo de iniciativas do poder estatal em mobilizar os demais setores sociais em conformidade com interesses nacionais mais amplos, do qual o ciberespaço é parte componente.

Nesse sentido, o Reino Unido foi um dos primeiros Estados a abordar iniciativas de diplomacia cibernética em sua documentação estratégica. Estes esforços podem tomar forma no fomento ao que o Reino Unido chama de "diplomacia regulatória" em fóruns internacionais acerca da governança cibernética, ou como parte de esforços em política externa direcionados ao desenvolvimento tecnológico e científico, bem como a expansão de esforços capacitativos de segurança cibernética (Cabinet Office, 2021; Cabinet Office, 2023).

Reiterando o escopo e ineditismo da diplomacia cibernética, Elaine Korzak, afiliada ao Centro de Segurança Internacional e Cooperação da Universidade Stanford destaca que:

> À medida que a tecnologia se torna cada vez mais importante, várias discussões sob o guarda-chuva da 'diplomacia cibernética' são notáveis, pois buscam construir um quadro normativo para o ciberespaço. Este quadro normativo é significativo e consequente - suas escolhas regulatórias têm implicações econômicas, políticas, sociais e de segurança para os estados individuais e para a comunidade internacional como um todo (Handler, 2021, s.p., tradução nossa).

Ademais, englobando a ênfase da política externa na documentação britânica, bem como o ponto de Korzak, Kaja Ciglic, diretora de diplomacia digital da Microsoft, argui que "A diplomacia cibernética difere de outras formas de diplomacia, pois é a primeira diplomacia verdadeiramente multistakeholder" (Handler, 2021, s.p., tradução nossa). Nesse sentido, abarca práticas e iniciativas essenciais para a digitalização e segurança de diferentes países, em especial de Estados como o Brasil, que tem a chance de usar seu histórico diplomático associado a uma economia emergente e em digitalização para um desenvolvimento sustentável no ciberespaço, bem como promoção de seus objetivos estratégicos na arena diplomática (Hurel, 2023).

5.21 Diretor de Segurança de Informação (*Chief Information Security Officer* - CISO)

O *Chief Information Security Officer* (CISO) é um cargo de executivo sênior responsável pela estratégia geral e pelo gerenciamento das iniciati-

vas voltadas para segurança da informação dentro de uma organização. O CISO desempenha um papel crucial em garantir a confidencialidade, integridade e disponibilidade dos ativos de informação da organização: as atividades geralmente exercidas por este profissional incluem a liderança estratégica e visão para os esforços de cibersegurança da organização, alinhando-os aos objetivos e metas de negócios. Dentre suas funções, pode-se mencionar: *i)* a identificação, avaliação e mitigação dos riscos de cibersegurança para proteger a organização contra possíveis ameaças e vulnerabilidades; *ii)* o desenvolvimento e a aplicação de políticas e procedimentos de segurança para garantir que os ativos de informação da organização estejam adequadamente protegidos; *iii)* o supervisionamento das operações de segurança, incluindo resposta a incidentes, detecção de ameaças e gerenciamento de vulnerabilidades, e a promoção de uma cultura de segurança dentro da organização; e, *iv)* a liderança de iniciativas de educação e treinamento aos funcionários sobre as melhores práticas de cibersegurança ("Papel do CISO em Negócios Digitais | Claranet", *[S.d.]*; "What Is a CISO?", [S.d.]; Phill, 2022).

5.22 Encarregado pelo tratamento de dados

O Encarregado é a pessoa responsável por garantir a conformidade de uma entidade, pública ou privada, em relação à implementação e ao cumprimento da Lei Geral de Proteção de Dados (LGPD), servindo como um canal de comunicação entre o controlador, os titulares dos dados e a Autoridade Nacional de Proteção de Dados. Sua previsão normativa no Brasil encontra-se nos artigos 5º, VIII e 41 da LGPD. Esse dispositivo não diferencia a obrigatoriedade entre entidades públicas ou privadas, motivo pelo qual ambas devem ter em seus quadros o encarregado.

Há exceção dessa figura que se encontra prevista na Resolução Normativa nº 2 da ANPD de 27 de janeiro de 2022 (Brasileiro, 2021), que regula a aplicação da LGPD para agentes de tratamento de pequeno porte. Nesse documento foi estabelecido, em seu artigo 11, que "os agentes de tratamento de pequeno porte não são obrigados a indicar o encarregado" (Brasileiro, 2021). Nesses casos, basta ao agente de tratamento disponibi-

lizar um canal de comunicação com o titular de dados. Caso haja essa indicação, entretanto, ela será considerada como política de boas práticas.

A lei não determina se o encarregado deve ser pessoa física ou jurídica ou se deve ser um funcionário da empresa ou um agente externo. A Agência Nacional de Proteção de Dados (2021) já se pronunciou no sentido de que encarregado poderá ser tanto um funcionário da instituição quanto um agente externo, de natureza física ou jurídica, mas a agência recomenda que o encarregado seja nomeado por um ato formal, tal como um contrato de prestação de serviços (entes privados) ou um ato administrativo (entes públicos) (Brasileiro, 2021).

Outro ponto importante é que não há proibição de que o encarregado represente diversas entidades ao mesmo tempo, contudo, é importante ressaltar que o controlador se certifique de que a função esteja sendo desempenhada de forma eficaz, vez que o controlador permanece sendo responsável legalmente pelas atividades de tratamento de dados pessoais (artigo 42 da LGPD).

Nomeado o encarregado, a LGPD determina que suas informações devem ser disponibilizadas publicamente no sítio eletrônico da empresa (sem necessidade de registro na ANPD), de forma clara e objetiva. Não se tem de forma expressa na lei que tipo de informações são essas, mas as boas práticas indicam que os detalhes para o contato dos usuários devem ser facilmente acessíveis, o que contribui para maior transparência para a proteção de dados.

A lei estabelece as seguintes competências, conforme determinação do artigo 41, § 2º: I - aceitar reclamações e comunicações dos titulares, prestar esclarecimentos e adotar providências; II - receber comunicações da autoridade nacional e adotar providências; III - orientar os funcionários e os contratados da entidade a respeito das práticas a serem tomadas em relação à proteção de dados pessoais; e IV - executar as demais atribuições determinadas pelo controlador ou estabelecidas em normas complementares.

Destaca-se, por fim, que o encarregado no Brasil é figura similar ao DPO (*data protection officer*) europeu, mas eles não são coincidentes, vez que a comparação das disposições legais pode evidenciar uma certa redução de previsões legais. A título de exemplo, a LGPD, diferentemente da *General Data Protection Regulation* (GDPR), não exige que o encarregado

seja independente. Contudo, é relevante que esse fato não afaste a importância de que os controladores assegurem autonomia para o exercício da atividade, a fim de evitar conflitos de interesse.

5.23 *Endpoint* (Ponto Final) e *Endpoint Security* (Segurança de Ponto Final)

Um *Endpoint* em termos de tecnologia da informação e segurança cibernética refere-se a qualquer dispositivo remoto que se comunica de volta e para com uma rede à qual está conectado. Os *endpoints* podem ser computadores (desktops e laptops), dispositivos móveis (como smartphones e tablets), servidores, terminais de ponto de venda (POS) e até dispositivos de Internet das Coisas (IoT). Em essência, qualquer dispositivo que esteja conectado a uma rede pode ser considerado um *endpoint* (Kadrich, 2007).

Na segurança de rede, a proteção de *endpoints* é crucial, pois esses dispositivos servem como pontos de acesso que podem ser explorados por agentes mal-intencionados para lançar ataques, roubar dados ou disseminar *malware*. Como os *endpoints* são os pontos finais da comunicação na rede, eles frequentemente armazenam, processam e transmitem dados sensíveis, tornando-os alvos atraentes para ataques cibernéticos.

A variedade de dispositivos *endpoint* possíveis torna incrivelmente desafiador instituir um sistema único adequado para protegê-los. Seus números em grandes redes de empresas também aumentam a chance de exploração, e a interação entre usuários e *endpoints* introduz preocupações comportamentais e de cultura de segurança. Outro ponto é que a digitalização dos serviços e mobilidade empresarial, bem como o crescente número de dispositivos conectados entre si, tornou ainda mais crítica a garantia da segurança. Neste sentido, para garantir uma segurança de *endpoint,* as empresas devem ter uma abordagem que requer que cada dispositivo de computação em uma rede corporativa cumpra certos padrões antes que o acesso à rede seja concedido.

Esses padrões podem exigir que o *endpoint* execute softwares especializados, por exemplo, produtos AntiVirus (AV) ou firewalls pessoais. Eles também podem especificar a configuração de segurança necessária para os *endpoints*, como, por exemplo, se o *endpoint* deve ser bloqueado

quando não estiver em uso, exigindo uma senha ou PIN para desbloquear. Aplicação de patches e atualizações de segurança regularmente para corrigir vulnerabilidades conhecidas nos sistemas operacionais e aplicativos também é exemplo de medidas. O importante é considerar que diferentes tipos de *endpoint*s terão diferentes capacidades e podem exigir diferentes padrões de segurança (Sandberg, 2013).

5.24 Engenharia Social

A Engenharia Social, no contexto da segurança da informação, contempla várias ações voltadas à exploração da falha ou do comportamento de uma pessoa com o fim de obter acesso a informações ou serviços (ENISA, 2023). As técnicas utilizadas para manipular ou ludibriar os indivíduos estão cada vez mais elaboradas e muito se assemelham a situações reais. Nesse cenário, as vítimas são induzidas a fornecerem as informações solicitadas, concederem acessos a arquivos ou a instalarem - deliberadamente ou por erro - softwares espiões, vulnerando, dessa maneira, as suas redes e sistemas no ciberespaço.

Essa prática normalmente contempla outros atos ilícitos como, por exemplo, fraudes, falsidade ideológica, utilização de identidade falsa e, após o acesso aos dados confidenciais e/ou pessoais, ameaças, chantagens, roubos bancários e outros. Ademais, ocorrem em ambientes plurais e, portanto, nos meios físicos (pelo contato direto com a vítima), digitais (como por e-mail ou aplicações de mensagens instantâneas), e por recursos de voz (ligações telefônicas).

Conforme o "Data Breach Investigations Report" ("2023 Data Breach Investigations Report", [S.d.]; "2023 Data Breach Investigations Report", [S.d.]), os ataques de engenharia social são muito eficazes e extremamente lucrativos, o que justifica o volume de incidência e crescimento contínuo. Pelo relatório, 74% de todas as violações mapeadas incluem o elemento humano e, portanto, pessoas envolvidas pelo erro, uso indevido de privilégios, uso de credenciais roubadas ou engenharia social. Isso enaltece a relevância da implementação de programas de sensibilização/conscientização e capacitação de profissionais nas organizações. Por fim, insta mencionar que o material elenca como as três principais formas de golpes o *phishing* (tipo de engenharia social, elucidado adiante), o roubo de credenciais e a exploração de vulnerabilidades.

5.25 *Phishing*

Phishing, no vernáculo, significa "estelionato de dados" (Belli *et al*., 2023b, p. 28). É um tipo de engenharia social no qual o(s) criminoso(s), por meio de fraude, engana(m)/ludibria(m) o indivíduo ao fazê-lo crer em uma determinada informação e, em razão disso, levá-lo a entregar voluntariamente dados pessoais e sigilosos ou a conceder acessos a determinados bancos de dados (com ou sem a respectiva ciência). Essa prática ilícita poderá envolver outras condutas ou recursos como, por exemplo, a utilização de *malwares* para roubo de informações e, com acesso aos dados, a realização de ameaças e chantagens para moldar comportamentos, roubo de credenciais para obtenção de ganhos financeiros por transferências bancárias, contratação de empréstimos, pagamentos e outros. Importante ressaltar que, para além dos eventuais prejuízos supracitados, sobrevém, de forma intrínseca, a violação dos direitos dos titulares de dados.

Conforme o relatório da (ENISA, 2023, p. 11), as principais ameaças correlatas ao *phishing* são: *i)* o *spear-phishing*, ataque dedicado a uma pessoa especificamente, ou a grupo específico de pessoas; *ii)* a *whaling* (caça à baleia), tipo de ataque cujos alvos são indivíduos de alto escalão, como diretores, gerentes, cargos de confiança e outros; *iii) smishing*, golpe aplicado por meio de SMS; *iv) vishing*, quando se utiliza de recurso de voz como, por exemplo, ligações telefônicas; *v)* comprometimento de e-mail profissional; *vi)* fraude; *vii)* falsidade ideológica (*counterfeiting*); e *viii)* passar-se por terceiro (*impersonation*); por fim, acresce-se o *ix) QRishing*, no qual há a utilização de códigos QR maliciosos pela sobreposição do QR legítimo ou pelo redirecionamento do URL correspondente para outro (URL) ilegítimo (Belli *et al*., 2023b, p. 29).

5.26 Gestão de Identidade e Acesso (*Identity Access Management* - IAM)

A Gestão de Identidade e Acesso (IAM), também conhecida como Gerenciamento de Identidade e Acesso, refere-se a um conjunto de políticas e tecnologias que garantem que indivíduos, sistemas e serviços tenham representações virtuais que lhes permitam acessar dados e recursos

específicos. Essas identidades podem ser gerenciadas, alocadas e utilizadas para controlar, monitorar e relatar as atividades de pessoas e sistemas. O controle é alcançado através da clara articulação de procedimentos baseados em identidade em documentos de política, juntamente com o monitoramento diário da conformidade por parte da equipe.

O objetivo principal da gestão de identidade é assegurar que apenas usuários autenticados tenham acesso a aplicativos, sistemas ou ambientes de TI para os quais estão autorizados. Isso inclui controle sobre o provisionamento de usuários e o processo de integração de novos usuários, como funcionários, parceiros, clientes e outras partes interessadas. A gestão de identidade também abrange o controle sobre a autorização de permissões de sistema ou rede para usuários existentes, assim como a desativação de usuários não autorizados a acessar os sistemas da organização. Ainda, determina se um usuário poderá ter acesso a sistemas e define o nível de acesso e permissões que um usuário possui em um sistema específico. Por exemplo, um usuário pode ser autorizado a acessar um sistema, mas restrito a alguns de seus componentes. Já a gestão de acesso trata do controle e gerenciamento do acesso do usuário a recursos, incluindo definição e aplicação de políticas de acesso, controle baseado em funções (RBAC – *role-based access control*) e garantia de que os usuários tenham o nível apropriado de acesso com base em suas funções e responsabilidades (Pretesh Biswas, 2023; Souppaya; Scarfone, 2016).

5.27 Governança

Governança, assim como regulação, é uma palavra que possui muitos sentidos, existindo divergências que refletem a existência de disputas teóricas sobre um determinado fenômeno social. É por isso que, a depender da área que utiliza o conceito de governança como objeto ou do problema em que o autor está interessado, serão adotadas diferentes características e implicações do fenômeno que se tenta apreender (Goertz, 2006).

A literatura de ciência política aborda a governança como uma teoria sobre o controle concentrando-se em explicar como o setor público é capaz de fornecer direção para a sociedade e a economia (Peters, 2011) e apresen-

ta quatro possíveis sentidos, isto é, governança pode referir-se a estrutura, processo, mecanismo ou estratégia (Levi-Faur, 2012, p. 8).

Como estrutura, área em que o desenvolvimento pela literatura foi mais forte, a governança significa a arquitetura de instituições formais e informais. Como processo, volta-se à dinâmica e às funções de direção envolvidas nos processos de elaboração de políticas. Como mecanismo, significa os instrumentos de tomada de decisão, de cumprimento e de controle. Como estratégia, denota os esforços dos atores para governar e manipular a concepção de instituições e mecanismos, a fim de moldar escolhas e preferências (Levi-Faur, 2012, p. 8).

Robert Gorwa (2019, p. 4) explica que a governança, antes associada a governos domésticos, era entendida como uma "capacidade do governo elaborar, fazer cumprir as regras e prestar serviços" (Gorwa, 2019, p. 4). Contudo, após a década de 1990, sob a influência da globalização, o tema passou a ser tratado com uma dimensão muito mais abrangente. Essa nova concepção substituiu o estado-centrismo das relações de poder e conflito por formas mais híbridas e descentralizadas das estruturas de governança oriundas do século XX, formadas amplamente por atores não estatais, em resposta à complexidade das questões surgidas na sociedade contemporânea.

Hoje, conforme apontado por Clara Keller (2019, p. 78), essa terminologia está associada a novos processos de governar, o que faz com que governança possa englobar arranjos públicos, privados ou multissetoriais. Um conceito interessante (e aplicável no campo da cibersegurança) é trazido por Papaevangelou, para o qual, após uma revisão da bibliografia sobre o assunto, governança pode ser entendida como "uma estrutura complexa em rede que acomoda diferentes partes interessadas, que estão conectadas e coordenadas por meio de vários tipos de regulamentos, normas e práticas" (Papaevangelou, 2021, p. 3).

Dentro do cenário da cibersegurança, então, é recomendável que a governança seja entendida como estrutura em rede que acomoda diferentes partes interessadas, pois a complexidade da matéria inerente ao setor exige que o ambiente seja colaborativo para o compartilhamento de conhecimento e promoção de maior resiliência.

5.28 Hacking Ético (*Ethical hacking*)

Ethical hacking se refere à aplicação autorizada de técnicas de *hacking* para identificação de vulnerabilidades de sistemas, com o objetivo último de aprimorar as capacidades defensivas da organização-alvo. Hackers éticos atuam identificando e relatando vulnerabilidades, realizando testes de penetração (*pentests*) para pôr à prova as capacidades de resposta de uma organização, além de proverem informações a respeito de *malware* e análise de riscos. Sua atuação pode revelar, por exemplo, suscetibilidade a engenharia social, incluindo *phishing*, ou a existência de vulnerabilidades de dia zero ("What is Ethical Hacking?", *[S.d.]*; "What is Ethical Hacking | Who is an Ethical Hacker", *[S.d.]*).

De modo geral, o componente ético da atuação de um hacker ético é fundado em sua atuação ter sido autorizada, acordada e detalhada com a organização-alvo; não provocar danos duradouros aos sistemas avaliados, restringindo-se a identificar e apontar vulnerabilidades e explorá-las com este mesmo intuito; e observar segredo e privacidade das informações acessadas. Esquematicamente, a atuação do hacker ético parte de reconhecimento e estudo do alvo, passando à obtenção de acesso não autorizado ao sistema e avaliação das vulnerabilidades, manutenção do acesso, limpeza dos vestígios do ataque e, finalmente, provisão de um relatório detalhado ("Ethical Hacking", 2022).

5.29 Incerteza cibernética

A incerteza cibernética é um conceito elusivo por definição. Proveniente da arquitetura e complexidade do ciberespaço, a incerteza cibernética diz respeito à falta de clareza quanto ao alvo, escopo e responsabilidade de uma ocorrência cibernética (Medeiros; Goldoni, 2020). A incerteza cibernética decorre especificamente de dois elementos intrínsecos ao ciberespaço: a dificuldade de mensuração do sucesso e o anonimato.

A mensuração do sucesso no domínio cibernético apresenta desafios significativos. Devido à sua natureza altamente complexa, interconectada e mutável, uma ação nesse ambiente é difícil de ser prontamente detectada ou quantificada. Isso se deve, em parte, à não imediatez dos efeitos, espe-

cialmente em casos de obtenção de inteligência e monitoramento de alvos, que ficam ocultos sob complexas camadas de redes informacionais. Em vista dessa complexidade de redes, rastrear uma consequência específica até uma ação causadora torna-se uma tarefa desafiadora, uma vez que os resultados não são sempre precisos ou diretamente observáveis. Isso ocorre, em parte, porque os efeitos não são necessariamente cinéticos ou imediatos. Logo, em oposição aos efeitos imediatos e explícitos de uma explosão ou um roubo a banco nos domínios tradicionais, um ato de sabotagem ou de crime cibernético pode permanecer encoberto por longos períodos.

Por seu turno, o anonimato, concebido como a dificuldade de vincular ações a atores específicos em locais determinados, é inerente ao domínio cibernético devido aos processos de governança e à própria arquitetura da Internet (Wheeler; Larsen, 2003). A importância da atribuição no ciberespaço é crucial, pois é a partir da identificação dos infratores que se inicia o processo legal e político de responsabilização (Hunker; Hutchinson; Jonathan, 2008).

A incerteza cibernética, mais evidentemente, pode ser melhor compreendida como a não obviedade de uma ocorrência. Dada a complexidade e o anonimato do ciberespaço, todo tipo de ambiguidade ocorre. Como explica Libicki:

> A ambiguidade é o cerne da não obviedade. Se a vítima não tem certeza de quem realizou uma operação, pode hesitar em responder da mesma forma como faria se tivesse certeza. Alternativamente, o restante do mundo pode ter dúvidas mesmo se a vítima estiver certa, fazendo com que ela fique cautelosa ao responder, como se outros estivessem muito certos dos fatos (Libicki, 2012a, p. 89, tradução nossa).

Isto é, mesmo que determinada ocorrência seja identificada, seu escopo e atribuição podem ser debatidos, travando o processo de responsabilização, engendrando uma negação plausível a possíveis culpados.

A incerteza cibernética não provém apenas de elementos técnicos e administrativos, mas também se manifesta como um fator distinto no domínio cibernético, à medida que diversos atores exploram o anonimato, transformando-o em uma rede anônima onde a atribuição e a responsabilidade se tornam tarefas cada vez mais desafiadoras. Ainda, o elemento de

incerteza está intrinsecamente ligado à distribuição de poder no ciberespaço e à natureza desterritorializada desse domínio. Isso resulta em um contexto no qual múltiplos atores podem atuar globalmente, buscando seus interesses de maneira evasiva, pautada na incerteza cibernética.

5.30 Incidente de segurança

Incidente é um evento adverso (indesejado ou inesperado), isolado ou em série, que tenha o potencial expressivo de vulnerar a segurança da informação. Precisamente, pela concepção tradicional e restritiva, trata-se de ação voluntária ou acidental que compromete a confidencialidade, a integridade e/ou a disponibilidade da informação. Por definição de alcance mais amplo, consoante referência do padrão internacional ISO/IEC 27000:2012(E), acrescem-se as ofensas à autenticidade, à prestação de contas e à responsabilidade (*accountability*), ao não repúdio e à confiança (International Organization for Standardization, 2012, p. 10).

Ora, para (muito) além de ataques ou falhas que levam à perda, destruição, bloqueio ou acesso não autorizado às informações, sistemas, ou infraestruturas críticas, os incidentes de segurança referem-se igualmente aos comportamentos inseguros (irresponsáveis ou antijurídicos) que, especialmente quando situados no ambiente cibernético, podem afetar a segurança das estruturas democráticas, a proteção de dados pessoais e a própria coletividade (Belli et al., 2023b, p. 24–25).

Dessa maneira, no intuito de promover uma compreensão alargada sobre a expressão, evidencia-se a necessidade de reparti-la em quatro elementos, relativos, portanto, *i)* ao ambiente, na medida em que o evento poderá ocorrer tanto no espaço virtual ou cibernético (por exemplo, um ciberataque ou o compartilhamento de dados para pessoas não autorizadas), quanto no físico (como eventual acesso indevido aos arquivos físicos e aos documentos impressos); *ii)* ao aspecto material, haja vista que a informação em potencial risco poderá ser relativa às pessoas físicas (dados pessoais, dados pessoais sensíveis e dados anonimizados) e/ou às pessoas jurídicas (dados financeiros de organizações, dados estratégicos, organizacionais e outros); *iii)* volitivo, passível de advir de conduta ofensiva (ação criminosa como um ataque hacker, compartilhamento de segredo de ne-

gócio com terceiros etc.), de falha ou erro humano (como o mau uso de softwares, a exposição de telas por descuido, o descumprimento de políticas de segurança de informação e outros) e de problemas técnicos relacionados às redes, aos softwares e aos sistemas utilizados nas atividades de tratamento de informações (como a não atualização de softwares, as falhas nos acessos privilegiados ou de outros controles implementados); e *iv)* jurídico, evento decorrente de ação lícita ou ilícita.

Face ao potencial lesivo, aborda-se especificamente o ciberespaço. Assim, de maneira objetiva e sucinta, o padrão produzido pelo National Institute of Standards and Technology (NIST), "*Cybersecurity Framework*", define "incidente de cibersegurança" como "um evento de segurança cibernética que foi considerado de impacto na organização, gerando a necessidade de resposta e recuperação" ("Cybersecurity Framework", 2018, p. 45, tradução nossa). Nesse sentido, no âmbito nacional, cita-se definição proposta no Anteprojeto de lei relativo à Política Nacional de Cibersegurança (PNCiber) e ao Sistema Nacional de Cibersegurança (SNCiber), no qual "ciberincidente" significa "uma ciberofensa combinada ao ciberefeito real ou potencial dela resultante", sendo "ciberofensa" um "conjunto de ações tomadas no ciberespaço contra um ciberativo" (art. 4º, inciso II), "ciberefeito", "dano, permanente ou temporário, indisponibilidade ou limitação da operação, total ou parcial, ou mudança de comportamento, de um ativo cibernético ou não, resultante de uma ciberofensa" (art. 4º, inciso IV), que recairá sobre um "ciberativo", portanto, "hardware, software ou dados utilizados para o processamento e transmissão eletrônicos de informações" (art. 4º, inciso I).

As estratégias e metodologias orquestradas para elaboração das definições supramencionadas ilustrativamente são plurais. Sejam mais detalhadas, sejam de cariz procedimental, todas elevam os incidentes como eventos atípicos e danosos à segurança da informação, remetendo à conclusão impreterível da necessidade de ações preventivas de mitigação de riscos e, após a ocorrência, de resposta e restauração ágil do estado primário de segurança.

5.31 *Malware*, Vírus e *Ransomware*

Malware advém da fusão dos termos "*malicious* + *software*" e, portanto, significa "software malicioso" ("O que é malware?", 2021). Nesse sentido, re-

presenta toda aplicação capaz de causar danos e gerar prejuízos em sistemas e dispositivos. Podem se apresentar por *links* ou códigos QR disponibilizados, por exemplo, por e-mails e aplicações de mensageria instantânea, que direcionam a vítima a sua instalação (Belli *et al.*, 2023b, p. 28). Infectados por esses softwares, é possível que haja a intercepção, o sequestro e o roubo de dados, bem como danos aos sistemas e dispositivos, monitoramento de ações (*spyware* ou softwares espiões), entre outras violações.

Dentre aqueles recorrentes, elencam-se os diferentes vírus de dispositivos eletrônicos (tipo de *malware* que se fixa a arquivos e sistemas, capaz de se multiplicar e espalhar autonomamente), os softwares *worms* ("vermes" que se multiplicam com o fim de afetar diferentes dispositivos e/ou sistemas); os cavalos de Tróia (arquivos infectados por vírus) e os *ransomwares* (meio pelo qual os criminosos, após reterem arquivos, dispositivos e/ou sistemas, os tornam indisponíveis – normalmente pela encriptação – e requisitam resgate para a respectiva devolução) (ENISA, 2023).

As ameaças e ataques cibernéticos representam um risco a todas as esferas da sociedade, da economia e da democracia. Portanto, "Além de operações comerciais, são também interrompidos ou afetados por ataques de *ransomware*, vazamento de dados etc. serviços públicos, infraestrutura crítica e os próprios processos democráticos" (Belli *et al.*, 2023b, p. 19). Nesse sentido, ante o atual cenário, o *ransomware* figura como o ataque mais expressivo às infraestruturas críticas, precisamente nos setores do transporte e da aviação europeus (ENISA, 2022b, 2022b).

5.32 Medidas defensivas (*Defensive Measures*)

Correspondem às medidas práticas da defesa cibernética, comumente atuando em conjunto com medidas de cibersegurança, em decorrência da permeabilidade e sinergia entre defesa e segurança cibernética. Contudo, enquanto medidas de segurança são compreendidas como medidas destinadas a garantir sigilo, inviolabilidade, integridade, autenticidade e disponibilidade da informação classificada em qualquer grau de sigilo (GSI, 2021b, p. s. p.); medidas defensivas estão direcionadas a estratégias e práticas de defesa ativa contra adversários e ameaças externas.

Holisticamente, o termo "medidas defensivas" refere-se a qualquer ação, dispositivo, procedimento, assinatura, técnica ou outra abordagem aplicada a um sistema de informação, ou às informações armazenadas, processadas ou em trânsito nesse sistema, com o objetivo de detectar, prevenir ou mitigar uma ameaça cibernética conhecida ou suspeita, ou uma vulnerabilidade de segurança ("CISA Cyber Threat Indicator and Defensive Measure Submission System | CISA", *[S.d.]*). Essas medidas defensivas da ciberdefesa incluem:

- **Inteligência de ameaças**: monitoramento contínuo para identificar e antecipar possíveis ataques.
- **Sistemas de detecção de intrusão (IDS)**: ferramentas que identificam acessos não autorizados e atividades suspeitas nas redes.
- **Firewalls**: barreiras que controlam o tráfego de dados entre redes para bloquear acessos indesejados.
- **Software *antimalware***: proteção contra programas maliciosos, como vírus e *ransomware*.
- **Estratégias de resposta a incidentes**: planos estruturados para mitigar os danos e recuperar a segurança após um ataque.

Adicionalmente, dentro de um ambiente dinâmico como o da segurança cibernética, medidas defensivas também podem ocorrer em um contexto de disputa militar. Nesse sentido, a Doutrina Militar de Defesa Cibernética do Brasil (Ministério da Defesa, 2023, p. 18) destaca que, em conformidade com o arcabouço jurídico em voga, medidas de defesa cibernética podem incluir operações cibernéticas defensivas destinadas a detectar, conter e remediar ameaças, restaurando a segurança de redes ou sistemas comprometidos. Grande parte dessas operações envolve a identificação e neutralização de ameaças avançadas e persistentes, bem como a aplicação de contramedidas ativas para reduzir riscos e impactos. Ainda, em cenários críticos, tais medidas podem abranger ações para restabelecer a integridade operacional de infraestruturas digitais essenciais, garantindo a resiliência dos sistemas frente a ameaças emergentes e adversariais.

5.33 Negação de Serviço Distribuída (*Distributed Denial of Service* - DDoS)

Um ataque de Negação de Serviço (*denial of service*) busca impedir o provimento normal de um determinado serviço. Um ataque distribuído de negação de serviço tem o mesmo objetivo, mas atua por meio de múltiplas entidades atacantes. Em um sistema de computadores, portanto, um ataque DDoS pode visar interromper a capacidade de um roteador, um servidor ou outro tipo de serviço de responder às requisições recebidas de usuários genuínos. Isto acontece porque o serviço é inundado por requisições ilegítimas, o que sobrecarrega a sua capacidade de resposta a requisições legítimas.

Há muitas formas de se realizar um ataque DDoS, como métodos de múltiplas requisições a roteadores (os chamados ataques *smurf* e *fraggle*, hoje em dia mitigados pela tecnologia de roteadores mais moderna) e ataques de porta entreaberta ou ataques de requisições SYN (Cloudflare, *[S.d.]*). Este tipo se realiza, inclusive, por meio de *botnets*, como a Mirai ("O que é a botnet Mirai?", *[S.d.]*), composta por dispositivos IoT vulneráveis (Mirkovic; Reiher, 2004).

Este tipo de ataque pode interromper atividades cruciais e tem se tornado cada vez mais frequente: por exemplo, a empresa de segurança cibernética Akamai reportou (Dummer; Rath, *[S.d.]*) aumento de 50% em ataques DDoS de alto volume entre 2021 e 2023 dentre seus clientes, enquanto a Cloudflare aponta (Cloudflare, 2024), dentre outros dados, um aumento de 117% destes ataques contra sites de lojas de departamento, envios e relações públicas durante a Black Friday em 2023 e um aumento de 61,839% contra sites de serviços ambientais, em torno do período de realização da COP 28, em comparação com o mesmo período do ano anterior.

5.34 Organismos de compartilhamento de informação: CERT, CSIRT, ETIR e ISACs

Equipe de resposta a emergências informáticas (*Computer Emergency Response Team* - CERT), Equipe de resposta a incidentes de segurança in-

formática *(Computer Security Incident Response Team* – CSIRT) e/ou Equipe de Prevenção, Tratamento e Resposta a Incidentes Cibernéticos (ETIR) correspondem à linha de frente da defesa e segurança cibernética. Como indicado pela composição de seu acrônimo, são as equipes responsáveis por detectar, identificar, mitigar e prevenir incidentes cibernéticos.

As equipes de respostas a incidentes podem ser de origem privada ou pública e têm sua atividade marcada pela cooperação entre equipes, haja vista a capacidade de proliferação de incidentes cibernéticos. Dependendo da estrutura organizacional de um país, a cooperação entre as equipes de CERTs e CSIRTs pode ser institucionalizada. No caso brasileiro, as equipes atuam em conjunto com o CERT.br (Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil), um CSIRT multissetorial, de âmbito nacional, que oferece serviços especializados em Gestão de Incidentes de Segurança da Informação para qualquer rede que utilize recursos administrados pelo NIC.br, organização responsável pela implementação das decisões do Comitê Gestor da Internet no Brasil (CGI.br) e pela administração do domínio ".br" ("CERT.br - Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil", [s.d.]).

Adicionalmente, no tocante à notificação de incidentes cibernéticos, pela estrutura política administrativa do Brasil, consolidada pela ReGIC (Rede Federal de Gestão de Incidentes Cibernéticos - Decreto nº 10.748, de 16 de julho de 2021) (GSI, 2021a), CERTs locais devem se reportar às equipes de respostas de incidentes de sua respectiva agência setorial, que então notifica o CTIR.gov, o Centro de Prevenção, Tratamento e Resposta a Incidentes Cibernéticos de Governo.

Por fim, é pertinente apresentar a definição proposta pela ReGIC, e compartilhada pelo Glossário de Segurança da Informação - elaborado pelo GSI, e mantendo, portanto, o escopo de entidade pública - no qual uma ETIR diz respeito a um:

> grupo de agentes públicos com a responsabilidade de prestar serviços relacionados à segurança cibernética para o órgão ou a entidade da administração pública federal, em observância à política de segurança da informação e aos processos de gestão de riscos de segurança da informação do órgão ou da entidade (GSI, 2021b, s.p.).

Enquanto CERTs têm como foco principal a resposta técnica a incidentes cibernéticos, ISACs (Centros de Análise e Compartilhamento de Informações) correspondem a entidades confiáveis e especializadas que coletam, analisam e disseminam alertas e relatórios de incidentes, além de compartilhar e fornecer apoio analítico a governos e a outros ISACs (ENISA, 2025). Nesse sentido, seu propósito é fortalecer a consciência situacional, antecipar ameaças por meio do compartilhamento de alertas e tendências e consolidar uma cultura colaborativa de cibersegurança. Além disso, enquanto os CERTs costumam ser estruturas menores e operacionais, os ISACs possuem escopos mais amplos e envolvem diversos *stakeholders*, indicando boas práticas internacionais em governança, confiança e interoperabilidade. Dessa forma, os ISACs não substituem, mas complementam e potencializam a atuação dos CERTs, desempenhando um papel central na construção de uma resiliência cibernética mais integrada e eficaz (Sekoia, 2025).

5.35 Poder cibernético

Como conceito, o poder cibernético evoca definições similares aos demais domínios. Isto é, bem como existem o poder marítimo e o poder aéreo, nos mares e céus; o poder cibernético se desenvolve no ciberespaço (Nye, 2012). Joseph Nye, por exemplo, compara o poder cibernético aos poderes marítimo, aéreo e espacial, estabelecendo paralelos entre a operacionalização desses domínios tradicionais para atingir objetivos estratégicos específicos (Nye, 2012). Contudo, a operacionalização destes domínios não ocorre de forma estanque e assim como os poderes aéreo e marítimo podem influenciar resultados no domínio terrestre, e vice-versa, o poder cibernético demonstra uma interoperacionalidade intrínseca decorrente da permeabilidade do ciberespaço na sociedade atual. Nesse contexto, Nye define o poder cibernético como a capacidade de obter efeitos estratégicos no e através do ciberespaço.

Essa interoperacionalidade é o que permite a Daniel Kuehl (Kuehl, 2009) expandir a concepção de poder cibernético, considerando a multidimensionalidade sinérgica do ciberespaço. Para Kuehl, o poder cibernético é a capacidade de usar o ciberespaço para criar vantagens e influenciar eventos em todos os ambientes operacionais, não se limitando ao domínio cibernético ou aos instrumentos militares.

John Sheldon, por sua vez, introduz uma distinção importante entre os termos "ciberespaço" e "poder cibernético" (Sheldon, 2014). Enquanto o ciberespaço é o domínio onde ocorrem operações cibernéticas, o poder cibernético é a soma dos efeitos estratégicos gerados por essas operações, influenciando os domínios terrestre, marítimo, aéreo, espacial e cognitivo. Sheldon destaca que o ciberespaço não apenas promove efeitos estratégicos sinérgicos por meio da interoperacionalidade, mas também permite a operacionalização dos domínios tradicionais na atualidade ao passo que a vasta maioria das tecnologias modernas depende de *hardwares* que compõem a camada física do ciberespaço e/ou das redes que lhe proporcionam alcance global e caracterizam a sociedade globalizada. Nesse sentido, segundo Sheldon, o ciberespaço capacita a ação nos instrumentos nacionais de poder, como economia, diplomacia e militares.

As definições propostas por Kuehl (2009), Sheldon (2011) e Nye (2012) não apenas percebem o poder cibernético em sua dimensão mais direta, através do uso coercitivo de operações cibernéticas ofensivas ou defensivas, mas também como uma forma de poder brando, vislumbrado pela economia e diplomacia. Isso significa que o poder cibernético engloba diversas abordagens nas quais os efeitos desejados podem ser alcançados não apenas coercitivamente, mas também por meio da influência cultural ou econômica, potencializadas pela onipresença do ciberespaço.

5.36 Privacidade desde a concepção (*Privacy by design*) e Privacidade por Padrão (*Privacy by default*)

Não há um conceito preciso sobre privacidade, embora a literatura tente defini-la. É importante destacar que qualquer tentativa de conceituação, entretanto, deve considerar que a privacidade é uma noção cultural e que pode ser observada no curso do tempo por fatores condicionantes sociais, econômicos e políticos. O direito à privacidade passou a ter reconhecimento global após a Segunda Guerra Mundial, quando a noção dos direitos à personalidade tornou-se universal, notadamente, em razão do reconhecimento do direito à dignidade da pessoa humana como centro dos sistemas jurídicos (vide a Declaração Universal de Direitos Humanos, artigo 12).

O avanço das tecnologias, a digitalização e o uso massivo de dados forçaram a evolução do conceito de privacidade. Se antes a coleta de dados não era atraente para as empresas privadas em razão dos altos custos, tanto para o seu tratamento como para a própria coleta, esse cenário mudou (Doneda, 2019). Hoje, um acervo amplo de informações coletadas sobre uma determinada pessoa permite que organizações, estados ou empresas exerçam controle sobre a pessoa humana e coloquem em risco a privacidade das pessoas.

Nesse sentido, passou-se a entender que havia uma "certa defasagem entre seu conceito original e o que ele efetivamente representa" (Doneda, 2019, p. 29). O aspecto mais destacado da privacidade passou a ser o controle da circulação de informações pessoais. A preocupação passa a estar relacionada com o uso que as outras pessoas fazem das informações que digam respeito a uma determinada pessoa (Rodotà *et al*., 2008, p. 74–75).

A partir daí pode-se observar que diversos países adotaram leis de proteção de dados que refletiam as "Práticas Justas de Informação" (sigla em inglês: FIPs - *Fair Information Practices*), isto é, a adoção de princípios universais de privacidade para o manuseio de dados pessoais. Contudo, essas legislações passaram a ser ferramentas insuficientes para exigir conformidade nos produtos e serviços que eram oferecidos por tecnologias digitais e proteção à privacidade do consumidor. Uma postura proativa passou a ser necessária (Cavoukian, 2012).

Privacy by Design foi a abordagem abraçada pelas legislações dos mais variados países para estabelecer a proteção da privacidade dos usuários como um pilar essencial desde o início do desenvolvimento de um sistema, produto ou serviço. A ideia é integrar medidas de privacidade diretamente na arquitetura e no ciclo de vida do projeto, em vez de tratá-las como uma preocupação secundária.

Os princípios universais das Práticas Justas de Informação (FIPs) são afirmados pelos princípios do *Privacy by Design*, mas vão além deles em busca do mais alto padrão global possível, o que representa um aumento significativo no padrão de proteção da privacidade. Isso significa que a privacidade deve ser incorporada aos sistemas e tecnologias de dados em rede, por padrão. Essa abordagem, segundo Cavoukian, é exteriorizada por meio de princípios fundamentais, dentre eles o *Privacy by Design*, para orientar a implementação da privacidade desde a concepção (Cavoukian, [S.d.]).

Ao adotar a abordagem de *Privacy by Design*, as organizações buscam não apenas atender aos requisitos legais de privacidade, mas também estabelecer uma cultura e práticas que promovam a proteção da privacidade como um valor central em todas as suas atividades. Esse valor está expresso na Lei Geral de Proteção de Dados, bem como na Política Nacional de Cibersegurança.

5.37 Proteção de dados

A disciplina da Proteção de dados é um campo interdisciplinar que se concentra na regulamentação do tratamento dos dados pessoais para fortalecer os direitos das pessoas às quais se referem os dados e, ao mesmo tempo, permitir que os dados sejam utilizados de forma lícita e não abusiva.

O direito à proteção de dados pode ser considerado como uma evolução do direito à privacidade. Porém, vários autores destacam a existência de importantes diferenciais entre privacidade e proteção de dados em termos de âmbito e fundamentação. Conceitualmente, os direitos à privacidade e à proteção de dados pessoais podem ser enquadrados como sendo construídos sobre premissas divergentes: a proteção de dados almeja a transparência do tratamento de dados, enquanto a privacidade visa criar uma barreira de opacidade por volta da esfera pessoal do indivíduo (De Hert; Gutwirth, 2006).

Desde a década dos anos 1970, a disciplina da proteção de dados evoluiu em resposta às mudanças tecnológicas, sociais e legais. A introdução de leis e regulamentações específicas, como o Regulamento Geral de Proteção de Dados (GDPR), a Lei Geral de Proteção de Dados (LGPD), ou as mais recentes leis chinesa e indiana, representa marcos importantes na evolução da disciplina (Belli; Doneda, 2023). Essas regulações estabeleceram princípios fundamentais de proteção de dados, como o princípio de finalidade, de adequação, de necessidade, de livre acesso, de qualidade dos dados, de transparência, de segurança de prevenção, de não discriminação e de responsabilização e prestação de contas.

A ubiquidade de tecnologias de processamento de dados e computação, juntamente com a crescente emergência de riscos associados à divulgação indiscriminada de informações pessoais, impulsiona a necessidade de regulamentação e proteção legal dos dados. Assim, cabe ressaltar que a

proteção de dados não apenas protege os direitos individuais dos titulares dos dados, mas também promove a confiança e a transparência nas relações comerciais e sociais, impulsionando a inovação e o progresso tecnológico de forma sustentável.

5.38 Protocolo de Transferência de Arquivos Seguro (*Secure File Transfer Protocol* - SFTP)

O Protocolo de Transferência de Arquivos Seguro, também conhecido como SFTP (do inglês *Secure File Transfer Protocol*), é um protocolo de rede que facilita transferências seguras e criptografadas de arquivos e informações por meio de uma rede de dados. Ele é uma extensão do protocolo SSH (Secure Shell), fornecendo um canal seguro para transmissão e autenticação de dados (Barrett; Silverman; Byrnes, 2005). O SFTP é amplamente utilizado para transferir arquivos com segurança entre sistemas remotos, garantindo confidencialidade, integridade e autenticação dos dados transmitidos. Isso é feito por meio de uma combinação de mecanismos de criptografia e autenticação para garantir a segurança das transferências de arquivos entre o cliente e o servidor.

O cliente é o sistema ou usuário que inicia a solicitação de transferência de arquivos, podendo ser um computador, um software ou um indivíduo. Além disso, o cliente é responsável por estabelecer uma conexão segura com o servidor, autenticar-se usando chaves criptográficas (pares de chaves pública-privada) e solicitar transferências de arquivos. Já o servidor é o sistema remoto que hospeda os arquivos e fornece acesso a eles, aguardando conexões SFTP entrantes, autenticando o cliente e respondendo às solicitações de transferência de arquivos. O servidor é responsável por gerenciar o armazenamento e a recuperação de arquivos, garantindo a segurança e a integridade dos dados durante a transferência. O cliente desempenha um papel ativo na inicialização da conexão segura, autenticação e solicitação de transferências de arquivos, enquanto o servidor responde a essas solicitações e gerencia as operações reais de arquivos.

O canal de comunicação via SFTP é protegido por meio de algoritmos criptográficos, impedindo o acesso não autorizado e a espionagem das infor-

mações sendo transmitidas. O processo de autenticação envolve a validação da identidade tanto do cliente quanto do servidor usando chaves criptográficas.

Em relação à criptografia, ressalta-se que o protocolo SFTP suporta vários algoritmos de criptografia para garantir a segurança dos dados durante a transmissão. Algoritmos comuns incluem AES (Padrão de Criptografia Avançada, ou *Advanced Encryption Standard*), 3DES (Padrão Triplo de Criptografia de Dados, ou *Triple Data Encryption Standard*) e *Blowfish*. A escolha do algoritmo de criptografia deve levar em consideração os requisitos de segurança e de compatibilidade dos sistemas envolvidos.

Por sua vez, a autenticação no SFTP geralmente é baseada em pares de chaves criptográficas. Os usuários geram um par de chaves pública-privada, onde a chave pública é armazenada no servidor e a chave privada é mantida em segredo no cliente. Esse método aprimora a segurança eliminando a necessidade de autenticação baseada em senha, reduzindo o risco de acesso não autorizado.

5.39 Regulação

Regulação é um conceito polissêmico e interdisciplinar, pelo que pode variar de acordo com a área de estudo relacionada (economia, ciência política ou sociologia, por exemplo). Como conceito, é interessante pontuar que essas divergências refletem a existência de disputas teóricas sobre um determinado fenômeno social. É por isso que, a depender da área que utiliza o conceito de regulação como objeto ou do problema em que o autor está interessado, serão adotadas diferentes características e implicações do fenômeno que se tenta apreender.

Baldwin, Cave e Lodge explicam que o termo é, muitas vezes, identificado com atividade governamental. Contudo, os autores alertam que a palavra deve ser pensada em vários sentidos, citando três deles:

> a) como um conjunto específico de comandos, no qual a regulação envolve um conjunto de regras vinculantes aplicáveis por um determinado corpo e acompanhada de algum mecanismo para monitorar o cumprimento dessas regras;
> b) como influência estatal deliberada, na qual a regulação abrange todas as ações estatais que são projetadas para influenciar o comportamento social ou empresarial e dirigir a economia; e

> c) como forma de controle social, isto é, formas de influência social ou econômica, onde todos os mecanismos que afetam o comportamento, sejam eles provenientes do Estado ou de outras fontes, são considerados regulatórios (Baldwin; Cave; Lodge, 2012).

Segundo os autores, advogados, cientistas políticos e economistas focam nos dois primeiros sentidos, enquanto estudiosos sociojurídicos adotam mais comumente a terceira acepção.

Um conceito de grande relevância para aplicação de áreas que envolvem tecnologia é aquele trabalhado por Black e Kingsford Smith (2002, p. 26), que restringe o âmbito de aplicação do termo a um sistema de controle intencional e que requer a existência de três elementos: estabelecimento de padrões, coleta de informações e modificação de comportamento. Para a autora, regulação é "a tentativa sustentada e focada de alterar o comportamento de outros de acordo com padrões e propósitos definidos, com a intenção de produzir um resultado identificado, que pode envolver mecanismos de estabelecimento de padrões, recolhimento de informações e modificação de comportamento". Esse conceito é partilhado por autores que adotam uma visão mais descentralizada da regulação por todos, Hood (2005), destacando-se das visões que centralizam a regulação no Estado. Aqui, por exemplo, a autorregulação e outras formas não estatais estariam incluídas.

Koop e Lodge (Koop; Lodge, 2015) buscaram desenvolver um conceito interdisciplinar com base nos conceitos já trabalhados por outros autores de diversas áreas. Segundo eles, a definição do conceito de regulação é alvo de disputas conceituais. São elas: (i) ser intencional ou não; (ii) ser um tipo de intervenção diferente da tributação e dos subsídios; (iii) poder ser realizada por atores estatais ou não; (iv) ser direcionada somente a atividades econômicas ou não; e (v) equivalência dos atores regulados e regulador.

De forma geral, os autores mencionados entendem que é possível extrair um conceito comum pelo qual a regulação pode ser entendida como:

> a intervenção intencional nas atividades de uma população-alvo, onde a intervenção é tipicamente direta, envolvendo padrões vinculativos, monitoramento e sancionamento, e exercida pelo setor público na atividade econômica dos atores privados (Koop; Lodge, 2015, p. 11).

No campo da cibersegurança, entretanto, é conveniente que se adote um conceito mais descentralizado, tal como proposto por Black e Kingsford Smith (2002), pois, no caso de adotarmos conceitos centralizados no Estado, será difícil explicar os fenômenos sociais que envolvem relações complexas e contemporâneas de governo e tecnologia. Igualmente, é conveniente um conceito que aceite a regulação para outras atividades além das econômicas. Isso porque a regulação pode envolver atividades intergovernamentais, tal como salientam Schultz (1982, p. 6) e Selznick (1985, p. 364). Assim, a regulação deverá envolver tanto a atividade privada como poderá envolver o setor público.

5.40 Resposta a Incidentes de Segurança (*Security Incident Response* – SIR)

A Resposta a Incidentes é um conjunto de procedimentos organizados com o objetivo de coordenar recursos de forma eficiente diante de eventos adversos relacionados à segurança ou integridade do sistema de informações de uma organização. A resposta a incidentes de segurança inclui, também, a formalização de uma equipe especializada (geralmente denominada de *Security Incident Response Team* - SIRT), composta por líderes, membros técnicos, representantes legais e de equipes de relações públicas (Johnson, 2014, p. 18–19).

A resposta a incidentes é um processo que percorre as fases de preparação, detecção, análise, contenção, investigação, erradicação, recuperação e atividades pós-incidente e busca atingir objetivos cruciais para preservar a segurança e a continuidade operacional. A fase inicial, de preparação, resume-se à criação de políticas robustas, procedimentos claros e à formação de uma equipe especializada de Resposta a Incidentes de Segurança (SIRT). Essa equipe, composta por um líder sênior, membros técnicos e do time jurídico, é responsável pela investigação e pela resposta aos incidentes e deverá ter autoridade para tomada de decisões inclusive no âmbito de outras equipes, buscando sempre a mitigação dos riscos e dos danos associados ao incidente detectado (Johnson, 2014, p. 18-19).

Os principais objetivos do processo de resposta a incidentes de segurança são:

1. Limitar o impacto imediato do incidente para clientes e parceiros de negócios, com a proteção dos dados como prioridade central em todas as atividades de segurança;
2. Recuperar-se do incidente, destacando a importância crucial da retomada das operações normais para a estabilidade de qualquer empresa ou agência;
3. Determinar as circunstâncias do incidente por meio de uma avaliação detalhada e análise, proporcionando *insights* valiosos para a compreensão do ocorrido;
4. Descobrir como evitar a exploração adicional da mesma vulnerabilidade, uma prática essencial para mitigar os riscos identificados;
5. Evitar a escalada de incidentes adicionais, enfatizando a contenção como uma etapa vital em qualquer ação de tratamento de incidentes;
6. Avaliar o impacto e os danos, considerando fatores como impacto financeiro, perda de dados, interrupção de processamento, violações de dados e reputação. Avaliações de risco e impacto pós-incidente proporcionam uma abordagem mais centrada nos problemas reais de segurança e operações em uma organização;
7. Atualizar políticas e procedimentos de segurança corporativos conforme necessário, buscando melhorar a postura de segurança e os procedimentos em esforços reais de segurança e conformidade. O desenvolvimento de lições aprendidas a partir dos incidentes oferece às organizações oportunidades tangíveis de aprimoramento em suas práticas de segurança e conformidade.

5.41 Segurança desde a concepção (*Security by design*) e Segurança por padrão (*Security by default*)

A insegurança na tecnologia pode abrir espaço para violações e vulnerabilidades, tais como invasões cibernéticas maliciosas que coloquem em risco informações sobre pessoas ou Estados. Ante a crescente digitalização e, por consequência, aumento da exposição de sistemas a ataques

cibernéticos, é preciso que haja uma mudança sobre os riscos na segurança cibernética, devendo os fornecedores de programas produzir programas seguros desde a sua concepção.

Se antes os fornecedores de tecnologia focavam na correção de vulnerabilidades após o uso do produto ou serviço pelo cliente, deixando a cargo dos consumidores as atualizações (*patches*), hoje não é essa premissa que vigora no mercado. É crucial que os fornecedores desenvolvam produtos de maneira a incorporar segurança, evitando que consumidores tenham de realizar constantemente monitorização, atualizações de rotina e controle de danos nos seus sistemas para mitigar invasões cibernéticas. Os fabricantes são incentivados a assumir a responsabilidade pela melhoria dos resultados de segurança dos seus clientes.

Nesse contexto, a União Europeia apresentou uma proposta de regulamento, o *Cyber Resilience Act*, que enfatiza a importância de se garantir a segurança do produto desde a concepção e durante todo o seu desenvolvimento como forma de garantir a não introdução de produtos vulneráveis no mercado. A exposição de motivos estabelece como objetivo específico, dentre outros: "assegurar que os fabricantes melhorem a segurança dos produtos com elementos digitais desde a fase de concessão e desenvolvimento e ao longo de todo o ciclo de vida" (European Commission, 2022, s.p.).

Nesse sentido, a Agência Americana de Cibersegurança (Cybersecurity and Infrastructure Security Agency - CISA) ao expedir uma recomendação sobre segurança em conjunto com outras Agências e parceiros ("Shifting the Balance of Cybersecurity Risk: Principles and Approaches for Security-by-Design and -Default", *[S.d.]*), explicou 3 tarefas fundamentais para os fabricantes de tecnologia: *i)* exercer o dever de segurança, assumindo essa responsabilidade sem repassá-las aos consumidores; *ii)* adotar a transparência como ferramenta chave para a divulgação dos desafios da segurança sobre um determinado produto; e *iii)* construir estrutura organizacional e liderança para atingir esses objetivos, vez que os executivos seniores são os principais tomadores de decisão para implementar mudanças em uma organização.

Dessa forma, o que esses princípios propõem é que os fabricantes desenvolvam produtos seguros desde a sua concepção, além de prever formas de atualização para que essa segurança seja mantida. A segurança deve ser por *design* e por *default*. A diferença entre os termos reside no fato de que,

na segurança por design, essa deve ocorrer desde a concepção da ideia do produto, não é apenas um recurso técnico, mas faz parte de sua essência. Isso significa que, antes do desenvolvimento dos produtos, os fabricantes devem pensar em estratégias, após a elaboração de avaliação de riscos, que incluam medidas de proteção aos consumidores geradas por atores mal-intencionados. Reconhece-se que essa exigência pode aumentar os custos de desenvolvimento, contudo, os benefícios oferecidos pela segurança dentro do ambiente digital podem diminuir os custos de manutenção e atualizações a longo prazo (Easterly, 2023).

Por outro lado, a segurança por padrão (*default*) é considerada uma espécie de segurança por design. Isto é, produtos são seguros desde o início da venda e do uso pelo consumidor, não havendo, portanto, necessidade de alterações de configuração ou aquisição de outros recursos de segurança com custos adicionais. Isso significa que os produtos estão protegidos de ameaças e vulnerabilidades mais comuns, segundo a avaliação de risco daquele produto, sem que os usuários finais precisem incorporar medidas adicionais. É uma configuração padrão de fábrica ("Shifting the Balance of Cybersecurity Risk: Principles and Approaches for Security-by-Design and -Default", *[S.d.]*).

Dessa forma, a segurança não é uma opção, mas uma regra padrão que deve ser seguida por todos os fabricantes. Um guia que pode auxiliar as empresas e executivos a conhecerem as práticas para um melhor desenvolvimento seguro de software é o *Secure Software Development Framework* (SSDF), conhecido como *National Institute of Standards and Technology's* (NIST) SP 800-218, que estabelece boas práticas para os fabricantes de software.

5.42 Segurança em Nuvem (*Cloud security*)

A computação em nuvem é um modelo que permite acesso virtual e sob demanda à rede para um ambiente compartilhado relacionado a um conjunto de recursos de computação configuráveis (por exemplo, redes, servidores, armazenamento, aplicativos e serviços) (Mell; Grance, 2011). A segurança na nuvem se faz fundamental, ao passo que muitas organizações estão migrando seus sistemas e dados para a nuvem para ganhar escalabili-

dade, eficiência e economia de custos. Essa migração, no entanto, expõe as organizações a novos vetores de ameaças e desafios de segurança em várias camadas, tais como a gestão de acesso, a proteção de dados e o cumprimento das regulações que envolvem os serviços digitais. Os principais aspectos da segurança na nuvem incluem (Verdi; Rothenberg; Pasquini, 2010):

1. Gestão de Identidade e Acesso (IAM): Controle de quem pode acessar o que está na nuvem, geralmente através de autenticação e autorização;
2. Segurança de Dados: Inclui criptografia de dados em repouso e em trânsito, além de medidas para garantir a privacidade e a integridade dos dados;
3. Proteção de Infraestrutura: Inclui a segurança da rede e dos sistemas operacionais hospedados na nuvem, além de proteção contra DDoS e outras ameaças à infraestrutura;
4. Governança, Risco e Conformidade (GRC): Assegura que a organização esteja em conformidade com leis e regulamentos de proteção de dados referentes aos países pertinentes;
5. Resiliência e Recuperação de Desastres: Estratégias e soluções para backup de dados e recuperação rápida de sistemas em caso de falhas ou ataques cibernéticos;
6. Segurança de Aplicativos: Foca na segurança dos aplicativos que são executados na nuvem, incluindo as práticas de desenvolvimento seguro e a avaliação de vulnerabilidades.

Todas essas medidas são direcionadas a trazer mais segurança. É essencial que os fornecedores do serviço em nuvem adotem um conjunto de políticas, controles e tecnologias para proteger dados, aplicativos e serviços de infraestrutura que juntos promovam maior segurança. Para trazer mais segurança, adotam-se modelos de responsabilidade compartilhada, que é um princípio fundamental da segurança na nuvem. Esse modelo define claramente os limites de responsabilidade entre o provedor de serviços de nuvem (*Cloud Service Provider* - CSP) e o cliente, pois direciona a distribuição das obrigações de segurança de maneira que aproveite as competências de ambas as partes.

5.43 Servidor de Nuvem (Servidor de Cloud)

Servidor de nuvem é um servidor virtualizado, que é hospedado, operado e entregue através de uma plataforma de computação em nuvem pela Internet. O servidor opera no nível do hardware e equipamentos de rede e transmissão e a sua oferta pode ser tratada como computação utilitária entregue ao provedor de serviços (CETEC; Tujal, 2010, p. 72). Ele pode ser acessado remotamente, oferecendo os mesmos recursos e capacidades de um servidor físico tradicional, mas com a flexibilidade, escalabilidade e eficiência que a computação em nuvem proporciona. Assim, quando se fala que um recurso de computação está na "nuvem", remete-se à ideia de que ele foi fornecido via Internet e não em um local físico com acesso direto (Sousa, 2009).

Os servidores de nuvem são projetados para fornecer uma ampla gama de serviços, como hospedagem de sites, armazenamento de dados, processamento e execução de aplicações, banco de dados, análise de *big data*, dentre outros. Diferentemente dos servidores físicos, os servidores em nuvem podem ser compartilhados por muitos usuários, sendo gerenciados por um terceiro e não pela organização que está usufruindo o serviço.

Esses servidores podem ser implementados em três tipos de nuvem: *i)* nuvem privada: quando as organizações optam por estabelecer seus próprios servidores, mantendo controle sobre sua gestão e operação; *ii)* nuvem pública: é o meio mais comum e ocorre quando um provedor de terceiros detém e gerencia os servidores que são oferecidos às organizações sob demanda; *iii)* nuvem híbrida: quando é possível encontrar as duas formas antes explicadas, sendo certo que esse modelo oferece às organizações uma versatilidade maior, permitindo-lhes gerenciar dados e aplicações com maior segurança e eficácia, e escalar recursos externamente para atender picos de demanda de forma ágil; e, *iv)* nuvem comunidade: quando ocorre o compartilhamento por diversas entidades, que suportam os mesmos requisitos de segurança, políticas e flexibilidade (Martins, 2010).

Os servidores de nuvem são uma parte fundamental da infraestrutura de TI de muitas organizações, proporcionando benefícios como redução de custos com equipamentos físicos, maior flexibilidade e escalabilidade, melhor continuidade de negócios e recuperação de desastres e acesso facilitado a novas tecnologias. No entanto, trazem desafios, pois exigem uma estratégia de segurança robusta, que inclua práticas como criptografia de

dados, autenticação multifatorial, políticas de controle de acesso baseadas no mínimo privilégio, auditorias regulares e a implementação de soluções de segurança específicas para ambientes de nuvem. Além disso, a educação contínua e a conscientização sobre segurança da informação para todos os usuários que interagem com recursos de nuvem são fundamentais para mitigar os riscos.

5.44 Soberania Digital

Soberania Digital refere-se à capacidade de uma dada entidade para entender o funcionamento de tecnologias digitais, conseguir desenvolvê-las e regulá-las efetivamente, conseguindo, portanto, exercer agência, autodeterminação e controle sobre tecnologias digitais (Belli, 2021b; Belli *et al.*, 2023b; Belli; Jiang, 2024; Floridi, 2020). Embora a soberania digital tenha atraído uma atenção crescente tanto dos decisores políticos como dos acadêmicos, este conceito continua a ser vago, fluido e multifacetado, não tendo ainda encontrado uma definição universalmente aceita.

É importante destacar que, dependendo da política ou iniciativa em jogo, o "soberano digital" pode ser um indivíduo, uma comunidade, uma corporação, um estado ou um grupo de estados, que é capaz de recuperar a sua capacidade de controlar e assegurar as suas infraestruturas digitais enquanto determina o seu desenvolvimento (digital).

A soberania digital deve, portanto, ser vista como a capacidade de uma nação, de um grupo ou de uma pessoa – física ou jurídica – de entender o funcionamento da tecnologia digital e ter um controle efetivo sobre as infraestruturas e dados digitais (Belli; Jiang, 2024). Porém, dados e infraestruturas não são os únicos itens a serem considerados para se tornar soberanos digitalmente, sendo necessária uma abordagem multicamadas, capaz de entender a relevância e a interconexão de *i)* dados; *ii) software*; *iii) hardware*; *iv)* educação e treinamento; e *v)* governança.

5.45 Superfície de Ataque (*Attack Surface*)

A Superfície de Ataque de um sistema compreende o conjunto de vulnerabilidades ou pontos de entrada a partir dos quais se pode empreender

um ataque ao sistema. A superfície de ataque, portanto, configura a extremidade externa, o perímetro do sistema, no qual um atacante pode tentar obter acesso não autorizado, exercer influência ou extrair dados do sistema.

O conceito pode assumir um escopo mais restrito, como apresentado por Manadhata e Wing:

> A superfície de ataque de um sistema é o subconjunto de seus recursos que um invasor pode usar para atacar o sistema. Um invasor pode usar os pontos de entrada e de saída de um sistema, canais e itens de dados não confiáveis para enviar (receber) dados para (de) o sistema para atacar o sistema. Portanto, o conjunto de pontos de entrada e saída, o conjunto de canais e o conjunto de itens de dados não confiáveis são o subconjunto relevante de recursos que fazem parte da superfície de ataque (Manadhata; Wing, 2011, p. 375, tradução nossa).

No entanto, é comum que o conceito não se limite a componentes de *software*, incluindo elementos humanos e não humanos do sistema, sua rede, *hardware* e ambiente físico e virtual. Por exemplo, o guia "*Developing Cyber-Resilient Systems: A systems security engineering approach*" enumera uma série de componentes que podem configurar pontos em uma superfície de ataque:

> Finalmente, podem ser identificadas as superfícies de ataque às quais as soluções de resiliência cibernética podem ser aplicadas. As informações sobre o contexto programático, arquitetônico e operacional determinam quais superfícies de ataque estão dentro do escopo de potenciais soluções de resiliência cibernética. Por exemplo, se o contexto programático determina que os sistemas de suporte estejam no escopo, esses sistemas são uma superfície de ataque, além das interfaces e procedimentos pelos quais as atualizações são feitas no sistema em questão; se o sistema é um serviço corporativo (contexto arquitetônico), suas interfaces com outros serviços dos quais ele depende, bem como com aplicativos que o utilizam, também são superfícies de ataque; se o sistema tem usuários (contexto operacional), a comunidade de usuários é uma superfície de ataque (Ross *et al.*, 2021, p. 41, tradução nossa).

Ambas as abordagens trazem insumos cruciais para se pensar uma estratégia de cibersegurança. A mensuração proposta por Manadhata e Wing revela que a superfície de ataque de um sistema pode ser ampla mesmo que haja poucos pontos de entrada e/ou saída, pois considera o caráter crítico de um recurso para o funcionamento do sistema como um todo (Manadhata; Wing, 2011). Assim, um recurso com alto privilégio de acesso (e.g., *root privilege*) contribuirá mais para a formação da superfície de ataque do que um com privilégio menor. Em paralelo, a definição proposta por Ross *et al.* e encontrada em outros documentos de referência do NIST (e.g., Security and Privacy Controls for Information Systems and Organizations (National Institute of Standards and Technology; Joint Task Force Interagency Working Group, 2020), com uma visão mais ampla e contextual, ressalta a importância de se levar em consideração o ambiente físico e virtual em que o sistema está inserido, incorporando mais componentes a partir dos quais vulnerabilidades poderiam ser exploradas.

Alguns elementos que ampliam a superfície de ataque são o uso de dispositivos "inteligentes" que se conectam à Internet (US G.A.O., 2018, p. 13), utilização de *software* desatualizado e o uso de senhas fracas ou senhas padrão (NordVPN, *[S.d.]*). Estratégias de mitigação da superfície de ataque incluem a atualização frequente de sistemas e *softwares*, implementação de políticas de autenticação robustas (incluindo autenticação de múltiplos fatores), concessão de privilégios de acesso com base na estrita necessidade de acesso, segmentação de redes para evitar movimentação lateral em sistemas, uso de criptografia e VPNs e a eliminação de sistemas desnecessários.

5.46 Teste de Penetração (*Pentest*)

Umas das principais atividades realizadas no escopo de programas de gestão da segurança da informação são as auditorias para averiguação de vulnerabilidade de processos, sistemas e redes. Essas análises contemplam tanto aspectos organizacionais ou administrativos quanto técnicos, sendo esses últimos operados também por meio de ferramentas e modelos de validação de segurança.

Nesse contexto, elenca-se o *pentest*, *penetration test* ou, no vernáculo, "teste de penetração". Trata-se de processo de simulação de ataques dire-

cionados a potenciais vulnerabilidades. Nestes, haverá a ação de um agente habilidoso em busca de acessos privilegiados (Smyth, 2024). Pela identificação e exploração dessas lacunas de segurança, determina-se também qual o potencial impacto para a organização caso a ameaça seja bem-sucedida (Menezes; Cardoso; Rocha, 2015). Portanto, por lacunas entende-se falhas e erros na arquitetura de ambientes digitais, sistemas e redes.

Há, entretanto, uma distinção relevante entre os testes de vulnerabilidade (*vulnerability scanning*) propriamente ditos e o *pentest*. Enquanto os primeiros somente procuram por vulnerabilidades já conhecidas nos seus sistemas – geralmente realizados de forma automatizada - e reportam as possíveis exposições, os testes de penetração são efetuados manualmente por profissionais da segurança da informação com o objetivo de explorar as fraquezas da arquitetura da rede de tecnologia da informação, permitindo a determinação dos possíveis níveis de obtenção dos acessos não autorizados aos ativos da organização (Smyth, 2024).

Esses testes são relevantes na medida em que se experiencia um aumento exponencial nos ataques cibernéticos, capazes de expor dados confidenciais e/ou pessoais, tornar sistemas indisponíveis, gerar perdas financeiras, entre outros (TecMundo, 2025). Por meio dessa ação, mapeamento de riscos é realizado e as respectivas medidas de mitigação poderão ser estudadas e posteriormente implementadas.

Como exemplo das técnicas e serviços utilizados para essas varreduras de vulnerabilidades, citam-se *i)* os *portscan* (varredura de portas), que permite identificar os serviços que estão sendo executados ou os que estão em "estado de escuta"; *ii)* os *sniffers* (farejadores), programas que conseguem capturar todo o tráfego que passa em um segmento da rede; *iii)* os mapeamentos de redes; e *iv)* a engenharia social (Casagrande; Boas; Aquino, 2022).

5.47 Tríade da CIA: Confidencialidade, Integridade, Disponibilidade (*CIA triad: Confidentiality, Integrity, Availability*)

A definição de segurança da informação está atrelada à tríade da CIA (do inglês, confidencialidade, integridade e disponibilidade) desde

os anos 1960. Hodiernamente, entretanto, conforme a complexidade dos ambientes organizacionais – plurais, hiper e interconectados –, a menção a outras propriedades se impõe. Parafraseando Ayrton Jorge, cita-se ilustrativamente a inclusão por alguns autores de um conjunto amplo de possíveis acontecimentos: "danos acidentais ou intencionais, destruição, roubo, modificação não intencional ou não autorizada, ou outro uso indevido de ameaças humanas ou não humanas" (Jorge, 2021, p. 8), que, por conseguinte, demandam a garantia de proteções adicionais. Assim, é possível acrescer como propriedades da segurança da informação a autenticidade, a resiliência e o não repúdio. Ante o exposto, conceituam-se na sequência as respectivas propriedades.

Tradicionalmente, considerada um dos pilares incontroversos da segurança da informação, a confidencialidade remete à ideia central de que as informações consideradas como tal – confidenciais – não devem ser disponibilizadas ou divulgadas a indivíduos, entidades ou processos não autorizados (International Organization for Standardization, 2012, p. 2).

A classificação da informação conforme o seu respectivo grau ou nível de criticidade (capacidade de gerar danos) para a organização que a detém, seja ela entidade pública ou privada, é uma ação necessária (princípio da hierarquização). Em outras palavras, sobrevirá priorização de ação e reforço e/ou combinação de controles de segurança mais ou menos complexos conforme haja maior possibilidade de extensão dos danos face à exposição da informação. É, portanto, a partir da seleção desses critérios que se estabelece quais controles – como acessos privilegiados, logins, senhas complexas, criptografia, vedação de compartilhamentos, entre outros – serão implementados em prol da segurança e da garantia adicional.

Adicional ou alternativamente, acordos bilaterais de confidencialidade e sigilo são igualmente recursos recomendáveis, na medida em que antecipam as consequências da infringência das regras internas correlatas à segurança da informação.

A integridade, outro conceito da tríade, conforme a ISO/IECF 27000:2012 (International Organization for Standardization, 2012, p. 5), significa a propriedade de "precisão e completude" da informação. Em outras palavras, trata-se da necessidade de manutenção dos conteúdos informativos em sua integralidade e, portanto, sem adulteração, afetação ou corrompimento em relação ao formato original por pessoas não autoriza-

das. A proteção desta propriedade está atrelada à "capacidade de prevenir, recuperar e reverter alterações não autorizadas ou acidentais aos dados" (Jorge, 2021, p. 11).

A garantia da integridade permite que a informação seja confiável e autêntica. Os dados mantidos fielmente com as suas características originais, dos quais o receptor obtém acesso exato àquilo transmitido pelo emissor, serão considerados íntegros. Tal propriedade deve ser observada tanto no armazenamento quanto em outros tratamentos (processamentos) das informações, como no seu compartilhamento e utilização para finalidades plurais. Idealmente, a temática deve constar em protocolos de segurança. Outrossim, faz-se cogente a implementação de controles de segurança que não somente protejam diretamente a integridade (por acessos privilegiados e autenticação, criptografia, assinatura e certificação digital, bloqueios de edição, *hashing* (A função Hash converte matematicamente (por algoritmo) dados de tamanhos variados (arquivos) em um código de tamanho menor e fixo, formado por letras e números. Trata-se de uma função irreversível e que garante a integridade, na medida em que o material se torna "único", tal qual uma "impressão digital". Caso haja alguma alteração naqueles dados, por exemplo, com a instalação de um software malicioso (*malware*), a ação será facilmente identificada. Como exemplo, cita-se a assinatura digital. Pisa, 2012), sistemas de controle de versões e de detecção de invasão, entre outros) como, também, viabilizem o registro das atividades realizadas nos arquivos (como pelo registro de *logs)* Dentre os seus tipos, citam-se os logs de eventos, do sistema, de acesso, do servidor, de alterações, de disponibilidade, de recursos, de ameaças, dentre outros "O que são arquivos de log?", *[S.d.]*; Os arquivos de log representam um registro histórico de ocorrências num sistema computacional, são gerados por software e são organizados de forma estruturada (Ruiz, 2022) e a possibilidade de respectiva reversão pelo usuário administrador.

O último elemento da CIA, a disponibilidade de dados, significa a propriedade de estar acessível e de ser passível de utilização e manipulação, em tempo útil, por aquelas pessoas que obtiverem autorização (Cherdantseva; Hilton, 2013). Perante esse conceito, é evidente que a disponibilidade está conectada às definições dos acessos privilegiados e, portanto, à eleição dos permissionamentos individuais ou coletivos de acesso a arquivos e documentos. Algumas informações poderão estar disponíveis amplamen-

te (para todos), para determinadas áreas ou grupos de pessoas (gestão ou áreas das quais somente os profissionais atuantes diretamente com determinados dados poderão ver e, eventualmente, intervir e processá-los).

Nesse sentido, quando se tratar de conteúdos físicos (como os documentos impressos e os dispositivos de fixos ou móveis), convém que sejam classificados conforme a sensibilidade (ou complexidade) e, a partir disso, avalie-se a necessidade de alocá-los em ambientes de maior ou menor circulação de pessoas, com ou sem chaves (determinando-se aqueles que eventualmente obterão as suas cópias), com ou sem monitoramento por câmeras de vigilância, entre outros. Similarmente, quando forem materiais dispostos no ambiente digital, controles de segurança com as mesmas finalidades deverão ser implementados (eventualmente, com maior rigor, haja vista a ubiquidade e vulnerabilidades do ciberespaço).

A autenticidade, embora nem sempre listada dentre os elementos essenciais da segurança da informação, merece igual atenção na respectiva gestão. Trata-se de uma propriedade que "garante que a informação é proveniente da fonte anunciada, ou seja, não pode sofrer modificações ao longo do processo quanto a sua origem" (Freund; Sembay; Macedo, 2019). É um elemento que influencia diretamente o valor da informação e está relacionado à integridade desta, na medida em que impede distorções ou falsificações (Santana, 2021). Quando autêntica e, portanto, preservados os seus elementos formais de quando gerada e/ou transmitida, a informação é aquilo que deveria ser desde o princípio (genuína) e, consequentemente, é confiável (fidedigna) (Freitas, 2012). Como exemplos citam-se os logins e as senhas ou as assinaturas digitais.

Embora não tradicionalmente citada como pilar da segurança da informação, atualmente a resiliência deve ser elevada como tal. Trata-se da capacidade das organizações se adaptarem às condições mutáveis em razão do risco ao qual estão expostas e de se prepararem, resistirem e se recuperarem rapidamente de ameaças e eventuais incidentes de segurança. (National Initiative for Cybersecurity Careers and Studies (NICCS), 2025). Por óbvio, não se almeja eliminar os riscos, o que é impossível. Para obter o status de "resiliente", deve-se gerenciar esses riscos e ameaças organizando-se de forma proativa, empreendendo esforços para detectar, proteger e responder a eles. Reconhecendo as próprias vulnerabilidades, cabe às organizações implementar estratégias robustas de segurança da informação e aumentar a

conscientização interna de modo que as equipes e os processos estejam todos adequados às suas políticas e procedimentos padrão (Pinilla, 2015).

Por fim, enfeixa-se com o não repúdio, relativo à garantia de que qualquer pessoa física ou jurídica negue alguma ação específica relacionada a dados (Pinilla, 2015). Como exemplo, cita-se a impossibilidade de partes contratuais ou de uma comunicação negarem a autenticidade de uma assinatura, a efetiva entrega de uma mensagem ou a celebração de alguma transação (National Initiative for Cybersecurity Careers and Studies (NICCS), 2025). Dentre os recursos dispostos para essa finalidade, mencionam-se a criptografia, assinatura digital, *hash*, mecanismos de registro e cadeia de custódia. Conquanto seja fundamental cercar-se de novas tecnologias e melhores técnicas do mercado, reitera-se que a amálgama de todas essas ações explicitadas é um programa contínuo de formação e conscientização adequado às especificidades não somente das áreas de atuação, mas sobretudo da diversidade dos indivíduos envolvidos direta ou indiretamente na operação.

5.48 Vulnerabilidade e ataque de Dia Zero

Uma vulnerabilidade de Dia Zero em cibersegurança refere-se a uma falha de *hardware*, *firmware* ou *software* ainda não descoberta pelos seus desenvolvedores ou pela comunidade em geral. O "dia zero" é o momento em que a vulnerabilidade é identificada inicialmente. A partir desta vulnerabilidade ainda não corrigida, atacantes podem promover "ataques de dia zero" (sendo o "dia um" o momento em que uma correção para a vulnerabilidade é disponibilizada).

Estratégias de exploração dessas vulnerabilidades de dia zero são frequentemente utilizadas ou compartilhadas por atacantes antes que o desenvolvedor de *software* tome conhecimento da vulnerabilidade, tornando a defesa preventiva desafiadora.

Para se prevenir de ataques de dia zero, algumas medidas incluem: atualizar *softwares* regularmente para abordar vulnerabilidades conhecidas; acompanhar informações sobre possíveis vulnerabilidades por meio de bancos de dados de vulnerabilidade; cuidar para evitar ataques de *phishing*, comumente usados para entregar ataques de dia zero; monitorar

anomalias do sistema; segmentação da rede, evitando o espalhamento dos efeitos de um ataque deste tipo; e uso de ferramentas de mitigação de ataques (ENISA, *[S.d.]*).

Alguns exemplos célebres de ataques de dia zero foram o vírus Stuxnet, em 2010, que explorava quatro vulnerabilidades de dia zero do Windows e chegou a provocar prejuízos à infraestrutura nuclear do Irã (Naraine, 2010) e a vulnerabilidade de dia zero que, em 2014, permitiu um ataque aos sistemas da Sony, culminando no vazamento de amplos conjuntos de informações (Hesseldahl, 2015; NordVPN, *[S.d.]*).

5.49 *Zero Trust*

Zero Trust é um paradigma dentro da estruturação da segurança cibernética de organizações em que se parte do princípio de que a confiança deve ser sempre explícita, nunca implícita. Assim, uma arquitetura *zero trust* confirma contínua e reiteradamente essa confiança, incluindo verificações de identidades, credenciais, permissões de acesso, operações, *endpoints*, servidores e a infraestrutura de conexão, implementando o princípio de necessidade de acesso (*need to access*) como diretriz fundamental. Rose *et al.* proveem a seguinte definição do conceito:

> O Zero trust (ZT) fornece uma coleção de conceitos e ideias projetados para minimizar a incerteza na aplicação de decisões de acesso precisas e com privilégios mínimos por solicitação em sistemas de informação e serviços em face de uma rede vista como comprometida. A arquitetura de confiança zero (ZTA) é um plano de segurança cibernética da empresa que utiliza conceitos de confiança zero e engloba relacionamentos de componentes, planejamento de fluxo de trabalho e políticas de acesso. Portanto, um empreendimento de confiança zero compreende a infraestrutura de rede (física e virtual) e as políticas operacionais que estão em vigor para uma organização como produto de um plano de arquitetura de confiança zero (Rose *et al.*, 2020, p. 4, tradução nossa).

Uma arquitetura de confiança zero verifica permissões para cada operação, mesmo aquelas no interior de uma rede. Essa abordagem parte da presunção de uma brecha na segurança, aplicando o nível mais severo

de verificação de permissões e identidades a cada operação em paralelo a sistemas de resposta rápida a incidentes identificados e segmentação de redes e criptografia de dados para mitigar o efeito destes potenciais incidentes (Microsoft Security, *[S.d.]*).

Uma referência prática importante em relação à implementação de arquitetura *zero trust* é o modelo de maturidade de confiança zero construído pela Agência de Cibersegurança e Infraestrutura dos Estados Unidos (CISA) e adotada em janeiro de 2022 para órgãos do governo federal estadunidense por meio da Estratégia Federal *Zero Trust* publicada em memorando em resposta à Ordem Executiva federal n. 14028) (CISA Cybersecurity Division, 2023, p. s.p., tradução nossa; "Moving the U.S. Government Toward Zero Trust Cybersecurity Principles", *[S.d.]*). O modelo da CISA se baseia em cinco pilares, quais sejam ("Moving the U.S. Government Toward Zero Trust Cybersecurity Principles", *[S.d.]*):

Identidade: a equipe da agência usa identidades gerenciadas pela empresa para acessar os aplicativos que usa em seu trabalho. O MFA (*Multi Factor Authentication*) resistente a *phishing* protege esse pessoal de ataques on-line sofisticados.

Dispositivos: o Governo Federal tem um inventário completo de todos os dispositivos que opera e autoriza para uso do Governo, podendo prevenir, detectar e responder a incidentes nesses dispositivos.

Redes: as agências criptografam todas as solicitações DNS e tráfego HTTP em seu ambiente e começam a executar um plano para dividir seus perímetros em ambientes isolados.

Aplicativos e cargas de trabalho: As agências tratam todos os aplicativos como conectados à Internet, submetem rotineiramente seus aplicativos a testes empíricos rigorosos e recebem relatórios de vulnerabilidades externas.

Dados: as agências estão em um caminho claro e compartilhado para implantar proteções que fazem uso de categorização completa de dados. As agências estão aproveitando os serviços de segurança em nuvem para monitorar o acesso a seus dados confidenciais e implementaram o registro em log e o compartilhamento de informações em toda a empresa.

O conceito de confiança zero, como paradigma de organização de sistemas, já se encontra, portanto, traduzido em abordagens pragmáticas e serviços de segurança oferecidos a organizações, conforme explicitado pelo conjunto de ações de confiança zero extraído do modelo de maturi-

dade da CISA, que inclui, entre outras, validação contínua de identidade, rastreio de ativos físicos e virtuais, criptografia do tráfego em redes, utilização de ambientes de produção e testagem *ad hoc* e realização contínua de inventário de dados (CISA Cybersecurity Division, 2023, p. 10).

5.50 Zona Cinzenta (Gray Zone)

O conceito de *Gray Zone* (Zona Cinzenta) emana da incerteza que permeia o ciberespaço. Nesta, a complexidade das redes, bem como uma arquitetura que favorece o anonimato, suscitam uma nebulosidade acerca de incidentes cibernéticos. Em vista desta nebulosidade, a definição e imposição de limiares, assim como distinções acerca de permissões, comportamentos e atribuições, contribuem para um ambiente no qual imposições de normas não ocorrem de forma tão evidente, ou mesmo intuitiva, como acontece nos demais domínios naturais. Este ambiente passa a ser, portanto, uma zona cinzenta na qual as noções de guerra e paz em si, tal como práticas ofensivas e defensivas, são desafiadas ao passo que uma miríade de atores recorre ao ciberespaço para perseguirem seus interesses (Wirtz, 2017).

Essa zona cinzenta é endêmica do que Libicki (2012) chama de "não obviedade dos conflitos na atualidade". Dada a onipresença e dependência da sociedade hodierna para com o ciberespaço, estes conflitos invariavelmente transbordam para além do âmbito militar e afetam nações, empresas e indivíduos, abarcando dimensões econômicas, diplomáticas e/ou políticas. Os incidentes cibernéticos neste cenário, segundo Libicki, desde sua atribuição ao fato em si, são marcados pela ambiguidade e, consequentemente, discutíveis. Nesta condição, a não obviedade mina esforços nacionais ou privados de atribuírem e responsabilizarem determinados atores por suas ações. Diante deste contexto ambíguo, Hal Brands propõe a seguinte definição:

> O conflito na zona cinzenta é melhor compreendido como uma atividade coerciva e agressiva por natureza, mas que é deliberadamente projetada para permanecer abaixo do limiar de conflito militar convencional e guerra interestadual aberta. Abordagens na zona cinzenta são predominantemente características de potências revisionistas — aquelas que buscam modificar algum aspecto do

> ambiente internacional existente — e o objetivo é obter ganhos, sejam territoriais ou de outra natureza, normalmente associados à vitória em guerra. No entanto, as abordagens na zona cinzenta visam alcançar esses ganhos sem escalar para uma guerra aberta, sem ultrapassar as linhas vermelhas estabelecidas e, assim, sem expor o praticante às penalidades e riscos que tal escalada poderia trazer (Brands, 2016, s.p., tradução nossa).

A definição de Brands é complementada pela perspectiva do Coronel norte-americano Gary P. Corn:

> Alternativamente descritos como desafios na zona cinzenta ou conflitos na zona cinzenta, essas atividades são mais precisamente compreendidas como ações que são coercitivas e agressivas por natureza e ultrapassam a competição geopolítica normal do dia a dia em tempos de paz […]. Embora essas atividades não estejam limitadas a nenhum domínio ou modalidade específica, o ciberespaço oferece um terreno fértil para confrontos na zona cinzenta (Corn, 2017, p. 2, tradução nossa).

Trata-se, portanto, da exploração da incerteza e da nebulosidade em ações deliberadamente calibradas abaixo do limiar do conflito.

Anexo A – Uma proposta de Protocolo de Comunicação Intersetorial

Considerando a importância crescente da cibersegurança no funcionamento das agências governamentais e privadas, e a necessidade de estabelecer canais de comunicação eficientes, confiáveis e seguros entre os responsáveis pela segurança da informação, incluindo o Encarregado da Cibersegurança, este protocolo tem por objetivo definir as modalidades de comunicação, estabelecer pontos de contato e suplentes, e definir quais informações devem ser compartilhadas e como, visando a uma resposta rápida, efetiva e de confiança em caso de incidentes cibernéticos, bem como a coordenação e comunicação periódica entre os responsáveis, com o fim de fortalecer relações de confiança.

1. Modalidades de Comunicação

1.1. As comunicações serão realizadas através de canais seguros, preferencialmente utilizando ferramentas de mensagens criptografadas, redes privadas virtuais (VPNs) e/ou correio eletrônico certificado.

1.2. Para comunicações urgentes, serão utilizados telefones celulares seguros e/ou linhas telefônicas dedicadas e seguras.

1.3. Reuniões periódicas serão realizadas de forma presencial ou por videoconferência utilizando plataformas seguras.

2. Pontos de Contato e Suplentes

2.1. Cada agência designará um Encarregado da Cibersegurança como ponto de contato principal, responsável pela coordenação das atividades de cibersegurança e comunicação.

2.2. Cada Encarregado da Cibersegurança indicará um suplente que assumirá suas funções em caso de indisponibilidade.

2.3. Os contatos, incluindo nomes, cargos, números de telefone e endereços de e-mail, serão compartilhados entre as agências participantes.

3. Informações a Serem Compartilhadas

3.1. As agências compartilharão informações sobre incidentes cibernéticos, incluindo naturezas, impactos, respostas e medidas preventivas adotadas.

3.2. Serão compartilhados boas práticas, análises de vulnerabilidades, relatórios de inteligência de ameaças e alertas de segurança cibernética.

3.3. As agências poderão solicitar assistência técnica e compartilhar recursos em caso de incidentes.

4. Procedimentos de Comunicação

4.1. Em caso de incidente cibernético, o Encarregado da Cibersegurança da agência afetada notificará imediatamente os Encarregados da Cibersegurança das demais agências através dos canais definidos no item 1.

4.2. As notificações de incidentes incluirão a natureza do incidente, o impacto potencial, as medidas já tomadas e a assistência necessária.

4.3. As reuniões periódicas serão agendadas com antecedência e terão como objetivo principal a troca de informações, a discussão de estratégias conjuntas e o fortalecimento das relações de confiança.

5. Confidencialidade e Segurança

5.1. Todas as informações compartilhadas serão tratadas como confidenciais e sujeitas a acordos de não divulgação.

5.2. As agências adotarão medidas para garantir a segurança das informações compartilhadas, incluindo o uso de criptografia e controles de acesso.

6. Revisão e Atualização

6.1. Este protocolo será revisado anualmente ou sempre que necessário, de acordo com as mudanças nas ameaças cibernéticas e nos requisitos regulatórios.

6.2. As alterações serão aprovadas por consenso entre os Encarregados da Cibersegurança das agências participantes.

Anexo B – Regulação ANTT – Obrigações em cibersegurança e segurança da informação para regulados

Este anexo compila alguns artigos que poderiam ser considerados como obrigações fragmentárias de uma política de segurança da informação para os atores regulados pela ANTT. As normas do estoque regulatório foram separadas por tema regulado, e trazidos somente os artigos que permitam inferir algumas dessas obrigações. Embora não configurem normas de cibersegurança de forma sistemática, entendemos que o conhecimento aqui pode servir como ponto de partida para a elaboração de uma Política Geral que se aplique aos regulados no futuro. A investigação deste estoque regulatório ocorreu em outubro de 2024.

Regulado	Norma	Artigos
Gestão de RODOVIAS	RESOLUÇÃO Nº 6.000, DE 1º DE DEZEMBRO DE 2022	Art. 175 Art. 176 Art. 177 Art. 178 Art. 180 Art. 184
	RESOLUÇÃO Nº 6.032, DE 21 DE DEZEMBRO DE 2023	Art. 59 Art. 117 Art. 120
TRANSPORTE DE CARGAS – Ferroviário	RESOLUÇÃO Nº 5.862, DE 17 DE DEZEMBRO DE 2019	Art. 16 Art. 17
	RESOLUÇÃO Nº 6.024, DE 3 DE AGOSTO DE 2023	Art. 12 Art. 14 Art. 13
	RESOLUÇÃO Nº 5.379, DE 5 DE JULHO DE 2017	Art. 30 Art. 32 Art. 33

Regulado	Norma	Artigos
TRANSPORTE DE PASSAGEIROS – Rodoviário	RESOLUÇÃO N° 4.499, DE 28 DE NOVEMBRO DE 2014	Art. 3° Art. 12 ANEXO, item 4
	PORTARIA N° 2, DE 11 DE ABRIL DE 2024	Art. 1°
TRANSPORTE DE PASSAGEIROS – Ferroviário	RESOLUÇÃO N° 5.999, DE 3 DE NOVEMBRO DE 2022	Art. 11
	RESOLUÇÃO N° 3.535, DE 10 DE JUNHO DE 2010	Art. 13 Art. 15
	RESOLUÇÃO N° 5.902, DE 21 DE JULHO DE 2020	Art. 1° Art. 4° Art. 5°

Referências bibliográficas

2023 Data Breach Investigations Report. Disponível em: https://www.verizon.com/business/resources/reports/dbir/. Acesso em: 19 fev. 2024.

AGU. **Contratos de encomenda tecnológica: Noções introdutórias**. Disponível em: https://www.gov.br/agu/pt-br/composicao/cgu/cgu/modelos/cti/consulta/encomenda-tecnologica-introducao-versao-2021-3.pdf. Acesso em: 23 fev. 2024.

AMORIM, Celso. Segurança Internacional: novos desafios para o Brasil. **Contexto Internacional**, v. 35, p. 287–311, jun. 2013.

ANATEL. **Anatel - Resolução nº 740, de 21 de dezembro de 2020**. Disponível em: https://informacoes.anatel.gov.br/legislacao/resolucoes/2020/1497-resolucao-740. Acesso em: 16 maio 2024.

ANATEL. **Anatel - Resolução nº 767, de 7 de agosto de 2024 (Atualiza a nº740 de 2020)**. Disponível em: https://informacoes.anatel.gov.br/legislacao/component/content/article/168-resolucoes/2024/1965-resolucao-767. Acesso em: 1 out. 2024.

ANEEL. **RESOLUÇÃO NORMATIVA ANEEL Nº 964, DE 14 DE DEZEMBRO DE 2021 - DOU - Imprensa Nacional**. Disponível em: https://www.in.gov.br/web/dou. Acesso em: 16 maio 2024.

ANPD. **Comunicação de incidente de segurança**. Disponível em: https://www.gov.br/anpd/pt-br/canais_atendimento/agente-de-tratamento/comunicado-de-incidente-de-seguranca-cis/comunicacao-de-incidentes-de-seguranca. Acesso em: 29 jan. 2024a.

ANPD. RESOLUÇÃO 15. RESOLUÇÃO CD/ANPD Nº 15. Aprova o Regulamento de Comunicação de Incidente de Segurança. 24 abr. 2024 b.

ANPD, (Autoridade Nacional de Proteção de Dados). **SEGURANÇA DA INFORMAÇÃO PARA AGENTES DE TRATAMENTO DE PEQUENO**

PORTE. Brasil, 2021. Disponível em: https://www.gov.br/anpd/pt-br/centrais-de-conteudo/materiais-educativos-e-publicacoes/guia-vf.pdf.

ANTONOPOULOS, Nick; GILLAM, Lee (ORGS.). **Cloud Computing: Principles, Systems and Applications**. Cham: Springer International Publishing, 2017.

ARAGÃO, Alexandre Santos de. **Agências reguladoras e a evolução do direito administrativo econômico**. 3. ed. Rio de Janeiro: *[S.n.]*.

ARDISSONE, Carlos Maurício. **Propriedade intelectual e relações internacionais nos governos FHC e Lula**. Paraná: Editora Appris, 2017.

ASHRAF, Cameran. Defining cyberwar: towards a definitional framework. **Defense & Security Analysis**, v. 37, n. 3, p. 274–294, 3 jul. 2021.

ASSIMAKOPOULOS, Dimitris *et al*. Oxford and Grenoble: multiple anchors, strong dyadic relationships and national policy in fostering cluster architectures. **Regional Studies**, v. 56, n. 10, p. 1618-1632, 3 out. 2022.

ATWELL, Jason P. Re-Framing the Problem: Applying Strategic Thinking to the Cyber Threat Environment. **SAIS Review of International Affairs**, v. 41, n. 2, p. 35–49, 2021.

AYERS, CYNTHIA E. **Rethinking Sovereignty in the Context of Cyberspace: The Cyber Sovereignty Workshop Series**. Disponível em: https://apps.dtic.mil/sti/citations/AD1124691. Acesso em: 11 mar. 2025.

BACEN. **Resolução CMN nº 4.893 de 26/2/2021**, 26 fev. 2021. Disponível em: https://www.bcb.gov.br/estabilidadefinanceira/exibenormativo?tipo=Resolu%C3%A7%C3%A3o%20CMN&numero=4893. Acesso em: 27 mar. 2025

BALDWIN, Robert; CAVE, Martin; LODGE, Martin. **Understanding regulation: theory, strategy, and practice**. 2nd ed. New York: Oxford University Press, 2012.

BANK FOR INTERNATIONAL SETTLEMENTS. Guidance on cyber resilience for financial market infrastructures. 29 jun. 2016.

BARRETO, Andréa. **Cyber Guardian Exercise Strengthens Cyber Defense Partnerships**. **Diálogo Américas**, 19 out. 2022. Disponível em: https://

dialogo-americas.com/articles/cyber-guardian-exercise-strengthens-cyber-defense-partnerships/. Acesso em: 20 maio 2024

BARRETT, Daniel J.; SILVERMAN, Richard E.; BYRNES, Robert G. **SSH, the secure shell: the definitive guide**. 2nd ed. Sebastopol, CA: O'Reilly, 2005.

BARRINHA, André; RENARD, Thomas. Cyber-diplomacy: the making of an international society in the digital age. **Global Affairs**, v. 3, n. 4–5, p. 353–364, 20 out. 2017.

BBC NEWS. **PL das fake news: 3 pontos para entender a disputa entre governo e Google**. Disponível em: https://www.bbc.com/portuguese/articles/crg2jx75y40o. Acesso em: 31 ago. 2024.

BBC NEWS BRASIL. **Ataque hacker que afetou o Pix: suspeito é preso; o que se sabe**. Disponível em: https://www.bbc.com/portuguese/articles/cx2475peey2o. Acesso em: 14 ago. 2025.

BECKER, Gary S. A Theory of Competition Among Pressure Groups for Political Influence. **The Quarterly Journal of Economics**, v. 98, n. 3, p. 371, ago. 1983.

BELLI, Luca. **De la gouvernance à la régulation de l'internet**. *[S.l.: S.n.]*.

BELLI, Luca. **De la gouvernance à la régulation de l'internet**. Boulogne-Billancourt: Berger-Levrault, 2016.

BELLI, Luca. **Network self-determination: When building the Internet becomes a right**. **IETF Journal**, 28 mar. 2018. Disponível em: https://wayback.archive-it.org/20635/20230207113525/https://www.ietfjournal.org/network-self-determination-when-building-the-internet-becomes-a-right/. Acesso em: 7 jun. 2023.

BELLI, Luca *et al.* **Governança e regulações da Internet na América Latina: análise sobre infraestrutura, privacidade, cibersegurança e evoluções tecnológicas em homenagem aos dez anos da South School on Internet Governance**. *[S.l.]*: FGV Direito Rio, 2018.

BELLI, Luca (ORG.). **CyberBRICS: Cybersecurity Regulations in the BRICS Countries**. Cham: Springer International Publishing, 2021a.

BELLI, Luca. Cybersecurity Policymaking in the BRICS Countries: From Addressing National Priorities to Seeking International Cooperation. **The African Journal of Information and Communication**, v. 28, p. 1–14, 2021b.

BELLI, Luca *et al.* **L' État digital: numérisation de l'administration publique et administration publique du numérique / sous la direction de Luca Belli et Gilles J. Guglielmi**. *[S.l.]*: Berger-Levrault, 2022.

BELLI, Luca. **O Brasil aderiu à Convenção sobre o Cibercrime: o que isso significa? JOTA Jornalismo**, 19 fev. 2022. Disponível em: https://www.jota.info/opiniao-e-analise/artigos/convencao-sobre-o-cibercrime-o-que-isso-significa. Acesso em: 26 jun. 2025.

BELLI, Luca. **Building Good Digital Sovereignty through Digital Public Infrastructures and Digital Commons in India and Brazil**. **ThinkTwenty (T20) India 2023 - Official Engagement Group of G20**, 2023a. Disponível em: https://t20ind.org/research/building-good-digital-sovereignty-through-digital-public-infrastructures/. Acesso em: 1 jul. 2025.

BELLI, Luca *et al.* **Cibersegurança: Uma Visão Sistêmica Rumo A Uma Proposta De Marco Regulatório Para Um Brasil Digitalmente Soberano**. Rio de Janeiro: FGV Direito Centro de Tecnologia e Sociedade, 2023a.

BELLI, Luca. Exploring the Key AI Sovereignty Enablers (KASE) of Brazil, towards an AI Sovereignty Stack. **SSRN Electronic Journal**, 2023b.

BELLI, Luca. **To Get Its AI Foothold, Brazil Needs to Apply the Key AI Sovereignty Enablers (KASE)**. Rochester, NY, 25 maio 2023c. Disponível em: https://papers.ssrn.com/abstract=4465501. Acesso em: 6 dez. 2023.

BELLI, Luca. **Building Good Digital Sovereignty through Digital Public Infrastructures and Digital Commons in India and Brazil**. **ThinkTwenty (T20) India 2023 - Official Engagement Group of G20**, jun. 2023d. Disponível em: https://t20ind.org/research/building-good-digital-sovereignty-through-digital-public-infrastructures/. Acesso em: 10 jul. 2024.

BELLI, Luca *et al.* **Cibersegurança: uma visão sistêmica rumo a uma Proposta de Marco Regulatório para um Brasil Digitalmente soberano**. Rio de Janeiro, RJ: Luca Belli, 2023b.

BELLI, Luca. **AI Meets Cybersecurity: A Brazilian Perspective. (2024).** Carnegie Endowment for International Peace, 2024a.

BELLI, Luca. **Soberania em Inteligência Artificial: O que é e quais facilitadores essenciais podem tornar o Brasil um país soberano em IA?; (Sovereignty in Artificial Intelligence: What Is It and What Key Enablers Can Make Brazil a Sovereign Country in AI?)**. Rochester, NYSocial Science Research Network, 26 mar. 2024b. Disponível em: https://papers.ssrn.com/abstract=4961537. Acesso em: 1 jul. 2025.

BELLI, Luca *et al.* **Transferência internacional de dados pessoais na América Latina**. *[S.l.: S.n.]*.

BELLI, Luca. **Da soberania digital à soberania em IA**. Disponível em: https://www.jota.info/opiniao-e-analise/colunas/ia-regulacao-democracia/da-soberania-digital-a-soberania-em-ia. Acesso em: 11 mar. 2025a.

BELLI, Luca. **Da soberania digital à soberania em IA**. Disponível em: https://www.jota.info/opiniao-e-analise/colunas/ia-regulacao-democracia/da-soberania-digital-a-soberania-em-ia. Acesso em: 11 mar. 2025b.

BELLI, Luca. **When AI Meets Cybersecurity: Framing Brazil's Information Security and AI Challenges**. **CyberBRICS**, 2 jun. 2025c. Disponível em: https://cyberbrics.info/when-ai-meets-cybersecurity-framing-brazils-information-security-and-ai-challenges/. Acesso em: 30 jul. 2025.

BELLI, Luca; CURZI, Yasmin; BRITTO GASPAR, Walter. Online Content Regulation in the BRICS Countries: A Cybersecurity Approach to Responsible Social Media Platforms. **SSRN Electronic Journal**, 2023.

BELLI, Luca; DONEDA, Danilo. Data protection in the BRICS countries: legal interoperability through innovative practices and convergence. **International Data Privacy Law**, v. 13, n. 1, p. 1–24, 1 fev. 2023.

BELLI, Luca; GALDINO DE MAGALHÃES SANTOS, Larissa. Editorial: Toward a BRICS stack? Leveraging digital transformation to construct digital sovereignty in the BRICS countries. **Computer Law & Security Review**, v. 55, p. 106064, nov. 2024.

BELLI, Luca; GASPAR, Walter B. The Quest for AI Sovereignty, Transparency and Accountability. 2023a.

BELLI, Luca; GASPAR, Walter B.; JASWANT, Shilpa Singh. Data sovereignty and data transfers as fundamental elements of digital transformation: Lessons from the BRICS countries. **Computer Law & Security Review**, v. 54, p. 106017, 1 set. 2024.

BELLI, Luca; GASPAR, Walter Britto (ORGS.). AI Transparency, AI Accountability, and AI Sovereignty: An Overview. *In*: **The Quest for AI Sovereignty, Transparency and Accountability**. Rio de Janeiro: FGV Direito Rio, 2023b. p. 21-28.

BELLI, Luca; GOLDONI, Luiz Rogério Franco; KARINA, Furtado Rodrigues. Brasil precisa de uma política nacional de cibersegurança - 07/12/2023 - Mercado - Folha. **Brasil precisa de uma política nacional de cibersegurança Só ao compreender os riscos cibernéticos é que a sociedade brasileira será digitalmente soberana**, 7 dez. 2023.

BELLI, Luca; HADZIC, Senka. **Community Networks: Building Digital Sovereignty and Environmental Sustainability**. Rio de Janeiro, RJ: Publicações Direito Rio, 2023.

BELLI, Luca; JIANG, Min. Digital Sovereignty in the BRICS Countries. 2024.

BELLI, Luca; ZINGALES, Nicolo. **Interoperability to Foster Open Digital Ecosystems in the BRICS Countries**. Rochester, NYSocial Science Research Network, 2023. Disponível em: https://papers.ssrn.com/abstract=4641496. Acesso em: 11 mar. 2025.

BENKLER, Yochai. **The wealth of networks: how social production transforms markets and freedom**. New Haven London: Yale University Press, 2006.

BERNSTEIN, Marver H. **Regulating Business by Independent Commission**. *[S.l.]*: Princeton University Press, 1966.

BIONI, Bruno; DIAS, Daniel. Responsabilidade civil na proteção de dados pessoais: construindo pontes entre a Lei Geral de Proteção de Dados Pessoais

e o Código de Defesa do Consumidor. **Civilistica.com**, v. 9, n. 3, p. 1–23, 22 dez. 2020.

BIONI, Bruno Ricardo. **Proteção de Dados Pessoais: a função dos limites do consentimento**. *[S.l.]*: Forense, 2019.

BLACK, Julia; KINGSFORD SMITH, Dimity. Critical reflections on regulation [Plus a reply by Dimity Kingsford Smith.]. **Australasian Journal of Legal Philosophy**, v. 27, n. 2002, p. 1–46, 2002.

BLACKWOOD-BROWN, Carlene; LEVY, Yair; D'ARCY, John. Cybersecurity Awareness and Skills of Senior Citizens: A Motivation Perspective. **Journal of Computer Information Systems**, v. 61, n. 3, p. 195–206, 4 maio 2021.

BNAMERICAS. **Why is Brazil so vulnerable to cyber attacks?** Disponível em: https://www.bnamericas.com/en/features/why-is-brazil-so-vulnerable-to-cyber-attacks. Acesso em: 13 jun. 2024.

BOECHAT, Gabriela. **Entenda o sistema de informações do governo que pode ter sofrido ataque hacker**. Disponível em: https://www.cnnbrasil.com.br/politica/entenda-o-sistema-de-informacoes-do-governo-que-pode-ter-sofrido-ataque-hacker/. Acesso em: 31 jul. 2024.

BRANDS, Hal. **Paradoxes of the Gray Zone - Foreign Policy Research Institute**. Disponível em: https://www.fpri.org/article/2016/02/paradoxes-gray-zone/. Acesso em: 19 jan. 2024.

BRASIL. **Lei 7783**. Disponível em: https://www.planalto.gov.br/ccivil_03/leis/l7783.HTM. Acesso em: 31 ago. 2024.

BRASIL. Portaria Normativa n. 899. Política Nacional da Indústria de Defesa. 19 jul. 2005.

BRASIL. **Estratégia Nacional de Defesa**. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2007-2010/2008/decreto/d6703.htm. Acesso em: 7 maio 2024.

BRASIL. **Livro Branco de Defesa Nacional 2012**, 2012. Disponível em: https://www.gov.br/defesa/pt-br/arquivos/ajuste-01/estado_e_defesa/

livro_branco/Versao2012dolivroLBDNportuguescompactado.pdf. Acesso em: 27 mar. 2025

BRASIL. **Livro Branco de Defesa Nacional 2020**, 2020a. Disponível em: https://www.gov.br/defesa/pt-br/assuntos/copy_of_estado-e-defesa/livro-branco-de-defesa-nacional-lbdn-1.

BRASIL. **Decreto n. 10.222/20**, 5 fev. 2020b. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2019-2022/2020/decreto/d10222.htm. Acesso em: 2 mar. 2023.

BRASIL. **Decreto nº 12.572, de 4 de agosto de 2025 - Institui a Política Nacional de Segurança da Informação**. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2023-2026/2025/decreto/D12572.htm. Acesso em: 12 ago. 2025.

BRASIL, Tribunal de Contas da União. **Cinco Controles de Segurança Cibernética para ontem**. Brasília: Tribunal de Contas da União, 2022. Disponível em: https://portal.tcu.gov.br/publicacoes-institucionais/cartilha-manual-ou-tutorial/5-controles-de-seguranca-cibernetica. Acesso em: 29 jun. 2025.

BRASILEIRO, Governo. Guia Orientativo para Definições dos Agentes de Tratamento de Dados Pessoais e do Encarregado. **Agência Nacional de Proteção de Dados. https://www. gov. br/anpd/pt-br/documentos-e-publicacoes/2021**, v. 5, 2021.

BUYYA, Rajkumar; BROBERG, James; GOSCINSKI, Andrzej. **Cloud Computing: Principles and Paradigms | Wiley**. *[S.l.]*: John Wiley & Sons, Inc., 2011.

BUZAN, Barry *et al.* Security: A New Framework for Analysis. 30 set. 1997.

CABINET OFFICE. **Global Britain in a Competitive Age: the Integrated Review of Security, Defence, Development and Foreign Policy**. Disponível em: https://www.gov.uk/government/publications/global-britain-in-a-competitive-age-the-integrated-review-of-security-defence-development-and-foreign-policy. Acesso em: 18 jan. 2024.

CABINET OFFICE. **Integrated Review Refresh 2023: Responding to a more contested and volatile world**. Disponível em: https://www.gov.uk/government/publications/integrated-review-refresh-2023-responding-to-a-more-contested-and-volatile-world. Acesso em: 18 jan. 2024.

CADWALLADR, Carole *et al.* Revealed: 50 million Facebook profiles harvested for Cambridge Analytica in major data breach. **The Guardian**, 17 mar. 2018.

CARAMANCION, Kevin Matthe *et al.* The Missing Case of Disinformation from the Cybersecurity Risk Continuum: A Comparative Assessment of Disinformation with Other Cyber Threats. **Data**, v. 7, n. 4, abr. 2022.

CASAGRANDE, Luiz; BOAS, Evandro Cesar Vilas; AQUINO, Guilherme Pedro. Systems, Software, and Applications Updating for avoiding Cyber Attacks: A Pentest Demonstration. *In*: XL SIMPÓSIO BRASILEIRO DE TELECOMUNICAÇÕES E PROCESSAMENTO DE SINAIS. **Anais do XL Simpósio Brasileiro de Telecomunicações e Processamento de Sinais**. Sociedade Brasileira de Telecomunicações, 2022. Disponível em: https://biblioteca.sbrt.org.br/articles/3559. Acesso em: 4 ago. 2025.

CASSIOLATO, José Eduardo. Evolution and Dynamics of the Brazilian National System of Innovation. *In*: SHOME, Parthasarathi; SHARMA, Pooja (Orgs.). **Emerging Economies**. New Delhi: Springer India, 2015. p. 265–310.

CASTELLS, Manuel. **A Galáxia Internet: reflexões sobre a Internet, negócios e a sociedade**. *[S.l.]*: Zahar, 2003.

CAVALCANTE, Márcio André Lopes. **Legitimidade da prova obtida por meio de cooperação jurídica internacional**. Buscador Dizer o Direito, 2024. Disponível em: https://www.buscadordizerodireito.com.br/jurisprudencia/detalhes/130f1a8e9e102707f3f91b010f151b0b. Acesso em: 12 ago. 2024

CAVELTY, Myriam Dunn. From Cyber-Bombs to Political Fallout: Threat Representations with an Impact in the Cyber-Security Discourse. **International Studies Review**, v. 15, n. 1, p. 105–122, 1 mar. 2013.

CAVOUKIAN, Ann. Privacy by design: origins, meaning, and prospects for assuring privacy and trust in the information era. *In*: **Privacy protection**

measures and technologies in business organizations: aspects and standards. *[S.l.]*: IGI Global, 2012. p. 170–208.

CAVOUKIAN, Ann. Privacy by Design The 7 Foundational Principles. *[S.d.]*.

CEBULA, James J.; YOUNG, Lisa R. A Taxonomy of Operational Cyber Security Risks. **Software Engineering Institute, Carnegie Mellon University**, 2010.

CENTRO DE INOVAÇÃO PARA A EDUCAÇÃO BRASILEIRA. **Marco conceitual: Escola Conectada**. São Paulo, SP: Lumos Assessoria Editorial, 2021.

CERT.BR. **Internet Segura**. Disponível em: https://internetsegura.br/pdf/guia-internet-segura.pdf. Acesso em: 7 jul. 2025.

CERT.BR. **CERT.br - Estatísticas**. Disponível em: https://stats.cert.br/. Acesso em: 30 jun. 2025.

CERT.br - Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil. Disponível em: https://www.cert.br/. Acesso em: 20 dez. 2024.

CETEC; TUJAL, Luiz Cláudio. Modelo de Referência de Cloud. *In*: **Amãpytuna Computação em Nuvem: Serviços livres para a sociedade do conhecimento**. Brasília: FUNAG, 2010.

CGEE; MCTI. **Estratégia Brasileira para a Transformação Digital (E-Digital): Ciclo 2022-2026**. Brasília: Ministério da Ciência, Tecnologia e Inovações, 2022. Disponível em: https://www.gov.br/mcti/pt-br/acompanhe-o-mcti/transformacaodigital/arquivosestrategiadigital/e-digital_ciclo_2022-2026.pdf.

CHACON, Guilherme; BAWDEN SILVERIO DE CASTRO, Henrique; XAVIER MORALES, Luiza. **Análise: Termos De Uso e Políticas De Privacidade do Google Workspace for Education e Microsoft 365 (Office 365 Educação)**. *[S.l.]*: Zenodo, 17 maio 2022. Disponível em: https://zenodo.org/records/7718863. Acesso em: 1 jul. 2025.

CHANG, Ha-Joon. Breaking the mould: an institutionalist political economy alternative to the neo-liberal theory of the market and the state. **Cambridge Journal of Economics**, v. 26, n. 5, p. 539–559, 1 set. 2002.

CHERDANTSEVA, YULIA; HILTON, Jeremy. Information Security and Information Assurance. The Discussion about the Meaning, Scope and Goals,". *In*: *[S.l.: S.n.]*.

CHESNEY, Robert; CITRON, Danielle Keats. **Deep Fakes: A Looming Challenge for Privacy, Democracy, and National Security**. Rochester, NYSocial Science Research Network, 14 jul. 2018. Disponível em: https://papers.ssrn.com/abstract=3213954. Acesso em: 30 jun. 2025

CIO-DOD. **DoD Strategy for Defending Networks, Systems, and Data**. Washington, DC: Department of Defense, 13 nov. 2013. Disponível em: https://dodcio.defense.gov/Portals/0/Documents/DoD%20Strategy%20for%20Defending%20Network%20Systems%20and%20Data.pdf. Acesso em: 8 fev. 2024.

CISA Cyber Threat Indicator and Defensive Measure Submission System | CISA. Disponível em: https://www.cisa.gov/forms/share-indicators. Acesso em: 20 dez. 2024.

CISA CYBERSECURITY DIVISION. **Zero trust maturity model**. Washington, DC: Cybersecurity and Infrastructure Security Agency, abr. 2023. Disponível em: https://www.cisa.gov/sites/default/files/2023-04/zero_trust_maturity_model_v2_508.pdf. Acesso em: 18 jan. 2024.

CISCO. **Cybersecurity Readiness Index 2025**. Disponível em: https://newsroom.cisco.com/c/r/newsroom/en/us/a/y2025/m05/cybersecurity-readiness-index-2025.html. Acesso em: 12 maio 2025.

CISCO. **What Is a Cyberattack? - Most Common Types**. Disponível em: https://www.cisco.com/c/en/us/products/security/common-cyberattacks.html. Acesso em: 3 mar. 2023.

CLOUDFLARE. **DDoS threat report for 2023 Q4**. Disponível em: https://blog.cloudflare.com/ddos-threat-report-2023-q4. Acesso em: 17 jan. 2024.

CLOUDFLARE. **Ataque de DDoS de inundação SYN**. Disponível em: https://www.cloudflare.com/pt-br/learning/ddos/syn-flood-ddos-attack/. Acesso em: 17 jan. 2024.

CNDI. **Nova Indústria Brasil: Plano de ação para a Neoindustrialização**. Brasília: Conselho Nacional de Desenvolvimento Industrial, MDIC, 2024. Disponível em: https://www.gov.br/mdic/pt-br/composicao/se/cndi/plano-de-acao/nova-industria-brasil-plano-de-acao.pdf. Acesso em: 20 fev. 2024.

CNI; FUNCEX. Coeficientes de abertura comercial. **Indicadores Econômicos CNI**, v. 10, n. 1, p. 8, dez. 2022.

CNJ. **Estratégia Nacional de Segurança Cibernética do Poder Judiciário**. Disponível em: https://atos.cnj.jus.br/atos/detalhar/3975. Acesso em: 9 maio 2024.

COHEN, Julie. Cyberspace As/And Space. **Georgetown Law Faculty Publications and Other Works**, 1 jan. 2007.

COLOMBINI, Iderley. Limites lógicos das teses do capitalismo cognitivo e do tecnofeudalismo. **Revista da Sociedade Brasileira de Economia Política**, v. 4, n. 65, p. 164–190, 2023.

CONNEL, Michael; VOGLER, Sarah. **Russia's Approach to Cyber Warfare (1Rev). 2017**. Center for Naval Analyses Arlington United States, 2017.

CORN, Gary. **Cyber National Security: Navigating Gray Zone Challenges In and Through Cyberspace**. Rochester, NY, 16 dez. 2017. Disponível em: https://papers.ssrn.com/abstract=3089071. Acesso em: 17 jan. 2024.

COULDRY, Nick; MEJIAS, Ulises A. The Costs of Connection: How Data Are Colonizing Human Life and Appropriating It for Capitalism | Request PDF. **ResearchGate**, 22 out. 2024.

COUNCIL OF EUROPE. **Budapest Convention on Cybercrime**. Disponível em: https://www.coe.int/en/web/cybercrime/the-budapest-convention. Acesso em: 14 jun. 2023.

COUTO, Natalia de Macedo. O papel regulatório do Estado na moderação de conteúdo exercida pelas plataformas de redes sociais. 21 set. 2022.

COUTURE, Stéphane; TOUPIN, Sophie. **What Does the Concept of "Sovereignty" Mean in Digital, Network and Technological Sovereignty?** Rochester, NYSocial Science Research Network, 22 jan. 2018. Disponível em: https://papers.ssrn.com/abstract=3107272. Acesso em: 11 mar. 2025.

CROZE, Hervé; BISMUTH, Yves. **Droit de l'informatique: éléments de droit à l'usage des informaticiens**. Paris: Econômica, 1986.

CRUZ, Francisco Brito *et al.* Internet e eleições no Brasil. 2019.

CSRC. **Asset**. Disponível em: https://csrc.nist.gov/glossary/term/asset. Acesso em: 24 jan. 2024.

DE FILIPPI, Primavera; BELLI, Luca. **The Law of the Cloud V the Law of the Land: Challenges and Opportunities for Innovation**. Rochester, NY, 26 out. 2012. Disponível em: https://papers.ssrn.com/abstract=2167382. Acesso em: 22 jan. 2024.

DE HERT, P. J. A.; GUTWIRTH, S. Privacy, data protection and law enforcement: Opacity of the individual and transparency of power. *In*: CLAES, E.; DUFF, A.; GUTWIRTH, S. (Orgs.). **Privacy and the criminal law**. Antwerp/Oxford: Intersentia, 2006. p. 61–104.

DEIBERT, Ronald J. Toward a Human-Centric Approach to Cybersecurity. **Ethics & International Affairs**, v. 32, n. 4, p. 411–424, dez. 2018.

DEVANNY, Joe; BUCHAN, Russel. **Brazil's Cyber Strategy Under Lula: Not a Priority, but Progress Is Possible**. ago. 2023.

DEVANNY, Joe; GOLDONI, Luiz Rogério Franco; MEDEIROS, Breno Pauli. The rise of cyber power in Brazil. **Revista Brasileira de Política Internacional**, v. 65, 2022.

DIAS, Daniel Pires Novais *et al.* Plataformas no Marco Civil da Internet: a necessidade de uma responsabilidade progressiva baseada em riscos. **Civilistica.com**, v. 12, n. 3, p. 1–24, 29 dez. 2023.

DIEGUES, Antônio Carlos; ROSELINO, José Eduardo. **Política Industrial, Tecno-nacionalismo e Indústria 4.0: a Guerra Tecnológica entre China e EUA**: Textos para discussão. Campinas: IE-UNICAMP, jan. 2021. Disponível em: https://www.eco.unicamp.br/noticias/politica-industrial-tecno-nacionalismo-e-industria-40-a-guerra-tecnologica-entre-china-e-eua. Acesso em: 16 set. 2023.

DIGI AMERICAS ALLIANCE. **Information sharing in LATAM: UNDERSTANDING THE ROLE OF ISACS IN THE REGION**. *[S.l.]*: Belisario Contreras; Alexis Steffaro; Pallavi Bhargava, 2025.

Diretiva (UE) 2016/680 DO PARLAMENTO EUROPEU E DO CONSELHO - de 27 de abril de 2016 - relativa à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais pelas autoridades competentes para efeitos de prevenção, investigação, deteção ou repressão de infrações penais ou execução de sanções penais, e à livre circulação desses dados, e que revoga a Decisão-Quadro 2008/ 977/ JAI do Conselho, 4 maio 2016. Disponível em: https://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=CELEX:32016L0680.

DOD. **DoD Strategy for Operating in Cyberspace**. Washington, DC: Department of Defense, jul. 2011. Disponível em: https://dodcio.defense.gov/Portals/0/Documents/Cyber/DoD%20Strategy%20for%20Operating%20in%20Cyberspace%20July%202011.pdf. Acesso em: 8 fev. 2024.

DONEDA, Danilo. **Da privacidade à proteção de dados pessoais**. 2. ed. São paulo: Thomas Reuters Brasil, 2019.

DUMMER, Sven; RATH, Sandeep. **A Retrospective on DDoS Trends in 2023 and Actionable Strategies for 2024**. Disponível em: https://www.akamai.com/blog/security/a-retrospective-on-ddos-trends-in-2023. Acesso em: 17 jan. 2024.

DUNN CAVELTY, Myriam; WENGER, Andreas. Cyber security meets security politics: Complex technology, fragmented politics, and networked science. **Contemporary Security Policy**, v. 41, n. 1, p. 5–32, 2 jan. 2020.

EASTERLY, Jen. **The Cost of Unsafe Technology and What We Can Do About It | CISA**. Disponível em: https://www.cisa.gov/news-events/news/cost-unsafe-technology-and-what-we-can-do-about-it. Acesso em: 23 fev. 2024.

EDWARDS, Benjamin *et al.* Strategic aspects of cyberattack, attribution, and blame. **Proceedings of the National Academy of Sciences**, v. 114, n. 11, p. 2825–2830, 14 mar. 2017.

EHRHARDT JR., Marcos; MODESTO, Jéssica Andrade. Breves Notas Sobre Anonimização E Proteção De Dados Pessoais. *In*: REQUIÃO, Maurício (Org.). **Proteção de dados pessoais: novas perspectivas**. Professor Edvaldo Brito. *[S.l.]*: EDUFBA, 2022. p. 123–126.

ELING, Martin; SCHNELL, Werner. What do we know about cyber risk and cyber risk insurance? **The Journal of Risk Finance**, v. 17, n. 5, p. 474–491, 1 jan. 2016.

EMCFA. **Doutrina Militar de Defesa Cibernética**. Brasília: Ministério da Defesa, 2023. Disponível em: https://www.gov.br/defesa/pt-br/assuntos/estado-maior-conjunto-das-forcas-armadas/doutrina-militar/publicacoes-1/publicacoes/MD31M07DoutrinaMilitardeDefesaCiberntica2Edio2023.pdf. Acesso em: 8 fev. 2024.

ENISA. **Foreign Information Manipulation and Interference (FIMI) and cybersecurity: threat landscape.** LU: Publications Office, 2022a.

ENISA. **Foreign Information Manipulation and Interference (FIMI) and cybersecurity: threat landscape**. Report/Study. Disponível em: https://www.enisa.europa.eu/publications/foreign-information-manipulation-interference-fimi-and-cybersecurity-threat-landscape. Acesso em: 19 fev. 2024b.

ENISA. **ENISA Transport Threat Landscape**. Report/Study. Disponível em: https://www.enisa.europa.eu/publications/enisa-transport-threat-landscape. Acesso em: 19 fev. 2024.

ENISA. **Cryptography**. Topic. Disponível em: https://www.enisa.europa.eu/topics/cryptography. Acesso em: 23 fev. 2024a.

ENISA. **Foresight Cybersecurity Threats For 2030 - Update 2024: Extended report**. Report/Study. Disponível em: https://www.enisa.europa.eu/publications/foresight-cybersecurity-threats-for-2030-update-2024-extended-report. Acesso em: 11 jun. 2024b.

ENISA. **Cyber Hygiene | ENISA**. Disponível em: https://www.enisa.europa.eu/publications/cyber-hygiene. Acesso em: 1 jul. 2025c.

ENISA. **Glossary of Terms | ENISA**. Disponível em: https://www.enisa.europa.eu/media/media-press-kits/enisa-glossary. Acesso em: 24 jun. 2025.

ENISA. **Zero-Day**. Disponível em: https://www.enisa.europa.eu/topics/incident-response/glossary/zero-day. Acesso em: 18 jan. 2024.

ESTACHE, Antonio; MARTIMORT, David. **Politics, Transaction Costs, and the Design of Regulatory Institutions**. Rochester, NYSocial Science Research Network, 1 mar. 1999. Disponível em: https://papers.ssrn.com/abstract=620512. Acesso em: 30 jul. 2025.

Ethical Hacking: Understanding the Basics. **Cybersecurity Exchange**, 12 jun. 2022. Disponível em: https://www.eccouncil.org/cybersecurity-exchange/ethical-hacking/ethical-hacking-understanding-basics/. Acesso em: 17 jan. 2024.

EUROPEAN COMMISSION. **Proposta de REGULAMENTO DO PARLAMENTO EUROPEU E DO CONSELHO relativo aos requisitos horizontais de cibersegurança dos produtos com elementos digitais e que altera o Regulamento (UE) 2019/1020**. Disponível em: https://eur-lex.europa.eu/legal-content/PT/TXT/HTML/?uri=CELEX:52022PC0454. Acesso em: 11 ago. 2025.

EUROPEAN COMMISSION. **COMUNICAÇÃO DA COMISSÃO AO PARLAMENTO EUROPEU, AO CONSELHO, AO COMITÉ ECONÓMICO E SOCIAL EUROPEU E AO COMITÉ DAS REGIÕES sobre o plano de ação para a democracia europeia**, 27 ago. 2020. Disponível em: file:///C:/Users/user/Downloads/090166e5d6c8f02d.pdf. Acesso em: 31 ago. 2024.

EUROPEAN NETWORK AND INFORMATION SECURITY AGENCY. **Information sharing and analysis centres (ISACs): cooperative models.** LU: Publications Office, 2017.

EUROPEAN UNION AGENCY FOR CYBERSECURITY. **Best practices for cyber crisis management: February 2024.** LU: Publications Office, 2024.

EUROPEAN UNION AGENCY FOR NETWORK AND INFORMATION SECURITY. **Review of cyber hygiene practices.** LU: Publications Office, 2016.

FERNANDES, Jorge Henrique Cabral. **INTRODUÇÃO À GESTÃO DE RISCOS DE SEGURANÇA DA INFORMAÇÃO**. UNB, 2009. Disponível em: https://www.trf3.jus.br/documentos/rget/seguranca/CLRI/GSIC302_Introducao_Gestao_Riscos_Seguranca_Informacao.pdf.

FERRAZ, João Carlos; PAULA, Germano Mendes de; KUPFER, David. Política industrial. *In*: KUPFER, David; HASENCLEVER, Lia (Orgs.). **Economia industrial: fundamentos teóricos e práticas no Brasil**. 2. ed. Rio de Janeiro: Elsevier, 2016. p. 313–323.

FERREIRA, Ivete Senise. **A Criminalidade Informática**. Bauru: EDIPRO, 2001.

FICHTNER, Laura. What kind of cyber security? Theorising cyber security and mapping approaches. **Internet Policy Review**, v. 7, n. 2, 15 maio 2018a.

FICHTNER, Laura. What kind of cyber security? Theorising cyber security and mapping approaches. **Internet Policy Review**, v. 7, n. 2, 15 maio 2018b.

FISCHER, E. A. Cybersecurity issues and challenges: In Brief. *In*: **Cyberspace Threat Landsc.: Overv., Response Authorities, and Capab.** *[S.l.]*: Nova Science Publishers, Inc., 2015. p. 45–54.

FLORIDI, Luciano. The Fight for Digital Sovereignty: What It Is, and Why It Matters, Especially for the EU. **Philosophy & Technology**, v. 33, n. 3, p. 369–378, 1 set. 2020.

FORTINET. **FortiGuard Labs apresenta relatório sobre ciberataques no Brasil**. Disponível em: https://www.fortinet.com/br/corporate/about-us/newsroom/press-releases/2022/fortiguard-labs-relatorio-ciberataques-brasil-2021.html. Acesso em: 25 jun. 2025.

FORTINET. **What is Cryptography? Definition, Importance, Types**. Disponível em: https://www.fortinet.com/resources/cyberglossary/what-is-cryptography. Acesso em: 23 fev. 2024.

FORTINET. **Relatório de ameaças da Fortinet revela aumento recorde em ataques cibernéticos automatizados, com adversários utilizando IA e novas técnicas como armas**. Disponível em: https://www.fortinet.com/br/corporate/about-us/newsroom/press-releases/2025/fortinet-threat-report-reveals-record-surge-in-automated-cyberattacks.html. Acesso em: 25 jun. 2025.

Framework for Improving Critical Infrastructure Cybersecurity. 16 abr. 2018. Disponível em: https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf.

FRANCILLON, Aurélien *et al*. Backdoors: Definition, Deniability & Detection. *In*: 2018. Disponível em: https://www.semanticscholar.org/paper/Backdoors:-Definition,-Deniability-&-Detection-Francillon-Bailey/86335230956671f85d4d967dcbc7843d720f06e3. Acesso em: 8 fev. 2024.

FREITAS, Cristiana. E-Prints in Library & Information Science. **Garantir a autenticidade e o acesso continuado à informação digital: os desafios da preservação digital em arquivos**, 11º Congresso Nacional de Bibliotecários, Arquivistas e Documentalistas. 21 out. 2012.

FREUND, Gislaine Parra; SEMBAY, Márcio José; MACEDO, Douglas Dyllon Jeronimo De. RICI. Revista Ibero-Americana de Ciência da Informação. **Proveniência de dados e segurança da informação: relações interdisciplinares no domínio da Ciência da Informação**, 3. v. 12, p. 807–825, dez. 2019.

FRYE, Jason *et al.* **Cyber threat metrics.** *[S.l.: S.n.]*. Disponível em: https://www.osti.gov/servlets/purl/1039394/. Acesso em: 2 fev. 2024.

FUCHS, Christian. Labor in Informational Capitalism and on the Internet. **The Information Society**, v. 26, n. 3, p. 179–196, 30 abr. 2010.

G1. **Suspeito do maior vazamento de dados da internet brasileira é preso na BA; 223 milhões de pessoas tiveram informações divulgadas**. Disponível em: https://g1.globo.com/ba/bahia/noticia/2024/04/09/suspeito-de-hackear-sites-do-senado-exercito-e-tse-e-preso-na-ba.ghtml. Acesso em: 13 jun. 2024.

GADELHA, Carlos Augusto Grabois; TEMPORÃO, José Gomes. Desenvolvimento, Inovação e Saúde: a perspectiva teórica e política do Complexo Econômico-Industrial da Saúde. **Ciência & Saúde Coletiva**, v. 23, p. 1891–1902, jun. 2018.

GAIDA, Jaime *et al.* **Critical Technology Tracker**. Disponível em: https://techtracker.aspi.org.au/. Acesso em: 16 maio 2023.

GCAZA, Noluxolo; THOMSON, Kerry-Lynn. Factors contributing to the successful development of cyber safety education for foundation phase children: a systematic literature review. **Information & Computer Security**, v. ahead-of-print, n. ahead-of-print, 17 fev. 2025.

GELUVARAJ, B.; SATWIK, P. M.; KUMAR, T. A. Ashok. The future of cybersecurity: Major role of artificial intelligence, machine learning, and deep learning in cyberspace. **International Conference on Computer Networks and Communication Technologies**, 2018.

GERDING, Erik. **Cybersecurity Disclosure**. Disponível em: https://www.sec.gov/news/statement/gerding-cybersecurity-disclosure-20231214. Acesso em: 29 jan. 2024.

GOERTZ, Gary. **Social Science Concepts: A User's Guide**. *[S.l.]*: Princeton University Press, 2006.

GOLDONI, Luiz Rogério Franco *et al*. The meaning of cyberwarfare in Brazil. *In*: **Research handbook on cyberwarfare**. *[S.l.]*: Edward Elgar Publishing, 2024. p. 115–130.

GOLDONI, Luiz Rogério Franco; RODRIGUES, Karina Furtado; MEDEIROS, Breno Pauli. Qual é o futuro da governança de cibersegurança no Brasil? **Cadernos Gestão Pública e Cidadania**, v. 29, p. e90972–e90972, 17 abr. 2024.

GORWA, Robert. What is platform governance? **Information, Communication & Society**, v. 22, n. 6, p. 854–871, 12 maio 2019.

GREENBERG, Andy. **Sandworm: A New Era of Cyberwar and the Hunt for the Kremlin's Most Dangerous Hackers**. First Edition ed. New York: Doubleday, 2019.

GREENWALD, Glenn; MACASKILL, Ewen. NSA Prism program taps in to user data of Apple, Google and others. **The Guardian**, 7 jun. 2013.

GROHMANN, Rafael. Plataformas de propriedade de trabalhadores: cooperativas e coletivos de entregadores. **MATRIZes**, v. 16, n. 1, p. 209–233, 9 maio 2022.

GSI. **Estratégia Nacional de Segurança Cibernética (E-Ciber)**. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2019-2022/2020/decreto/d10222.htm. Acesso em: 7 fev. 2023.

GSI. **REGIC - DECRETO Nº 10.748 - Rede Federal de Gestão de Incidentes Cibernéticos (REGIC)**, 16 jul. 2021a. Disponível em: https://www.in.gov.br/en/web/dou/-/decreto-n-10.748-de-16-de-julho-de-2021-332610022.

GSI. **Glossário de Segurança da Informação**. Disponível em: https://www.gov.br/gsi/pt-br/ssic/glossario-de-seguranca-da-informacao-1. Acesso em: 29 maio 2024b.

GSI. **PNCiber - Política Nacional de Cibersegurança e o Comitê Nacional de Cibersegurança.** Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2023-2026/2023/decreto/D11856.htm. Acesso em: 10 jan. 2024.

GSI. **E-Ciber (Estratégia Nacional de Cibersegurança) - Decreto Nº 12.573, de 4 de agosto de 2025**. Disponível em: https://www.gov.br/gsi/pt-br/assuntos/seguranca-da-informacao-e-cibernetica/estrategia-nacional-de-ciberseguranca-eciber/E-Ciber. Acesso em: 8 ago. 2025a.

GSI. **E-Ciber (Estratégia Nacional de Cibersegurança)**. Disponível em: https://www.gov.br/gsi/pt-br/assuntos/seguranca-da-informacao-e-cibernetica/estrategia-nacional-de-ciberseguranca-eciber/E-Ciber. Acesso em: 6 ago. 2025b.

GUZMAN, Chad de. **A Timeline of the U.S.-China Trade War During Trump's Second Term**. Disponível em: https://time.com/7292207/us-china-trade-war-trump-tariffs-timeline/. Acesso em: 15 ago. 2025.

HAESBAERT, Rogério. Territórios Alternativos. **GEOgraphia**, v. 4, n. 7, p. 97–98, 2002.

HAESBAERT, Rogério. Território e multiterritorialidade: um debate. **GEOgraphia**, v. 9, n. 17, 2007.

HANDLER, Simon. **The 5×5—The future of cyber diplomacy**. Disponível em: https://www.atlanticcouncil.org/content-series/the-5x5/the-5x5-the-future-of-cyber-diplomacy/. Acesso em: 18 jan. 2024.

HANSEN, Lene; NISSENBAUM, Helen. Digital Disaster, Cyber Security, and the Copenhagen School. **International Studies Quarterly**, v. 53, n. 4, p. 1155–1175, dez. 2009.

HARTMAN, Ivar *et al.* **Moderação de conteúdo online: Contexto, cenário brasileiro e suas perspectivas regulatórias | FGV Direito Rio**. *[S.l.: S.n.]*.

HATHAWAY, Oona A. *et al.* The Law of Cyber-Attack. **California Law Review**, v. 100, n. 4, p. 817–885, 2012.

HESSELDAHL, Arik. **Here's What Helped Sony's Hackers Break In: Zero-Day Vulnerability**. Disponível em: https://www.vox.com/2015/1/20/11557888/heres-what-helped-sonys-hackers-break-in-zero-day-vulnerability. Acesso em: 18 jan. 2024.

HOEPERS, Cristine. A Importância dos Fatores Humanos para a Cibersegurança. **Computação Brasil**, n. 52, p. 61–66, 11 jun. 2024.

HOLANDA, Marianna; GARCIA, Nathalia. **Governo desautoriza proposta de taxar usuários da internet**. Disponível em: https://www1.folha.uol.com.br/mercado/2023/07/governo-quer-taxar-todos-os-usuarios-de-internet-para-bancar-agencia-de-ciberseguranca.shtml. Acesso em: 25 jun. 2025.

HOOD, Christopher. **Controlling modern government: Variety, commonality and change**. *[S.l.]*: Edward Elgar Publishing, 2005.

HUNKER, Jeffrey; HUTCHINSON, Bob; JONATHAN, Margulies. **Roles and Challenges for Sufficient Cyber-Attack Attribution - I3P**. Disponível em: https://www.yumpu.com/en/document/view/51339084/roles-and-challenges-for-sufficient-cyber-attack-attribution-i3p. Acesso em: 15 jan. 2024.

HUREL, Louise Marie. SEGURANÇA CIBERNÉTICA E DIGITAL: PILAR PARA UMA AGENDA DE DESENVOLVIMENTO SUSTENTÁVEL. *In*: CONFEDERAÇÃO NACIONAL DA INDÚSTRIA (Ed.). **Panorama dos Desafios Brasileiros da Indústria de Defesa e Segurança**. *[S.l.]*: Confederação Nacional da Indústria, 2023.

INFRASTRUCTURE. **infrastructure**. Disponível em: https://dictionary.cambridge.org/dictionary/english/infrastructure. Acesso em: 31 ago. 2024.

INSTITUTO LOCOMOTIVA. **Modelo de internet restrito prejudica acesso a direitos básicos, diz pesquisa**. Disponível em: https://idec.org.br/noticia/modelo-de-internet-restrito-prejudica-acesso-direitos-basicos-diz-pesquisa. Acesso em: 25 jun. 2025.

INTER AMERICAN DEVELOPMENT BANK; ORGANIZATION OF AMERICAN STATES. 2020 Cybersecurity Report: Risks, Progress, and the Way Forward in Latin America and the Caribbean. **IDB Publications**, 28 jul. 2020.

INTERNATIONAL ORGANIZATION FOR STANDARDIZATION. **ISO/IEC 27000:2012**. Disponível em: https://www.iso.org/standard/56891.html. Acesso em: 7 fev. 2024.

INTERNET GOVERNANCE FORUM. **Best Practices Forum on Establishing and Supporting Computer Security Incident Response Teams (CSIRTs) for Internet Security**. *[S.l.: S.n.]*. Disponível em: https://www.first.org/global/governance/bpf-csirt-2015-report.pdf.

ISACA. **ISACA Interactive Glossary**. Disponível em: https://www.isaca.org/resources/glossary. Acesso em: 24 jan. 2024.

ITU-T - INTERNATIONAL TELECOMMUNICATION UNION. **Recommendation ITU-T X.1205: Overview of Cybersecurity**, 2008. Disponível em: file:///C:/Users/user/Downloads/T-REC-X.1205-200804-I!!PDF-E.pdf. Acesso em: 31 ago. 2024.

JACKSON, Rosanna. The purpose of policy space for developing and developed countries in a changing global economic system. **Research in Globalization**, v. 3, p. 100039, 1 dez. 2021.

JACOBI, P. R. **Aprendizagem social e áreas de proteção ambiental**. *[S.l.]*: Annablume Editora, 2015.

JIANG, Min; BELLI, Luca. Digital Sovereignty in the BRICS Countries. 2024.

JOHNSON, Leighton. **Computer incident response and forensics team management: conducting a successful incident response**. Amsterdam; Boston: Elsevier, Syngress, 2014.

JORDÃO, Eduardo; RIBEIRO, Maurício Portugal. COMO DESESTRUTURAR UMA AGÊNCIA REGULADORA EM PASSOS SIMPLES. **REI - REVISTA ESTUDOS INSTITUCIONAIS**, v. 3, n. 1, p. 180–209, 20 ago. 2017.

JORGE, Ayrton Décio de Jesus. **Segurança e Integridade da Informação em contexto organizacional**. Dissertação de Mestrado—Lisboa: Instituto Superior de Tecnologias Avançadas de Lisboa, out. 2021.

KADRICH, Mark. **Endpoint Security**. *[S.l.]*: Pearson Education, 2007.

KARIMI, Seyed Majid *et al.* A Comprehensive Model for Parental Education Content to Prevent Cyber-Space Harm in Students. **Journal of Study and Innovation in Education and Developmen**, v. 4, n. 2, p. 1–15, 2024.

KASPERSKY. **Flowing through Amazonia: The dark web threat landscape for Brazil. Analytical report.** Disponível em: https://dfi.kaspersky.com/blog/flowing-through-amazonia. Acesso em: 25 jun. 2025.

KELLER, Clara Iglesias. Regulação nacional de serviços na Internet: exceção, legitimidade e o papel do Estado. 2019.

KIM, Min-hyung. North Korea's Cyber Capabilities and Their Implications for International Security. **Sustainability**, v. 14, n. 3, p. 1744, jan. 2022.

KOOP, Christel; LODGE, Martin. What is regulation? An interdisciplinary concept analysis. **Regulation & Governance**, v. 11, 1 ago. 2015.

KOUPAEI, Alireza Nik Aein. The Evolving Nature of Cyber Attacks and the Need for Proactive Defense Measures. **Journal of Research in Engineering and Applied Sciences**, v. 8, n. 4, p. 634–639, 29 dez. 2023.

KUEHL, Daniel T. From Cyberspace to Cyberpower: Defining the Problem. *In*: KRAMER, Franklin D.; STARR, Stuart H.; WENTZ, Larry K. (Orgs.). **Cyberpower and National Security**. *[S.l.]*: University of Nebraska Press, 2009. p. 24–42.

LACERDA, Antonio Corrêa de; SEVERIAN, Danilo. Política industrial e desindustrialização no Brasil: Inspirações de David Kupfer ao debate. **Revista de Economia Contemporânea**, v. 27, p. e232724, 18 dez. 2023.

LAGE, Daniel Dore. Do crime de invasão de dispositivo informático: Uma análise do tipo penal à luz da legalidade estrita. **Do crime de invasão de dispositivo informático: Uma análise do tipo penal à luz da legalidade estrita**, 2013.

LEE, Keun; LIM, Chaisung. Technological regimes, catching-up and leapfrogging: findings from the Korean industries. **Research Policy**, v. 30, n. 3, p. 459–483, mar. 2001.

LEE, Keun; MALERBA, Franco. Catch-up cycles and changes in industrial leadership: Windows of opportunity and responses of firms and countries in the evolution of sectoral systems. **Research Policy**, v. 46, n. 2, p. 338–351, mar. 2017.

LEVI-FAUR, David. Regulation and Regulatory Governance. *In*: **Handbook on the Politics of Regulation**. Edward Elgar Publishing: David Levi-Faur, 2011. chapter 1.

LEVI-FAUR, David. **From "Big Government" to "Big Governance"?** *[S.l.]*: Oxford University Press, 2012.

LEVY, Brian; SPILLER, Pablo T. The Institutional Foundations of Regulatory Commitment: A Comparative Analysis of Telecommunications Regulation. **The Journal of Law, Economics, and Organization**, out. 1994.

LI, Yuchong; LIU, Qinghui. A comprehensive review study of cyber-attacks and cyber security; Emerging trends and recent developments. **Energy Reports**, v. 7, p. 8176–8186, 1 nov. 2021.

LIBICKI, Martin C. **Cyberdeterrence and Cyberwar**. *[S.l.]*: RAND Corporation, 2009a.

LIBICKI, Martin C. Cyberdeterrence and Cyberwar. 22 set. 2009b.

LIBICKI, Martin C. The Specter of Non-Obvious Warfare. **Strategic Studies Quarterly**, v. 6, n. 3, p. 88–101, 2012a.

LIBICKI, Martin C. The Specter of Non-Obvious Warfare. **Strategic Studies Quarterly**, v. 6, n. 3, p. 88–101, 2012b.

LIM, Chaisung *et al*. Frugal innovation and leapfrogging innovation approach to the Industry 4.0 challenge for a developing country. **Asian Journal of Technology Innovation**, v. 29, n. 1, p. 87–108, 2 jan. 2021.

LINDSAY, Jon R. Stuxnet and the Limits of Cyber Warfare. **Security Studies**, v. 22, n. 3, p. 365–404, 1 ago. 2013.

LOBATO, Luísa Cruz; KENKEL, Kai Michael. Discourses of cyberspace securitization in Brazil and in the United States. **Revista Brasileira de Política Internacional**, v. 58, p. 23–43, dez. 2015.

LUO, Siping; LOVELY, Mary E.; POPP, David. Intellectual returnees as drivers of indigenous innovation: Evidence from the Chinese photovoltaic industry. **The World Economy**, 14 ago. 2017.

MAJONE, G. The Rise of the Regulatory State in Europe. *In*: BALDWIN, Robert; SCOTT, Colin; HOOD, Christopher (Orgs.). **A Reader on Regulation**. *[S.l.]*: Oxford University Press, 1998.

MAJONE, Giandomenico. The new European agencies: regulation by information. **Journal of European Public Policy**, v. 4, n. 2, p. 262–275, 1 jun. 1997.

MALATJI, Masike; TOLAH, Alaa. Artificial intelligence (AI) cybersecurity dimensions: a comprehensive framework for understanding adversarial and offensive AI. **AI and Ethics**, 15 fev. 2024.

MALATJI, Masike; TOLAH, Alaa. Artificial intelligence (AI) cybersecurity dimensions: a comprehensive framework for understanding adversarial and offensive AI. **AI and Ethics**, v. 5, n. 2, p. 883–910, 1 abr. 2025.

MANADHATA, Pratyusa K.; WING, Jeannette M. An Attack Surface Metric. **IEEE Transactions on Software Engineering**, v. 37, n. 3, p. 371–386, maio 2011.

MANAGEMENT DIRECTORATE, DHS. **DHS Lexicon Terms and Definitions**. Department of Homeland Security, 16 out. 2017. Disponível em: https://www.dhs.gov/sites/default/files/publications/18_0116_MGMT_DHS-Lexicon.pdf.

MARTINS, Adriano. Fundamentos de computação nuvem para governos. *In*: **Amãpytuna Computação em Nuvem: Serviços livres para a sociedade do conhecimento**. Anais do Anais do II WCGE, Belo Horizonte, Brasil. Brasília: Fundação Alexandre de Gusmão, 2010.

MARTINS, Ronei Ximenes; FLORES, Vânia de Fátima. A implantação do Programa Nacional de Tecnologia Educacional (ProInfo): revelações de pesquisas realizadas no Brasil entre 2007 e 2011. **Revista Brasileira de Estudos Pedagógicos**, v. 96, p. 112–128, abr. 2015.

MAYMÍ, Fernando; HARRIS, Shon. **Cissp All-In-One Exam Guide**. 9th ed. ed. *[S.l.]*: McGraw-Hill Companies, *[S.d.]*.

MAZZUCATO, Mariana. **The Entrepreneurial State**. London: Penguin, 2018.

MAZZUCATO, Mariana; RYAN-COLLINS, Josh. Putting value creation back into "public value": from market-fixing to market-shaping. **Journal of Economic Policy Reform**, v. 25, n. 4, p. 345–360, 2 out. 2022.

MCGOWAN, Iverna. **United Nations Human Rights Chief Warns of the Dangers of Breaking Encryption & Mass Surveillance**. **Center for Democracy and Technology**, 16 set. 2022. Disponível em: https://cdt.org/insights/united-nations-human-rights-chief-warns-of-the-dangers-of-breaking-encryption-mass-surveillance/. Acesso em: 23 fev. 2024.

MCTI. **Estratégia Brasileira para a Transformação Digital**. Disponível em: https://www.gov.br/mcti/pt-br/acompanhe-o-mcti/transformacaodigital/estrategia-digital. Acesso em: 21 fev. 2024.

MEDEIROS, Breno Pauli *et al.* O uso do ciberespaço pela administração pública na pandemia da COVID-19: diagnósticos e vulnerabilidades. **Revista de Administração Pública; v. 54, n. 4 (2020): A resposta da administração pública brasileira aos desafios da pandemia**, 2020.

MEDEIROS, Breno Pauli. **Cyber power: challenges (and opportunities) for military power**. Tese de Doutorado – Rio de Janeiro, RJ: Escola de Comando e Estado-Maior do Exército – ECEME, 2024.

MEDEIROS, Breno Pauli; GOLDONI, Luiz Rogério Franco. A Trindade Conceitual Fundamental do Ciberespaço. **Contexto Internacional**, v. 42, p. 31–54, 17 jul. 2020.

MELL, Peter; GRANCE, Timothy. The NIST Definition of Cloud Computing. NIST Special Publication 800-145. n. National Institute of Standards and Technology, 2011.

MENEZES, Pablo Marques; CARDOSO, Lanay Marques; ROCHA, Fabio Gomes. Segurança em redes de computadores uma visão sobre o processo de Pentest. **Interfaces Científicas - Exatas e Tecnológicas**, v. 1, n. 2, p. 85–96, 28 maio 2015.

MGI. **Plano Nacional de Internet das Coisas**. Disponível em: https://www.gov.br/governodigital/pt-br/estrategias-e-governanca-digital/estrategias-e-politicas-digitais/plano-nacional-de-internet-das-coisas. Acesso em: 21 fev. 2024.

MICROSOFT. **Microsoft Digital Defense Report 2024**. Disponível em: https://www.microsoft.com/en-us/security/security-insider/intelligence-reports/microsoft-digital-defense-report-2024. Acesso em: 1 jul. 2025.

MICROSOFT SECURITY. **Zero Trust Model - Modern Security Architecture**. Disponível em: https://www.microsoft.com/en-us/security/business/zero-trust. Acesso em: 18 jan. 2024.

MINISTÉRIO DA DEFESA. **Glossário das Forças Armadas - MD35-G-01**, 2015. Disponível em: https://bdex.eb.mil.br/jspui/bitstream/123456789/141/1/MD35_G01.pdf. Acesso em: 14 maio 2024.

MINISTÉRIO DA DEFESA. **Doutrina Militar de Defesa Cibernética - MD31-M-07 (2ª Edição/2023)**, 16 out. 2023. Disponível em: https://www.gov.br/defesa/pt-br/assuntos/estado-maior-conjunto-das-forcas-armadas/doutrina-militar/publicacoes-1/publicacoes/MD31M07DoutrinaMilitardeDefesaCiberntica2Edio2023.pdf. Acesso em: 23 maio 2024.

MINISTRY OF FOREIGN AFFAIRS OF THE PRC. **International Strategy of Cooperation on Cyberspace**. Disponível em: https://www.

fmprc.gov.cn/mfa_eng/wjb_663304/zzjg_663340/jks_665232/kjlc_665236/qtwt_665250/201703/t20170301_599869.html. Acesso em: 5 jun. 2023.

MIRKOVIC, Jelena; REIHER, Peter. A taxonomy of DDoS attack and DDoS defense mechanisms. **ACM SIGCOMM Computer Communication Review**, v. 34, n. 2, p. 39–53, abr. 2004.

MOTA. **Cartilha da desinformação: como agem os grupos que usam redes sociais para espalhar fake news e mobilizar eleitores**. Disponível em: https://www.bbc.com/portuguese/articles/ceq55vxe9leo. Acesso em: 31 ago. 2024.

Moving the U.S. Government Toward Zero Trust Cybersecurity Principles. Disponível em: https://zerotrust.cyber.gov/federal-zero-trust-strategy/. Acesso em: 18 jan. 2024.

MUGGAH, Robert; THOMPSON, Nathan. **O problema do cibercrime no Brasil**. Disponível em: https://brasil.elpais.com/brasil/2015/10/23/opinion/1445558339_082466.html. Acesso em: 13 jun. 2024.

MURATA, Ana Maria Lumi Kamimura; TORRES, Paula Ritzmann. A convenção de Budapeste sobre os crimes cibernéticos foi promulgada, e agora? **A convenção de Budapeste sobre os crimes cibernéticos foi promulgada, e agora?**, v. 31, n. 368, 2023.

NARAINE, Ryan. **Stuxnet attackers used 4 Windows zero-day exploits**. Disponível em: https://www.zdnet.com/article/stuxnet-attackers-used-4-windows-zero-day-exploits/. Acesso em: 18 jan. 2024.

NATIONAL INITIATIVE FOR CYBERSECURITY CAREERS AND STUDIES (NICCS). **ResilienceGlossary of Common Cybersecurity Terminology**. *[S.l.: S.n.]*. Disponível em: https://niccs.cisa.gov/resources/glossary. Acesso em: 4 ago. 2025.

NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY; JOINT TASK FORCE INTERAGENCY WORKING GROUP. **Security and Privacy Controls for Information Systems and Organizations**. *[S.l.]*: National Institute of Standards and Technology, 23 set. 2020. Disponível em: https://

nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r5.pdf. Acesso em: 18 jan. 2024.

NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY (NIST). Cryptography. **NIST**, 30 jun. 2016.

NEIGEL, Alexis R. *et al.* Holistic cyber hygiene education: Accounting for the human factors. **Computers & Security**, v. 92, p. 101731, 1 maio 2020.

NIC.BR. **Internet Segura**. Disponível em: https://internetsegura.br/. Acesso em: 7 jul. 2025.

NICCS. **Vocabulary**. Disponível em: https://niccs.cisa.gov/cybersecurity-career-resources/vocabulary. Acesso em: 24 jan. 2024.

NISS, Oscar (ORG.). **Ciberdefensa y el ciclo evolutivo del ciberespacio**. Ciudad Autónoma de Bueno Aires: Universidad de la Defensa Nacional, 2023.

NORDVPN. **Cyber defense**. Disponível em: https://nordvpn.com/cybersecurity/glossary/cyber-defense/.

NORDVPN. **Attack surface definition**. **Glossary - NordVPN**, *[S.d.]*. Disponível em: https://nordvpn.com/pt-br/cybersecurity/glossary/attack-surface/. Acesso em: 18 jan. 2024b.

NORDVPN. **Zero day**. **Glossary - NordVPN**, *[S.d.]*. Disponível em: https://nordvpn.com/pt-br/cybersecurity/glossary/zero-day/.

NORTH, Douglass C. Institutions, Institutional Change and Economic Performance. **Cambridge Books**, 1991.

NYE, J. S. **O Futuro Do Poder**. Tradução: M. Lopes. *[S.l.]*: BENVIRA, 2012.

NYE, Joseph S. **Cyber Power**. Disponível em: https://www.belfercenter.org/publication/cyber-power. Acesso em: 15 jan. 2024.

NYGARD, K. E. *et al.* Dimensions of cybersecurity risk management. *In*: **Adv. in Cybersecur. Manag.** *[S.l.]*: Springer International Publishing, 2021. p. 369–395.

O que é a botnet Mirai? Disponível em: https://www.cloudflare.com/pt-br/learning/ddos/glossary/mirai-botnet/. Acesso em: 17 jan. 2024.

O que é malware? Veja significado, tipos e saiba remover. Disponível em: https://www.techtudo.com.br/listas/2021/03/o-que-e-malware-veja-significado-tipos-e-saiba-remover.ghtml. Acesso em: 19 fev. 2024.

O que são arquivos de log? – Explicação sobre arquivos de log – AWS. Disponível em: https://aws.amazon.com/pt/what-is/log-files/. Acesso em: 19 fev. 2024.

OECD. **Recomendação do Conselho sobre política regulatória e governança**. Paris: OECD Publishing, 1 nov. 2012. Disponível em: https://doi.org/10.1787/9789264209084-pt.. Acesso em: 14 set. 2024.

OECD. **OECD Regulatory Policy Outlook 2015**. Disponível em: https://www.oecd.org/en/publications/oecd-regulatory-policy-outlook-2015_9789264238770-en.html. Acesso em: 1 jul. 2025.

Orlando Silva: Nova Indústria Brasil, um passo estratégico para a reconstrução nacional. **CartaCapital**, 31 jan. 2024. Disponível em: https://www.cartacapital.com.br/opiniao/frente-ampla/nova-industria-brasil-um-passo-estrategico-para-a-reconstrucao-nacional/. Acesso em: 23 fev. 2024.

OTTIS, Rain; LORENTS, Peeter. **Cyberspace: Definition and Implications**. Disponível em: https://ccdcoe.org/library/publications/cyberspace-definition-and-implications/. Acesso em: 15 jan. 2024.

PAPAEVANGELOU, Charilaos. The existential stakes of platform governance: A critical literature review. **Open Research Europe**, v. 1, n. 31, 2021.

Papel do CISO em Negócios Digitais | Claranet. Disponível em: https://www.claranet.com/br/blog/papel-do-ciso-negocios-digitais. Acesso em: 29 jan. 2024.

PAWLAK, Patryk; EUROPEAN UNION INSTITUTE FOR SECURITY STUDIES. **Ten major take-away points**. Paris, France, 13 mar. 2014.

PAWLICKA, Aleksandra *et al*. Human-driven and human-centred cybersecurity: policy-making implications. **Transforming Government: People, Process and Policy**, v. 16, n. 4, p. 478–487, 5 ago. 2022.

PENNA, Caetano; MAZZUCATO, Mariana. **The Brazilian Innovation System: A Mission-Oriented Policy Proposal**: Temas Estratégicos para o Desenvolvimento do Brasil. Brasília, DF: CGEE, mar. 2016.

PEREIRA, Flavia Goulart. Os crimes econômicos na sociedade de risco. **Revista brasileira de ciências criminais**, n. 51, p. 105–131, 2004.

PEREZ, Carlota; SOETE, Luc. **Catching up in technology: entry barriers and windows of opportunity**. (Giovanni Dosi *et al.*, Orgs.)**Technical change and economic theory**: LEM Book Series.London & New YorkPinter Publishers, 1988. Disponível em: https://www.scopus.com/inward/record.uri?eid=2-s2.0-0025658854&partnerID=40&md5=883d69b8b1ea569e70b13a212b8f8354.

PETERS, B. Guy. Governance as political theory. **Critical policy studies**, v. 5, n. 1, p. 63–72, 2011.

PFAFF, C. Anthony. The Ethics of Acquiring Disruptive Military Technologies (Winter 2019/2020). 2020.

PHILL, Ross. **What Is A CISO? Their Role and Responsibilities Clearly Explained**. **UpGuard**, 30 nov. 2022. Disponível em: https://www.upguard.com/blog/what-is-a-ciso. Acesso em: 29 jan. 2024.

PICCONE, Ted. Democracy And DigitalTechnology. **Sur - International Journal on Human Rights**, v. 15, n. 27, p. 29–38, 2018.

PINILLA, Alexander. Resiliencia en la seguridad informática. **Universidad Piloto de Colombia**, 2015.

PINTO, Renata Ávila. **Digital Sovereignty or Digital Colonialism? New tensions of privacy, security and national policies. | EBSCOhost**. Disponível em: https://openurl.ebsco.com/contentitem/gcd:133035238?sid=ebsco:plink:crawler&id=ebsco:gcd:133035238. Acesso em: 11 mar. 2025.

PISA, Pedro. **O que é Hash?** Disponível em: https://www.techtudo.com.br/noticias/2012/07/o-que-e-hash.ghtml. Acesso em: 19 fev. 2024.

POHLE, Julia; THIEL, Thorsten. **Digital sovereignty**. info:eu-repo/semantics/article. Disponível em: https://policyreview.info/concepts/digital-sovereignty. Acesso em: 11 mar. 2025.

PRESIDÊNCIA DA REPÚBLICA. LEI Nº 9.394. Lei nº 9.394, de 20 de dezembro de 1996. Estabelece as diretrizes e bases da educação nacional. 20 dez. 1996.

PRESIDÊNCIA DA REPÚBLICA. **Decreto 3.505 - Institui a Política de Segurança da Informação nos órgãos e entidades da Administração Pública Federal.** Disponível em: https://www.planalto.gov.br/ccivil_03/decreto/d3505.htm. Acesso em: 13 jun. 2024.

PRESIDÊNCIA DA REPÚBLICA. LEI Nº 13.415. Lei Nº 13.415, de 16 de fevereiro de 2017. 16 fev. 2017.

PRESIDÊNCIA DA REPÚBLICA. **Decreto 9.573 - Aprova a Política Nacional de Segurança de Infraestruturas Críticas.** Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/decreto/D9573.htm. Acesso em: 13 jun. 2024a.

PRESIDÊNCIA DA REPÚBLICA. **Decreto 9.637 Institui a Política Nacional de Segurança da Informação**. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/decreto/d9637.htm. Acesso em: 13 jun. 2024b.

PRESIDÊNCIA DA REPÚBLICA. **Decreto Nº 10.046, de 9 de outubro de 2019**. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2019-2022/2019/decreto/D10046.htm. Acesso em: 8 jul. 2025.

PRESIDÊNCIA DA REPÚBLICA. **Lei nº 14.180, de 1º de Julho de 2021 - Institui a Política de Inovação Educação Conectada.** Disponível em: https://www.in.gov.br/en/web/dou/-/lei-n-14.180-de-1-de-julho-de-2021-329472130. Acesso em: 7 jul. 2025a.

PRESIDÊNCIA DA REPÚBLICA. **Resolução Nº 396 de 07/06/2021 - Institui a Estratégia Nacional de Segurança Cibernética do Poder Judiciário (ENSEC-PJ)**. Disponível em: https://atos.cnj.jus.br/atos/detalhar/3975. Acesso em: 15 jul. 2025b.

PRESIDÊNCIA DA REPÚBLICA. **RESOLUÇÃO CD/ANPD Nº 2, DE 27 DE JANEIRO DE 2022 - DOU - Imprensa Nacional**. Disponível em:

https://www.in.gov.br/en/web/dou/-/resolucao-cd/anpd-n-2-de-27-de-janeiro-de-2022-376562019. Acesso em: 8 jul. 2025a.

PRESIDÊNCIA DA REPÚBLICA. **DECRETO Nº 11.200, DE 15 DE SETEMBRO DE 2022 - Aprova a Plansic**. Disponível em: https://planalto.gov.br/ccivil_03/_ato2019-2022/2022/decreto/D11200.htm. Acesso em: 14 jul. 2025b.

PRESIDÊNCIA DA REPÚBLICA. **Lei nº 14.533 de 11/01/2023 - Política Nacional de Educação Digital**. Disponível em: https://normas.leg.br/?urn=urn:lex:br:federal:lei:2023-01-11;14533. Acesso em: 7 jul. 2025a.

PRESIDÊNCIA DA REPÚBLICA. **Decreto 11.856 -Institui a Política Nacional de Cibersegurança e o Comitê Nacional de Cibersegurança.** Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2023-2026/2023/decreto/D11856.htm. Acesso em: 13 jun. 2024b.

PRESIDÊNCIA DA REPÚBLICA. LEI Nº 14.945. Lei nº 14.945, de 31 de Julho de 2024. 31 jul. 2024.

PRETESH BISWAS. **ISO 27001:2022 A 5.16 Identity management**. **Pretesh Biswas**, 1 ago. 2023. Disponível em: https://preteshbiswas.com/2023/01/08/iso-270012022-a-5-16-identity-management/. Acesso em: 29 jan. 2024.

RAFFESTIN, Claude. **Por uma Geografia do Poder**. *[S.l.: S.n.]*. v. 29

RATTRAY, Gregory J. An Environmental Approach to Understanding Cyberpower. *In*: KRAMER, Franklin D.; STARR, Stuart H.; WENTZ, Larry K. (Orgs.). **Cyberpower and National Security**. *[S.l.]*: University of Nebraska Press, 2009. p. 253–274.

RIBEIRO, Florbela da Graça Jorge da Silva. **O tratamento de dados pessoais de clientes para marketing**. *[S.l.: S.n.]*.

RICHARD A. CLARKE; CLARKE, Richard A.; KNAKE, Robert K. Cyber War: The Next Threat to National Security and What to Do About It. 2 abr. 2010.

RID, Thomas. Cyber War Will Not Take Place. **Journal of Strategic Studies**, v. 35, n. 1, p. 5–32, fev. 2012.

RID, Thomas; BUCHANAN, Ben. Attributing Cyber Attacks. **Journal of Strategic Studies**, v. 38, n. 1–2, p. 4–37, 2 jan. 2015.

RID, Thomas; BUCHANAN, Ben. Hacking Democracy. **SAIS Review of International Affairs**, v. 38, n. 1, p. 3–16, 2018.

RIKAP, Cecilia. Amazon: A story of accumulation through intellectual rentiership and predation. **Competition & Change**, v. 26, n. 3–4, p. 436–466, 1 jul. 2022.

RIKAP, Cecilia. The expansionary strategies of intellectual monopolies: Google and the digitalization of healthcare. **Economy and Society**, v. 52, n. 1, p. 110–136, 2 jan. 2023a.

RIKAP, Cecilia. Intellectual monopolies as a new pattern of innovation and technological regime. **Industrial and Corporate Change**, p. dtad077, 7 dez. 2023b.

RIKAP, Cecilia; LUNDVALL, Bengt-Åke. **The Digital Innovation Race: Conceptualizing the Emerging New World Order**. Cham: Springer International Publishing, 2021.

RIKAP, Cecilia; LUNDVALL, Bengt-Åke. Big tech, knowledge predation and the implications for development. **Innovation and Development**, v. 12, n. 3, p. 389–416, 2 set. 2022.

RNP. **Hackers do Bem seleciona grupos de trabalho para impulsionar a formação em cibersegurança no Brasil**. **RNP**, 31 out. 2024. Disponível em: https://www.rnp.br/pesquisa-e-desenvolvimento/hackers-do-bem-seleciona-grupos-de-trabalho-para-impulsionar-a-formacao-em-ciberseguranca-no-brasil/. Acesso em: 15 jul. 2025.

ROCHA, Bruno Carneiro da. **Prevenindo ameaças persistentes avançadas em redes corporativas utilizando um modelo de segurança baseado em zero trust e UEBA**. Brasília: Universidade de Brasília, 15 ago. 2023.

RODOTÀ, Stefano *et al. In*: **A vida na sociedade da vigilância: a privacidade hoje**. *[S.l.: S.n.]*.

RODRIK, Dani. **Industrial Policy for the Twenty-First Century**. Rochester, NYSocial Science Research Network, 1 nov. 2004. Disponível em: https://papers.ssrn.com/abstract=617544. Acesso em: 1 jul. 2025.

ROSE, Scott *et al.* **Zero Trust Architecture**. *[S.l.]*: National Institute of Standards and Technology, 11 ago. 2020. Disponível em: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-207.pdf. Acesso em: 18 jan. 2024.

ROSS, Ron *et al.* **Developing cyber-resilient systems: a systems security engineering approach**. Gaithersburg, MD: National Institute of Standards and Technology (U.S.), 8 dez. 2021. Disponível em: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-160v2r1.pdf. Acesso em: 18 jan. 2024.

RUIZ, Evandro Eduardo Seron. **All we need is log?** Disponível em: https://www.migalhas.com.br/coluna/migalhas-de-protecao-de-dados/378373/all-we-need-is-log. Acesso em: 19 fev. 2024.

RUPP, Isadora. **Como ressoa a invasão dos Três Poderes dois anos depois**. Disponível em: https://www.nexojornal.com.br/expresso/2025/01/07/stf-8-de-janeiro-invasao-tres-poderes-2023. Acesso em: 30 jun. 2025.

SALINAS, Natasha Schmitt Caccia. A INTERVENÇÃO DO CONGRESSO NACIONAL NA AUTONOMIA DAS AGÊNCIAS REGULADORAS. **REI - REVISTA ESTUDOS INSTITUCIONAIS**, v. 5, n. 2, p. 586–614, 6 out. 2019.

SANDBERG, Simen Espeseth. **Endpoint security in the modern enterprise**. Dissertação de mestrado - *[S.l.: S.n.]*.

SANGER, David E. Confront and Conceal: Obama's Secret Wars and Surprising Use of American Power. 5 jun. 2012.

SANTANA, Fausta Joaquina Clarinda de. **A SEGURANÇA DA INFORMAÇÃO NA CIÊNCIA DA INFORMAÇÃO NO BRASIL**. Tese de doutorado—Salvador: *[S.n.]*.

SANTOS, Milton. **A Natureza do Espaço: Técnica e Tempo, Razão e Emoção**. *[S.l.]*: EDUSP, 2022.

SAUAIA, Hugo Moreira Lima. **A proteção dos dados pessoais no Brasil.** *[S.l.]*: Lumen Juris, 2018.

SCHENDES, William. **Prefeitura do Rio de Janeiro sofre ataque hacker; serviços ficam indisponíveis**. **Olhar Digital**, 16 ago. 2022. Disponível em: https://olhardigital.com.br/2022/08/16/seguranca/prefeitura-rio-de-janeiro-ataque-hacker-servicos/. Acesso em: 13 jun. 2024

SCHULTZ, Richard. The Political Economy of Regulation: Creating, Designing and Removing Regulatory FormsBarry M. Mitnick New York: Columbia University Press, 1980, pp. xxv, 506-Industry Influence in Federal Regulatory AgenciesPaul J. Quirk Princeton: Princeton University Press, 1981, pp. xi, 260-Canadian Regulatory AgenciesC. Lloyd Brown-John Toronto: Butterworths, 1981, pp. ix, 268. **Canadian Journal of Political Science/Revue canadienne de science politique**, v. 15, n. 3, p. 624–628, 1982.

SECURITY REPORT. **Painel de incidentes cibernéticos 2021**. Disponível em: https://www.securityreport.com.br/email/InfoSR2021_Jan_a_dez.html. Acesso em: 8 fev. 2024.

SECURITY REPORT. **Painel de incidentes cibernéticos 2022**. Disponível em: https://www.securityreport.com.br/email/InfoSR2022_.html. Acesso em: 8 fev. 2024.

SECURITY REPORT. **Painel de incidentes cibernéticos 2023**. Disponível em: https://www.securityreport.com.br/email/InfoSR2023.html. Acesso em: 8 fev. 2024.

SEKOIA. **ISAC**. **Sekoia.io**, 2025. Disponível em: https://www.sekoia.io/en/glossary/what-is-an-isac/. Acesso em: 24 jun. 2025.

SELZNICK, Philip. Focusing organizational research on regulation. **Regulatory policy and the social sciences**, v. 1, n. 1, p. 363–367, 1985.

SHELDON, John B. Geopolitics and Cyber Power: Why Geography Still Matters. **American Foreign Policy Interests**, v. 36, n. 5, p. 286–293, 3 nov. 2014.

Shifting the Balance of Cybersecurity Risk: Principles and Approaches for Security-by-Design and -Default. *[S.d.]*.

SILVA SANCHEZ, Jesus-Maria. **expansão do direito penal – aspectos de política criminal nas sociedades pós-industriais**. São Paulo: RT - Revista dos Tribunais, 2007.

SILVA SÁNCHEZ, Jésus-Maria. **A expansão do direito penal: aspectos da política criminal nas sociedades pós-industriais**. 3. ed. São Paulo: Revista dos Tribunais, 2013.

SINGH, Deshraj. Cybersecurity and Human Rights: A Complex Interplay. **International Journal of Science and Research (IJSR)**, v. 12, n. 6, p. 1110–1112, 5 jun. 2023.

SMYTH, Sandra. **Penetration Testing and Legacy Systems**. arXiv, 2024. Disponível em: https://arxiv.org/abs/2402.10217. Acesso em: 4 ago. 2025.

SOLAR, Carlos. Cybersecurity and cyber defence in the emerging democracies. **Journal of Cyber Policy**, v. 5, n. 3, p. 392–412, 1 set. 2020.

SONTAN, Adewale Daniel; SAMUEL, Segun Victor. The intersection of Artificial Intelligence and cybersecurity: Challenges and opportunities. **World Journal of Advanced Research and Reviews**, v. 21, n. 2, p. 1720–1736, 2024.

SOUPPAYA, Murugiah P.; SCARFONE, Karen A. **Guide to Enterprise Telework, Remote Access, and Bring Your Own Device (BYOD) Security**. *[S.l.]*: National Institute of Standards and Technology, jul. 2016. Disponível em: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-46r2.pdf. Acesso em: 29 jan. 2024.

SOUSA, Flávio R. C. Computação em Nuvem: Conceitos, Tecnologias, Aplicações e Desafios 1 2. p. 150–175, 2009.

SOUZA, Raquel Aparecida; SILVA, Marcelo Soares Pereira da. Política de Inovação Educação Conectada: Universalização do acesso à internet e uso pedagógico de tecnologias. **Revista Ibero-Americana de Estudos em Educação**, p. e023060–e023060, 7 set. 2023.

SRNICEK, Nick. **Platform Capitalism**. London: polity, 2017.

STIGLER, George J. The Theory of Economic Regulation. **The Bell Journal of Economics and Management Science**, v. 2, n. 1, p. 3, 1971.

STIGLITZ, Joseph E. **Globalization and its discontents revisited: anti-globalization in the era of Trump**. New York, NY: W.W. Norton & Company, 2018.

STONE, John. Cyber War Will Take Place! **Journal of Strategic Studies**, v. 36, n. 1, p. 101–108, 1 fev. 2013.

STRUPCZEWSKI, Grzegorz. Defining cyber risk. **Safety Science**, v. 135, 1 mar. 2021.

SWALLOW, Robert Chandler. Considering the cost of cyber warfare: advancing cyber warfare analytics to better assess tradeoffs in system destruction warfare. **The Journal of Defense Modeling and Simulation**, v. 20, n. 1, p. 3–37, 2023.

SYDOW, Spencer Toth. **Curso de direito penal informático: partes geral e especial, processo penal informático e cibercriminologia**. 5. ed. São Paulo: Tirant lo Blanch, 2024.

SZAPIRO, Marina; CASSIOLATO, José Eduardo. **Estado e novas políticas de desenvolvimento produtivo e inovativo no século XXI**: A dinâmica global de produção e inovação e o papel do território e dos Estados nacionais. Rio de Janeiro: Instituto de Economia da UFRJ; Fiocruz; Redesist, dez. 2021.

TALESH, Shauhin; GONÇALVES, Péricles. Surety bond and the role of insurance companies as regulators in the context of brazilian infrastructure projects. **Revista de Direito Administrativo**, v. 282, n. 1, p. 63–107, 23 mar. 2023.

TECMUNDO. **Empresas brasileiras foram alvo de 356 bilhões de tentativas de ataques cibernéticos em 2024**. Disponível em: https://www.tecmundo.com.br/seguranca/403005-empresas-brasileiras-foram-alvo-de-356-bilhoes-de-tentativas-de-ataques-ciberneticos-em-2024.htm. Acesso em: 4 ago. 2025.

THE ECONOMIST. Why is Brazil a hotspot for financial crime? **The Economist**, jan. 2024.

THE MINISTRY OF FOREIGN AFFAIRS OF THE RUSSIAN FEDERATION. **[2016]_Doctrine of Information Security of the**

Russian Federation - Министерство иностранных дел Российской Федерации.pdf. 2016.

THE STATE COUNCIL INFORMATION OFFICE OF THE PEOPLE'S REPUBLIC OF CHINA. **Jointly Build a Community with a Shared Future in Cyberspace**. Disponível em: http://english.www.gov.cn/archive/whitepaper/202211/07/content_WS636894aac6d0a757729e2973.html. Acesso em: 23 maio 2023.

URBANOVICS, Anna. Cybersecurity Policy-Related Developments in Latin America. **AARMS – Academic and Applied Research in Military and Public Management Science**, v. 21, n. 1, p. 79–94, 9 nov. 2022.

US G.A.O. **Weapons systems cybersecurity: DoD just beginning to grapple with scale of vulnerabilities**. Washington, DC: U.S. Government Accountability Office, out. 2018. Disponível em: https://www.gao.gov/assets/gao-19-128.pdf. Acesso em: 18 jan. 2024.

VAN DEN BERG, Jan. A Basic Set of Mental Models for Understanding and Dealing with the Cyber-Security Challenges of Today. **Journal of Information Warfare**, v. 19, n. 1, p. 26–47, 2020.

VARGAS, Mateus; RODRIGUES, Eduardo. **Ministério da Saúde sofre nova invasão de 'hacker sincero': 'Arrumem esse site porco'**. Disponível em: https://www.estadao.com.br/saude/ministerio-da-saude-sofre-nova-invasao-de-hacker-sincero-arrumem-esse-site-porco/. Acesso em: 13 jun. 2024.

VEALE, M.; BROWN, I. Cybersecurity. **Internet Policy Review**, v. 9, n. 4, p. 1–22, 2020.

VERDI, Fábio Luciano; ROTHENBERG, Christian Esteve; PASQUINI, Rafael. Novas Arquiteturas de Data Center para Cloud Computing. *In*: *[S.l.]*: Minicursos do XXVIII SBRC, 2010. p. 103–152.

VERIZON. **2025 Data Breach Investigations Report**. Disponível em: https://www.verizon.com/business/resources/reports/dbir/. Acesso em: 1 jul. 2025.

VIANNA, Túlio Lima. **Fundamentos de direito penal informático: do acesso não autorizado a sistemas computacionais**. 1. ed. Rio de Janeiro: Forense, 2003.

VISHWANATH, Arun *et al.* Cyber hygiene: The concept, its measure, and its initial tests. **Decision Support Systems**, v. 128, p. 113160, 1 jan. 2020.

VITAL, Fernanda Valente, Danilo. **STJ sofre ataque hacker e suspende prazos até segunda (9/11)**. **Consultor Jurídico**, 4 nov. 2020. Disponível em: https://www.conjur.com.br/2020-nov-04/stj-sofre-ataque-hacker-suspende-prazos-segunda-911/. Acesso em: 25 jun. 2025.

VOO, Julia; HEMANI, Irfan; CASSIDY, Daniel. National Cyber Power Index 2022. **Cyber Power**, 2022.

WADE, Robert H. Return of industrial policy? **International Review of Applied Economics**, v. 26, n. 2, p. 223–239, mar. 2012.

WALT, Stephen M. **The Hell of Good Intentions**. Disponível em: https://us.macmillan.com/books/9780374712464/thehellofgoodintentions. Acesso em: 2 fev. 2024.

WEST, Sarah Myers. Data Capitalism: Redefining the Logics of Surveillance and Privacy. **Business & Society**, v. 58, n. 1, p. 20–41, 1 jan. 2019.

What Is a CISO? Chief Information Security Officer. Disponível em: https://www.cisco.com/c/en/us/products/security/what-is-ciso.html. Acesso em: 29 jan. 2024.

What is an Advanced Persistent Threats (APT). Disponível em: https://www.vmware.com/topics/glossary/content/advanced-persistent-threats.html. Acesso em: 29 jan. 2024.

What is Ethical Hacking? | IBM. Disponível em: https://www.ibm.com/topics/ethical-hacking. Acesso em: 17 jan. 2024.

What is Ethical Hacking | Who is an Ethical Hacker. Disponível em: https://www.malwarebytes.com/cybersecurity/basics/what-is-ethical-hacking. Acesso em: 17 jan. 2024.

WHEELER, David A.; LARSEN, Gregory N. **Techniques for Cyber Attack Attribution:** Fort Belvoir, VA: Defense Technical Information Center, 1 out. 2003. Disponível em: http://www.dtic.mil/docs/citations/ADA468859. Acesso em: 15 jan. 2024.

WHITE HOUSE. **WHITE HOUSE. The National Cybersecurity Strategy of the United States of America. Mar. de 2023.** mar. 2023. Disponível em: https://www.whitehouse.gov/wp-content/uploads/2023/03/National-Cybersecurity-Strategy-2023.pdf. Acesso em: 20 ago. 2023.

WIRTZ, James J. Life in the "Gray Zone": observations for contemporary strategists. **Defense & Security Analysis**, v. 33, n. 2, p. 106–114, 3 abr. 2017.

WOLFF, Josephine. What we talk about when we talk about cybersecurity: security in internet governance debates. **Internet Policy Review**, v. 5, n. 3, 30 set. 2016.

ZUBOFF, Shoshana. **The Age of Surveillance Capitalism**. London: Profile Books, 2019a.

ZUBOFF, Shoshana. Surveillance Capitalism and the Challenge of Collective Action. **New labor forum**, v. 28, n. 1, p. 10–29, 2019b.

Normas que formam o *corpus* documental estudado

Agência Nacional de Águas e Saneamento Básico (ANA). Resolução nº 253, de 2025.

Agência Nacional de Aviação Civil (ANAC). Instrução Normativa nº 128, de 2018. Alterada pela Instrução Normativa nº 173, de 2021.

Agência Nacional de Aviação Civil (ANAC). Resolução nº 458, de 2017.

Agência Nacional de Aviação Civil (ANAC). Regulamento Brasileiro da Aviação Civil – RBAC nº 108.

Agência Nacional de Telecomunicações (ANATEL). Resolução nº 17, de 2021.

Agência Nacional de Telecomunicações (ANATEL). Resolução nº 740, de 2020.

Agência Nacional de Telecomunicações (ANATEL). Resolução nº 767, de 2024.

Agência Nacional do Cinema (ANCINE). Portaria nº 589-E, de 2022.

Agência Nacional do Cinema (ANCINE). Instrução Normativa nº 123, de 2015.

Agência Nacional de Energia Elétrica (ANEEL). Resolução nº 6.143, de 2019.

Agência Nacional de Energia Elétrica (ANEEL). Resolução nº 964, de 2021.

Agência Nacional de Mineração (ANM). Resolução nº 206, de 2025.

Agência Nacional do Petróleo, Gás Natural e Biocombustíveis (ANP). Portaria nº 102.

Agência Nacional do Petróleo, Gás Natural e Biocombustíveis (ANP). Manual de Comunicação de Incidentes. Rio de Janeiro, 2024.

Agência Nacional de Saúde Suplementar (ANS). Resolução nº 62, de 2015. Alterada pela Resolução nº 81, de 2023.

Agência Nacional de Saúde Suplementar (ANS). Resolução Normativa nº 501, de 2022.

Agência Nacional de Saúde Suplementar (ANS). Resolução Normativa nº 443, de 2019.

Agência Nacional de Saúde Suplementar (ANS). Padrão TISS.

Agência Nacional de Transportes Aquaviários (ANTAQ). Portaria nº 423, de 2022.

Agência Nacional de Transportes Aquaviários (ANTAQ). Resolução CONPORTOS nº 53, de 2020.

Agência Nacional de Transportes Aquaviários (ANTAQ). Minuta PSP.

Agência Nacional de Transportes Terrestres (ANTT). Resolução nº 6.029, de 2023.

Agência Nacional de Transportes Terrestres (ANTT). Resolução nº 6.045, de 2024.

Agência Nacional de Vigilância Sanitária (ANVISA). Portaria nº 1.440, de 2018. Alterada pela Portaria nº 72, de 2023.

Agência Nacional de Vigilância Sanitária (ANVISA). Resolução RDC nº 654, de 2022.

Agência Nacional de Vigilância Sanitária (ANVISA). Resolução RDC nº 657, de 2022.

Agência Nacional de Vigilância Sanitária (ANVISA). Resolução RDC nº 848, de 2024.

Agência Nacional de Vigilância Sanitária (ANVISA). Instrução Normativa nº 134, de 2022.

Agência Nacional de Proteção de Dados (ANPD). Resolução nº 15, de 2024.

Agência Nacional de Proteção de Dados (ANPD). Guia de Segurança da Informação para Agentes de Tratamento de Pequeno Porte – versão 1.0, 2024.

Banco Central do Brasil (BCB). Resolução nº 115, de 2021. Alterada pela Resolução nº 287, de 2023.

Banco Central do Brasil (BCB). Resolução nº 4.893, de 2021.

Banco Central do Brasil (BCB). Resolução nº 454, de 2025.

Comissão de Valores Mobiliários (CVM). Portaria nº 155, de 2021.

Comissão de Valores Mobiliários (CVM). Instrução nº 35, de 2021. Alterada pelas Instruções nº 134, de 2022, e nº 179, de 2023.

Superintendência de Seguros Privados (SUSEP). Resolução nº 45, de 2024.

Superintendência de Seguros Privados (SUSEP). Circular nº 638, de 2021.

Comissão Nacional de Energia Nuclear (CNEN). Portaria nº 11, de 2021.

Ministério da Educação (MEC). Portaria nº 495, de 2022.

Superintendência Nacional de Previdência Complementar (PREVIC). Portaria nº 295, de 2023.

Secretaria de Prêmios e Apostas do Ministério da Fazenda. Portaria SPA/MF nº 722, de 2024.

Conheça melhor a editora Lumen Juris

www.lumenjuris.com.br
@lumenjuriseditora
publique@lumenjuris.com.br

A cibersegurança consolidou-se como tema crucial, na medida em que a crescente digitalização da vida cotidiana expõe indivíduos, empresas, organizações e o próprio Estado a crescentes riscos cibernéticos de diferentes naturezas. Este livro propõe uma análise sistemática da matéria, partindo da conceituação de cibersegurança como um conjunto de iniciativas voltadas à proteção de objetos de referência — pessoas e ativos digitais — diante de ameaças que podem gerar impactos em múltiplos níveis, do individual ao nacional. Ao examinar os elementos constitutivos e as diferentes dimensões – regulatória, técnica, pedagógica e desenvolvimentista – da cibersegurança, a obra oferece ao leitor um quadro teórico-metodológico capaz de sustentar reflexões jurídicas e institucionais mais amplas.

A ausência de mecanismos de governança eficazes voltados à comunicação, coordenação e cooperação na prevenção e mitigação de riscos cibernéticos pode atrapalhar enormemente a efetividade dos esforços voltados a evitar incidentes que podem ter consideráveis repercussões econômicas, sociais e políticas. Interessando desde pequenos empreendimentos até serviços essenciais como energia elétrica e infraestrutura financeira, as ciberameaças já são consideradas entre os riscos com maior impacto econômico, político e social.

Nesse contexto, a presente obra busca não apenas sistematizar conceitos e categorias analíticas, mas também destacar caminhos para construir uma governança da cibersegurança no Brasil, e alavancar tal governança para fortalecer a soberania digital brasileira. Este volume convida o leitor a compreender a conexão entre a dimensão conceitual, normativa, tecnológica e operacional da cibersegurança e a necessidade de políticas públicas, práticas organizacionais e marcos regulatórios capazes de responder aos enormes desafios do ambiente digital contemporâneo.

ISBN 978-85-519-3792-1

FGV DIREITO RIO

Lumen Juris Direito | 35 anos

9 788551 937921 >