



Luca Belli
Bruna Franqueira
Erica Bakonyi
Larissa Chen
Natalia Couto
Sofia Chang
Nina da Hora
Walter B. Gaspar

**CIBERSEGURANÇA:
UMA VISÃO SISTÊMICA
RUMO A UMA PROPOSTA
DE MARCO REGULATÓRIO
PARA UM BRASIL
DIGITALMENTE SOBERANO**

Cibersegurança: uma visão sistêmica rumo a uma proposta de Marco Regulatório para um Brasil digitalmente soberano

Luca Belli, Bruna Franqueira, Erica Bakonyi, Larissa Chen, Natalia Couto, Sofia Chang, Nina da Hora e
Walter B. Gaspar

O conteúdo, resultados e conclusões deste estudo são de responsabilidade da/os autora/es e não representam, de qualquer maneira, a posição institucional da Fundação Getúlio Vargas.

Edição produzida pela FGV Direito Rio
Praia de Botafogo, 190 | 13º andar
Rio de Janeiro | RJ | Brasil | CEP: 22250-900
55 (21) 3799-5445
www.fgv.br/diretorio

**Cibersegurança: uma visão sistêmica rumo a
uma proposta de Marco Regulatório para um
Brasil digitalmente soberano**

Luca Belli, Bruna Franqueira, Erica Bakonyi, Larissa
Chen, Natalia Couto, Sofia Chang, Nina da Hora e
Walter B. Gaspar

EDIÇÃO FGV Direito Rio

Obra Licenciada em Creative Commons

Atribuição - Uso Não Comercial - Não a Obras Derivadas



Impresso no Brasil

Fechamento da 1ª edição em agosto de 2023

Este livro foi aprovado pelo Conselho Editorial da FGV Direito Rio, e consta na Divisão de Depósito Legal da Biblioteca Nacional.

Os conceitos emitidos neste livro são de inteira responsabilidade dos autores.

Coordenação: Ludmilla Totinick e Christian Dannel

Estagiária: Gabriela Carioca

Capa: Andreza Moreira - Tangente Design

Diagramação: Andreza Moreira - Tangente Design

Dados Internacionais de Catalogação na Publicação (CIP)
Ficha catalográfica elaborada pelo Sistema de Bibliotecas/FGV

Cibersegurança [recurso eletrônico] : uma visão sistêmica rumo a uma proposta de marco regulatório para um Brasil digitalmente soberano / Luca Belli... [et al.]. - Rio de Janeiro : FGV Direito Rio, 2023.

118 p.

Inclui bibliografia.

ISBN 978-65-00-72715-9

1. Cibernética. 2. Computadores - Medidas de segurança. 3. Proteção de dados. 4. Crime por computador - Prevenção. I. Belli, Luca. II. Escola de Direito do Rio de Janeiro da Fundação Getulio Vargas. Ramos, Bruno de Souza. III. Fundação Getulio Vargas. IV. Título.

CDD - 364.168

Elaborada por Márcia Nunes Bacha - CRB-7/4403

SUMÁRIO

SOBRE OS AUTORES	7
SUMÁRIO EXECUTIVO	9
1 INTRODUÇÃO	15
1.1 Cibersegurança: uma visão sistêmica	17
1.2 Ataques e ameaças cibernéticas e vulnerabilidades exploradas	24
1.3 O impacto da Inteligência Artificial na cibersegurança e da cibersegurança na Inteligência artificial	36
1.3.1 Inteligência artificial como facilitador de ciberataques	39
1.4 Caráter tipicamente internacional e multidimensional	41
1.4.1 Uma perspectiva multidimensional e multissetorial	42
1.4.2 Uma perspectiva Internacional	45
2 SOBERANIA DIGITAL E CIBERSEGURANÇA	51
2.1 Como nasceu e como se popularizou o conceito de soberania digital? ..	52
2.2 Quais são os elementos fundamentais da soberania digital?	54
2.2.1 A necessária modernização da política educacional para um país digitalmente soberano	60
2.2.2 A conexão entre soberania digital e Inteligência artificial	64
2.3 Qual é a conexão entre soberania digital e cibersegurança	66
3 CIBERSEGURANÇA NO BRASIL: MAPEAMENTO E ANÁLISE CRÍTICA DO ARCABOUÇO NORMATIVO VIGENTE	69
3.1 Críticas gerais acerca das principais bases normativas federais	74
3.2 Medidas de cooperação internacional e de homogeneização de práticas	78
3.2.1 Normas e padrões internacionalmente reconhecidos como referências	78
3.2.2 Seguro cibernético	84
3.3 Convenção de Budapeste	88
4 CONCLUSÃO: UMA PROPOSTA DE MARCO DE CIBERSEGURANÇA E SOBERANIA DIGITAL	91
4.1 Proposta de Marco de Cibersegurança e Soberania Digital	92
BIBLIOGRAFIA	109

SOBRE OS AUTORES

Luca Belli, PhD, é Professor da FGV Direito Rio, onde coordena o Centro de Tecnologia e Sociedade da FGV (www.cts.fgv.br) e o projeto CyberBRICS (www.cyberbrics.info). Autor de mais de 50 publicações sobre regulação de Internet e políticas digitais, Luca é membro do Board da Alliance for Affordable Internet, Editor do International Data Privacy Law Journal da Oxford University Press, e Diretor da conferência CPDP LatAm, Computers Privacy and Data Protection Latin America (www.cpdp.lat). Luca é doutor (PhD) em direito público pela Université Panthéon-Assas, Paris 2.

Bruna Franqueira é mestre em Teoria do Estado e Direito Constitucional pela PUC-Rio. Graduiu-se na FGV Direito Rio em 2020. É Pesquisadora do Centro de Tecnologia e Sociedade da FGV e advogada na Bioni Consultoria, onde atua com temas de proteção de dados pessoais e direito digital.

Erica Bakonyi é mestre em Direito pela Universidade de Coimbra, possui MBA em “Gestão da Segurança da Informação” e especialização lato sensu em “Licitações e contratos administrativos”. É advogada e atua na área de privacidade e proteção de dados como consultora em projetos de adequação legislativa em empresas e DPO-as-a-service. É pesquisadora do Centro de Tecnologia e Sociedade, da FGV Direito Rio, atualmente no projeto “CyberBRICS”. Mentora na área de privacidade e proteção de dados na Associação Brasileira de Lawtechs e Legaltechs (AB2L), organizadora do LEGAL HACKERS, capítulo do Rio de Janeiro, e co-coordenadora do MyData BR.

Larissa Chen Yi Qian é pesquisadora do Centro de Tecnologia e Sociedade da FGV e participa do Projeto CyberBRICS. Possui pós-graduação em Direito Digital no Instituto de Tecnologia e Sociedade em parceria com a Universidade do Estado de Rio de Janeiro, e graduação no Instituto Brasileiro de Mercado de Capitais (Ibmec). Tradutora do Código Civil Chinês e é advogada inscrita na OAB/RJ.

Natália Couto é doutoranda e mestre em direito da regulação pela FGV/Direito Rio. Pesquisadora assistente do Centro de Tecnologia e Sociedade. Professora convidada da FGV/Direito Rio na disciplina “Regulação de Redes Sociais”. Participou do LLM Direito, Inovação e Tecnologia como assistente de ensino na FGV/Direito Rio.

Sofia Chang é mestra em Direito Transnacional pela Universidade de Pequim. É pesquisadora do Centro de Tecnologia e Sociedade no projeto CyberBRICS da FGV Direito Rio, advogada, e atua na área de proteção de dados e privacidade no mercado financeiro.

Nina da Hora se identifica como hackerantirracista, é Cientista da Computação pela PUC-Rio e pesquisa Justiça e Ética em IA. Colunista do MIT Technology Review Brasil. Pesquisadora do CTS/FGV-Rio. Faz parte do Tik Tok Brasil Security Advisory Board, onde colabora com discussões sobre temas como políticas de conteúdo, estratégias de segurança e lançamentos de produtos e também do conselho de IA Responsável da Chatham House. Também vem atuando nas frentes de tecnologias e direitos digitais no Governo. Em 2022, participou do conselho de transparência para as eleições de 2022, fez parte da equipe do grupo de transição do governo e hoje faz parte do conselho de desenvolvimento econômico e social da presidência.

Walter B. Gaspar é Advogado, Mestre em Saúde Coletiva pelo Instituto de Medicina Social da UERJ e estudante de doutorado do Programa de Políticas Públicas, Estratégias e Desenvolvimento do IE-UFRJ. Pesquisador do CTS-FGV, Diretor Executivo da CPDP LatAm (<https://cpdp.lat/>), membro do Comitê de Programação do *OpenForum Academy Symposium*, autor de publicações que exploram regulação e políticas em propriedade intelectual, tecnologia e inovação e sua relação com privacidade e proteção de dados, cibersegurança e desenvolvimento.

SUMÁRIO EXECUTIVO

SEGURANÇA SISTÊMICA E MULTIDIMENSIONAL

Este trabalho destaca que a cibersegurança é um assunto necessariamente multidimensional, multissetorial e, frequentemente, transnacional. Tal natureza é evidente, considerando que a elaboração e implementação de conceitos, estratégias, normas, ferramentas e mecanismos de governança de cibersegurança depende de atores de natureza extremamente diferente – pública, privada, associativa etc. – que não são necessariamente localizados na mesma jurisdição. Ao mesmo tempo, ciberataques implicam frequentemente atores de natureza diferente localizados em várias jurisdições, tornando a cooperação internacional uma necessidade não somente para conseguir respostas apropriadas aos ciberataques, mas, ainda mais basicamente, para conseguir um nível de certeza adequado na atribuição mesma dos ataques.

Em poucas palavras, **a cibersegurança é o conjunto de normas, práticas e processos que permitem proteger sistemas críticos, informações particularmente importantes, e sobretudo pessoas de potenciais riscos e ameaças cibernéticas.** Propõe-se uma visão sistêmica do cenário de cibersegurança brasileiro para a construção de políticas públicas nesta área. Esta visão passa pelo reconhecimento das seguintes premissas, tanto em análise quanto na prática:

- A segurança de sistemas digitais representa, atualmente, elemento basilar para o funcionamento de processos econômicos, políticos e sociais e o provimento de serviços públicos e privados;
- A cibersegurança é um assunto multidimensional que necessita a adoção de uma visão sistêmica, reconhecendo a complexa rede de atores e instituições envolvidos no tema e o importante papel da participação multissetorial na definição de normas, padrões e políticas;
- As dimensões da segurança de dados (pessoais e não pessoais), segurança de infraestruturas críticas, segurança de processos democráticos, e segurança de indivíduos são linhas-guias para a análise e o debate acerca de cibersegurança a partir de uma perspectiva que reconheça a sua complexidade;

- O quadro normativo e estratégico construído deverá estar a serviço de uma visão de país que posicione o Brasil como ator global em fluxos tecnológicos, bem como a uma visão fundamentada em direitos individuais exercidos nos meios digitais.

As consequências das ameaças e riscos cibernéticos fluem pelas diferentes dimensões da sociedade, podendo ocasionar efeitos sociais devastadores e comprometer o acesso às infraestruturas críticas do país. Assim, a construção de Estratégias Nacionais de Cibersegurança e os Marcos de Cibersegurança e Soberania Digital requer fundamentação sistêmica e coordenada que promova a cooperação entre os diferentes agentes dentro da sociedade Brasileira e seja capaz de diálogo internacional.

FUNDAMENTOS PARA UMA VISÃO SISTÊMICA DA CIBERSEGURANÇA

Devido à transversalidade do tema, é necessário que o Brasil desenvolva (i) políticas públicas de incentivo aos diferentes atores da sociedade (públicos, privados, acadêmicos, entidades civis); (ii) estabeleça uma Agência Nacional de Cibersegurança (ANC); e (iii) estabeleça um Comitê Multissetorial de Cibersegurança e uma Rede Nacional de Cibersegurança como órgãos dentro da estrutura da ANC, responsáveis pelo diálogo multissetorial, o desenvolvimento e a implementação de soluções de cibersegurança.

A visão adotada deve superar uma fundamentação da cibersegurança baseada exclusivamente na capacidade militar, na ciberdefesa, ou segurança nacional, estimulando o desenvolvimento da capacidade cibernética. Para tanto, é imprescindível o investimento em políticas públicas de incentivo e apoio financeiro à pesquisa e inovação, alinhando a política de cibersegurança às necessidades do Brasil para a construção de um sistema de inovação estratégico, autônomo e direcionado ao seu povo.

Este trabalho destaca também a necessidade de se colocar os indivíduos ao centro de qualquer abordagem de cibersegurança. Tal elemento parece uma evidência, mas, de fato acaba sendo omisso pela enorme maioria das abordagens existentes, que se concentram principalmente na segurança de sistemas

computacionais e dados, esquecendo de destacar o papel central das pessoas.

A soberania digital, outro eixo basilar para a perspectiva proposta, refere-se à capacidade de uma dada entidade de exercer agência, autodeterminação e controle sobre dados e infraestruturas digitais. A soberania digital implica ser apto a entender os efeitos – positivos e negativos – que cada escolha tecnológica determina. Neste sentido, é essencial ter uma visão sistêmica para entender como os diferentes elementos dos ecossistemas digitais se inter-relacionam e como desenvolver, usar e regular a tecnologia ao invés de ser regulado por ela.

Uma visão pautada pela soberania digital passa por quatro elementos. Primeiramente, a autodeterminação, no sentido de livre determinação de seu desenvolvimento econômico, político, social e cultural. Em segundo lugar, a cibersegurança das infraestruturas digitais, nas suas diferentes dimensões se justapõe a várias dimensões da soberania digital. Ser soberano significa ser capaz de controlar e proteger suas próprias infraestruturas críticas, suas redes eletrônicas, seus bancos de dados e as infraestruturas políticas que permitem a governança do País. Em terceiro lugar, a soberania digital é soberania sobre dados pessoais e críticos, sendo capaz de explorar economicamente, estrategicamente e tecnologicamente, ao invés de oferecer esses ativos valiosos para atores estrangeiros sem entender seu verdadeiro valor. Por fim, para a plena realização de soberania digital – bem como da cibersegurança – é essencial uma forte ação de capacitação e treinamento multigeracional, almejando não somente as novas gerações, mas também aquelas que, apesar de já terem deixado o ensino primário ou secundário, nunca foram preparadas para os desafios da tecnologia digital.

Portanto, apesar da cibersegurança e a soberania digital serem conceitos distintos e não sinônimos, ambos se caracterizam pela multidimensionalidade. Parece interessante considerar a cibersegurança e a soberania digital em conjunção devido à justaposição de várias dimensões destes dois conceitos.

MAPEAMENTO E ANÁLISE NORMATIVA E DE BOAS PRÁTICAS

Esta pesquisa mapeou os principais instrumentos normativos brasileiros, elaborados pelo Poder Executivo Federal e pelo Congresso Nacional, que envolvem medidas de cibersegurança, com o objetivo de identificar as normas existentes sobre cibersegurança em suas diversas dimensões. A partir daí, uma análise crítica dos instrumentos de segurança cibernética buscou identificar eventuais tratamentos normativos assimétricos, tanto em sentido material como em sentido subjetivo. Neste último ponto, ressaltou-se o problema da concentração da segurança cibernética nas Forças Militares, quando esta deveria ser tratada apenas como uma parte das diversas dimensões e, portanto, uma das pontas do sistema da governança da cibersegurança.

Paralelamente, a partir de uma perspectiva ampla e, portanto, sem adentrar às ações e aos controles específicos, a pesquisa mapeou boas práticas relacionadas à garantia da segurança da informação. De maneira geral, foram identificadas as seguintes linhas-gerais: (i) implementar estruturas e padrões delineados por entidades especializadas ou governamentais; (ii) adotar arranjos de certificação em cibersegurança; (iii) seguir códigos de condutas (internos ou externos/setorizados); (iv) assinalar contratos com cláusulas-tipo (padronizadas); (v) adotar regras corporativas vinculantes; e, (vi) avaliar a contratação de seguros cibernéticos.

A partir destas referências nacionais e internacionais construiu-se um esforço de análise do quadro da cibersegurança no país. O Brasil, em que pese a importância do tema para a promoção da segurança das pessoas e seus direitos como valor central, não evoluiu, ainda, em uma estratégia unificada adequada para solucionar o problema da segurança das infraestruturas, serviços e das pessoas no espaço digital. O principal documento existente (a par de outros anteriores sobre o tema que podem indicar mais de duas décadas de trabalho) é a Política Nacional de Segurança da Informação (PNSI), promulgada em 2018, mas que não foi totalmente implementada. Após esse movimento, o Executivo Federal apenas promulgou o Decreto 10.222/2020, conhecido como “E-ciber” que detalhou apenas um dos módulos anteriormente mencionados

– a segurança cibernética. Entretanto, a iniciativa tem a vigência estabelecida para o quadriênio de 2020-2023, evidenciando a necessidade de uma renovação do quadro estratégico para a segurança cibernética no Brasil.

A análise dos instrumentos normativos brasileiros indica: (i) vazios normativos em algumas áreas importantes para garantir a segurança das pessoas e seus direitos no espaço digital; (ii) a associação da segurança cibernética com competência militar; e (iii) a falta de alinhamento normativo e estratégico entre os diferentes setores que envolvem a segurança cibernética. Como resultado, há necessidade de uma estratégia em nível nacional, vinculativa, que traga princípios unificados para todas as dimensões, padrões mínimos para os níveis operacionais e formas de cooperação entre os diferentes atores que compõem a governança da cibersegurança no Brasil. Corolário de tais observações, embora ausente no ordenamento jurídico brasileiro, e face às vantagens e desvantagens associadas e brevemente mencionada neste trabalho, enfeixa-se com a proposição de um estudo interdisciplinar acerca de eventual programa de incentivos fiscais em benefícios de organizações que invistam em estruturas, sistemas e processos (ciber)seguros. Tratar-se-ia de uma tentativa de fomentar a cultura de cibersegurança também pelo afastamento de um modelo normativo exclusivamente repressivo.

CONCLUSÃO: UMA PROPOSTA DE MARCO DE CIBERSEGURANÇA E SOBERANIA DIGITAL

Um debate público que possa levar à definição de uma estratégia, de um sistema de governança e de um marco regulatório sobre cibersegurança e soberania digital se revelam essenciais para garantir o desenvolvimento sustentável do País. Neste sentido, o objetivo deste trabalho é fornecer ao leitor chaves essenciais para abordar o debate e entender as diferentes dimensões que caracterizam as pautas analisadas, para conseguir formar uma opinião de maneira crítica e informada.

Em 2023, a falta de um Marco de Cibersegurança e Soberania Digital, de uma Agência Nacional de Cibersegurança e de um sistema capaz de preservar a cibersegurança nas suas diferentes

dimensões e promover a soberania digital não é aceitável. Para contribuir de maneira proativa ao desenvolvimento de um debate público urgente sobre esses temas essenciais para o futuro do Brasil, este trabalho se conclui com uma proposta inicial para um Marco de Cibersegurança e Soberania Digital, voltada a promover um ambiente digital seguro e sustentável e capaz de traduzir o enorme conhecimento gerado pelos *stakeholders* brasileiros em políticas públicas e ações concretas pelo desenvolvimento do País.

Nossa proposta inicial para um Marco de Cibersegurança e Soberania Digital reflete todos os elementos apresentados ao longo deste trabalho em forma de sugestão normativa, com o objetivo de estimular um debate público aberto, inclusivo e democrático sobre como o País pode construir sua soberania digital e fortalecer sua cibersegurança. A proposta destaca a necessidade de uma Estratégia Nacional de Cibersegurança e Soberania Digital, define os elementos fundamentais da soberania digital, chama a atenção para a definição de padrões de cibersegurança, bem como de mecanismos de certificação de cibersegurança e de resposta a incidentes de cibersegurança.

Ao mesmo tempo, sugere a necessidade de construir a cibersegurança em sinergia com a luta ao cibercrime e destaca como prioridades a proteção de dados estratégicos e dados sensíveis e o enfoque na capacitação individual, na educação multigeracional e conscientização em cibersegurança. Por fim, nossa proposta de Marco de Cibersegurança e Soberania Digital deveria ser implementada por uma Agência Nacional de Cibersegurança dotada de orçamento e independência suficientes para garantir uma atuação eficiente e efetiva e assistida por um Comitê Multissetorial de Cibersegurança, permitindo a participação dos demais setores interessados, e por uma Rede Nacional de Cibersegurança, capaz de estimular a interação contínua com os centros de pesquisa e desenvolvimento que atuam diretamente na construção da cibersegurança e soberania digital nacional.

1 INTRODUÇÃO

A cibersegurança permaneceu um conceito amplamente ignorado pelo público em geral até que o ex-colaborador da *National Security Agency* (NSA), Edward Snowden, expôs os esquemas maciços de *hacking* e vigilância da NSA, particularmente direcionadas ao Brasil (BRIDI; GREENWALD, 2013), catapultando as questões de cibersegurança, antes reservadas a um nicho de especialistas, para o *mainstream* (BELLI, 2021a). Na verdade, todos os indivíduos, empresas, administrações públicas, instituições de ensino e tomadores de decisão devem considerar a cibersegurança como uma preocupação fundamental antes que alguns dos principais riscos e ameaças se tornem realidade.

Para usar uma metáfora muito adequada, a cibersegurança é como uma mudança climática sob esteroides. É um problema que afeta tudo e todos, embora poucos percebam sua importância e menos ainda tenham um plano para enfrentar seus desafios. A maioria começa a desenvolver planos de cibersegurança somente após acidentes (padrão reativo), o que pode causar perdas substanciais, enormes danos – inclusive reputacionais – ou interrupções de serviços. De forma crítica, exatamente como a mudança climática, a única maneira de abordar a segurança cibernética de forma eficiente e eficaz é por meio da cooperação envolvendo todas as partes interessadas afetadas (BELLI, 2021b).

Nos últimos anos, várias instituições reconheceram, conforme apontado pela Assembleia Geral das Nações Unidas, que a segurança cibernética em suas várias dimensões “é um tema cada vez mais importante na política internacional relacionada com a economia digital e outros aspectos da Sociedade da Informação” principalmente devido à verificação de “uma incidência crescente de ataques graves de segurança cibernética, alguns dos quais tiveram impactos significativos em indivíduos e serviços públicos” (UNGA, 2018). Porém, até o momento, a segurança cibernética ainda não é uma noção universalmente definida, apesar de ter se tornado uma preocupação geral.

Em poucas palavras, **a cibersegurança é o conjunto de normas, práticas e processos que permitem proteger sistemas críticos,**

informações particularmente importantes e, sobretudo, pessoas de potenciais riscos e ameaças cibernéticas. Porém, 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, 2009).

Como sugere a leitura desta definição particularmente extensiva, e como explicaremos ao longo deste breve trabalho, a cibersegurança é um assunto necessariamente multidimensional, multissetorial e, frequentemente, transnacional (BELLI, 2021b). Tal natureza é evidente, considerando que a elaboração e implementação das ferramentas, conceitos, diretrizes etc. mencionados anteriormente depende de atores de natureza extremamente diferente – pública, privada, associativa etc. – que não são necessariamente localizados na mesma jurisdição.

Ao mesmo tempo, ciberataques implicam frequentemente atores de natureza diferente, localizados em várias jurisdições, tornando a cooperação internacional uma necessidade não somente para conseguir respostas apropriadas aos ciberataques, mas, ainda mais basicamente, para conseguir um nível de certeza adequado na atribuição mesma dos ataques. Assim, a atribuição, longe de ser atividade trivial, requer primeiramente uma complexa atividade técnica de identificação dos responsáveis por atos ilícitos; a sucessiva atribuição em função de marcos normativos heterogêneos que podem incluir direito penal, direito de seguro e até normas sobre guerra cibernética; e, por fim, questões políticas altamente sensíveis sobre quando e como governos estrangeiros podem ser

acusados de responsabilidade por ciberataques (EICHENSEHR, 2020).

Assim, o objetivo principal deste trabalho é destacar, de maneira sintética, as principais dimensões da cibersegurança, as principais soluções existentes, a íntima conexão entre cibersegurança e soberania digital e fornecer pistas para que o Brasil possa começar um urgente debate sobre como estabelecer um Marco de Cibersegurança e Soberania Digital.

1.1 Cibersegurança: uma visão sistêmica

Uma importante premissa para entender esse trabalho é esclarecer que a noção de cibersegurança é muito elástica e multidimensional e pode levar a interpretações profundamente diferentes, dependendo do contexto, do setor e do sistema jurídico. 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 democrática¹ (FICHTNER, 2018; WOLFF, 2016). Neste trabalho, destacamos também a necessidade de se colocar os indivíduos ao centro de qualquer abordagem de cibersegurança. Tal elemento parece evidente, mas, de fato, acaba sendo omitido pela enorme maioria das abordagens existentes, que se concentram principalmente na

1 BROWN *et al.* (2020) explicam de maneira eloquente a importância e o caráter multidimensional das questões de segurança cibernética nas eleições. Assim, os autores destacam que as vulnerabilidades potenciais interessam aspectos tradicionais, como manutenção de listas de eleitores, verificação de eleitores, contagem de votos e anúncio de resultados, bem como aspectos mais amplos. Neste sentido a cibersegurança interessa a interação das tecnologias digitais com o ambiente eleitoral mais amplo, como campanhas online, gerenciamento de dados de candidatos e partidos, disseminação de desinformação ou "misinformação" por meio de redes sociais e hackeamento de sistemas de votação eletrônica. A menos que sejam cuidadosamente administrados, todos esses aspectos podem determinar vulnerabilidades e falhas de cibersegurança que podem representar uma ameaça crítica à confiança do público nos resultados das eleições, que são a pedra angular da democracia.

segurança de sistemas computacionais e dados, esquecendo de destacar o papel central das pessoas.

Junto com essas diferentes dimensões, o cibercrime representa uma ulterior dimensão transversal, sendo a invasão, manipulação ou sequestro de informações e sistemas digitais para finalidades criminosas uma preocupação que perpassa todas as dimensões citadas anteriormente. Nesta perspectiva, esta seção propõe uma visão sistêmica do cenário de cibersegurança brasileiro para a construção de políticas públicas nesta área.

O interesse de escolher uma perspectiva multidimensional parece ser confirmado pela abordagem brasileira, que se organiza em vários eixos, apesar de tais eixos não corresponderem à categorização exposta anteriormente. Como destacaremos na segunda seção deste trabalho, a Política Nacional de Segurança da Informação, instituída pelo Decreto n. 9.637/18, prevê a criação de uma Estratégia Nacional de Segurança da Informação composta pelos módulos temáticos de segurança cibernética; defesa cibernética; segurança das infraestruturas críticas; segurança da informação sigilosa; e proteção contra vazamento de dados. Destes, apenas a Estratégia Nacional de Segurança Cibernética (E-Ciber) (BRASIL, 2020) e o Plano Nacional de Segurança de Infraestruturas Críticas (BRASIL, 2022) já foram publicados. Estes instrumentos são voltados tanto para as instituições de governo, quanto para o setor privado, pois estabelecem diretrizes, guias, ações estratégicas e um planejamento direcionado a respeito dos assuntos de que tratam.

A esta constatação somam-se algumas percepções que informam a abordagem ora adotada para se pensar o tema da cibersegurança de forma sistêmica. O problema da segurança cibernética pode ser visto como questão pertencente exclusivamente ao campo da técnica em informática e sistemas de informação. No entanto, desde sempre, e ainda mais significativamente depois do período pandêmico – em que serviços públicos e privados, inclusive relacionados à saúde pública, justiça, tributação etc. passaram a depender fortemente de aplicações digitais –, a cibersegurança ultrapassa esta delimitação restrita.

No Brasil, apenas em 2022, aconteceram 103,16 bilhões de tentativas de ataques cibernéticos² (SECURITY REPORT, 2023). Diante de uma realidade na qual a conectividade se torna cada dia mais permanente, ubíqua e essencial, esta situação ameaça não apenas atividades que se desenrolem digitalmente, mas todas as esferas da sociedade, da economia e da democracia brasileira. 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.

Alguns exemplos recentes de instâncias em que incidentes cibernéticos afetaram o provimento de serviços públicos no Brasil incluem os ataques ao ConecteSUS (G1, 2021) e ao FormsUS (VARGAS; RODRIGUES, 2021), impactando o controle vacinal e vulnerabilizando dados pessoais sensíveis de pacientes; diversos ataques a sistemas de tribunais, forçando a interrupção de processos e extensão de prazos, como o ataque que afetou a Justiça do Rio Grande do Sul (VASCONCELLOS, 2021) e outro, contra o STJ (VALENTE; VITAL, 2020); o ataque recente ao sistema da Prefeitura do Rio de Janeiro, que obrigou a interrupção de serviços públicos ao cidadão (SCHENDES, 2022); e a invasão sofrida em sites do Governo do Ceará (EQUIPE TECMUNDO, 2022).

Este último caso revela com precisão a confluência entre cibersegurança e o processo democrático. O ataque sofrido por sites do governo cearense se manifestou como mensagens reivindicando a anulação de votos de cidadãos brasileiros da região Nordeste, sequestrando o espaço de grande visibilidade e credibilidade destes portais para a difusão de discurso de ódio e de fomento a um golpe antidemocrático. Este é um tipo de ação cujo efeito se dá sobre um dos alvos preferenciais mapeados por Rid e Buchanan (2018, p. 8) ao tratarem do “hackeamento” das democracias: as instituições e, mais especificamente, a confiança que as populações depositam nelas e que são o fundamento de seu funcionamento.

Em sua análise a respeito das medidas ativas (*active measures*) que influenciaram as eleições estadunidenses de 2016, Rid e Buchanan apontam quatro fatores de especial atenção para se pensar a

2 Ver seção 1.2.

cibersegurança no atual contexto informacional e das infraestruturas democráticas. Primeiro, a adoção de medidas direcionadas a eleitores, específica e imediatamente – principalmente com o uso de redes sociais. Segundo, a necessidade de se considerar a escala das medidas adotadas, especialmente devido aos usos possibilitados pelas redes sociais, capazes de alcançar milhões de pessoas de maneira difusa em um espaço de tempo extremamente reduzido. Terceiro, sua condução parcialmente às claras, no sentido de que as medidas em curso eram discutidas abertamente já em 2016. E, quarto, a eficácia e longevidade das medidas, que, segundo os autores, foram incorporadas ao léxico de agentes políticos, de modo que seus efeitos foram continuamente reciclados.

A experiência brasileira nas eleições de 2018 apresentou características que se relacionam em parte com o quadro analítico apresentado por Rid e Buchanan. Em análise a respeito do uso do aplicativo de mensagens WhatsApp como ferramenta de difusão de imagens contendo desinformação, Evangelista e Bruno (2019) destacam (i) o caráter direcionado da estratégia, por meio de ação aparentemente centralizada e não-espontânea em grupos de WhatsApp; e (ii) o amplo alcance das imagens utilizadas (“[a] pesar de o número total de imagens classificadas como desinformação ser relativamente baixo – apenas 1% do total de imagens compartilhadas –, estas imagens foram vistas em 44% dos grupos monitorados durante o período de campanha eleitoral, o que evidencia seu longo alcance” (EVANGELISTA; BRUNO, 2019, p. 7). No caso brasileiro, no entanto, tratava-se de estratégias conduzidas sub-repticiamente, por meio de contratação de empresas especializadas em marketing direcionado via WhatsApp que afirmavam realizar mero trabalho de curadoria do conteúdo produzido por apoiadores orgânicos do candidato, apesar de se tratar de um esforço coordenado de campanha, como destacam os autores. Mesmo assim, especialmente o caráter de aproximação direta do discurso em relação aos eleitores se verificou no caso brasileiro, processo descrito por Cesarino (2020) como uma “diluição ainda mais acentuada das fronteiras entre a esfera político-eleitoral e outros domínios da vida” (p. 112).

Ainda que a comparação direta entre democracias consideravelmente distintas dependa de um longo e consistente trabalho de contextualização, as considerações sobre o caso estadunidense e a experiência brasileira apontam alguns caminhos de análise. Tais caminhos são úteis para se considerar como pensar a cibersegurança numa sociedade da informação na qual os indivíduos conectados tipicamente ignoram o impacto das tecnologias digitais, particularmente no que diz respeito às dinâmicas manipulativas que caracterizam o chamado capitalismo de vigilância (ZUBOFF, 2019), que amplifica e renova antigas práticas de dominação. A desinformação ainda é uma dimensão ausente em padrões internacionais e análises especializadas de ameaças cibernéticas (CARAMANCION et al., 2022; EU DISINFOLAB, [s.d.]), apesar de seus efeitos concretos, sentidos reiteradamente no Brasil e no mundo (ENISA, 2022).

Diante de tudo isso, indicamos a necessidade de uma leitura da cibersegurança que extrapole limites estritos, nomeadamente as abordagens excessivamente setoriais, e alcance uma visão sistêmica capaz de confrontar a complexidade do problema. Estudos sobre cibersegurança muito frequentemente voltam-se a aspectos técnicos, como criptografia, ou ameaças específicas, como *malware* ou ataques DDoS. Por outro lado, estudos sobre regulação de telecomunicações, plataformas, desinformação, proteção de dados pessoais e outras áreas em que a ação humana é traduzida para a esfera digital frequentemente focam aspectos jurídicos, políticos ou econômicos próprios, chegando raramente a examinar de maneira completa e, ainda mais raramente, a conectar as diferentes dimensões da cibersegurança.

Assim, as abordagens mono-disciplinares utilizadas geralmente consideram somente uma das dimensões do problema, por exemplo focando somente na segurança das infraestruturas ou dos dados pessoais. Como visto, o próprio conceito de cibersegurança, sob uma abordagem renovada, deve ser reimaginado numa perspectiva sistêmica – dando conta, inclusive, das discordâncias do campo a respeito de seu uso (VAN DEN BERG, 2020).

Mais um ponto de preocupação que reforça a necessidade de uma visão sistêmica é a exigência de estratégias concertadas para lidar

de maneira eficiente e efetiva com um assunto complexo, multissetorial, multidisciplinar e, frequentemente, transnacional. A cacofonia entre setores, nichos da prática, especialidades acadêmicas e órgãos e agentes públicos contribui para um cenário de vulnerabilidade. A dificuldade de estabelecimento de um mecanismo de governança, coordenação e regulação eficiente, capaz de elaborar e implementar padrões, compartilhar informações sobre incidentes e favorecer a troca de boas práticas, tanto em nível nacional quanto internacional, contribui para essa vulnerabilidade (BARTOLOMÉ, 2021; RID; BUCHANAN, 2018; TORRIJOS RIVERA; JIMÉNEZ SALCEDO, 2021). Essa compartimentalização verificase, também, no Brasil, aliada a uma tendência à concentração das políticas públicas em torno de contextos militarizados, legado que vem se constituindo desde a realização dos megaeventos no país e incremento de legislações que facilitam e incentivam práticas de vigilância pelo Estado (CODING RIGHTS, 2020), cenário que se agravou nos últimos anos. A vulnerabilidade de um cenário fragmentado também pode ser estudada a partir da evolução do nível de maturidade em relação à cibersegurança da União Europeia em suas políticas públicas e propostas legislativas sobre o tema. Por exemplo, a Primeira Estratégia de Cibersegurança da União Europeia, publicada em 2013, consolidou o entendimento do termo “cibersegurança” como algo que, na União Europeia, representaria, ao menos, as dimensões de ciber-resiliência, cibercrime, ciberdefesa, cibersegurança e questões do ciberespaço a nível global. Apesar de o cenário jurídico e regulatório do bloco em relação ao tema ainda ser bastante fragmentado, resultado de políticas e iniciativas diversas focadas em aspectos diferentes da cibersegurança (FUSTER; JASMONTAITE, 2020), em 2017, foi publicada a Segunda Estratégia de Cibersegurança da União Europeia.

A Segunda Estratégia demonstrou de forma clara a evolução da União Europeia em relação a questões de cibersegurança e destacou, também, a noção de que cibersegurança se trata de um tema de responsabilidade de diversos atores, devendo ser implementada por camadas distintas do governo, da economia e da sociedade para se fortalecer (FUSTER; JASMONTAITE, 2020). Ressalta-se, ainda, que ambas as Estratégias se originaram após

a adoção de medidas legislativas diversas em relação a cibersegurança, todavia, elas também definem objetivos de políticas públicas que guiam e guiam propostas legislativas e regulatórias, inclusive o Regulamento (UE) 2019/881 do Parlamento Europeu e do Conselho, relativo à ENISA (Agência da União Europeia para a Cibersegurança) e à certificação da cibersegurança das tecnologias da informação e comunicação.

O Regulamento (UE) 2019/881 é a primeira estrutura de certificação buscando a padronização na abordagem de questões referentes à cibersegurança na União Europeia, e destaca a necessidade não só de um conjunto de medidas que intensifiquem e melhorem a cooperação entre os Estados-Membros e as empresas e instituições, mas também traz enfoque para a necessidade de se conscientizar cidadãos, fortalecer a confiança dos consumidores em relação a serviços e o mercado digital e que “a cibersegurança não é só uma questão relacionada com a tecnologia; o comportamento humano é igualmente importante” (PARLAMENTO EUROPEU; CONSELHO DA UE, 2019, art. 8). Percebe-se, assim, que buscaram tratar das mais diversas dimensões da cibersegurança para garantir que o desenvolvimento regulatório do tema na UE se torne cada vez menos fragmentado.

A abordagem compartimentada produz estratégias, regulações, instituições e ações fortemente limitadas e fragmentadas. Isto configura uma vulnerabilidade sistêmica adicional e frequentemente explorada. O valor por trás da proposta de se construir uma compreensão sistêmica da cibersegurança está em prover uma abordagem para o estudo da cibersegurança que dê conta dessa complexidade.

O enfoque em dados pessoais dá ensejo a investigações que podem ir ao âmago de mercados em franca ascensão e de acelerada inovação tecnológica, como o e-commerce, inteligência artificial, Internet das coisas (“IoT” na sigla inglês) e o mercado de atenção em plataformas digitais. Também permite lançar um olhar sobre esforços de governo digital e políticas públicas relativas a tecnologias que são nós de interseção entre diversos interesses e

problemáticas, como a criptografia, a criptografia pós-quântica³ e o reconhecimento facial, entre outras (HOSSAIN FARUK et al., 2022). Afinal, o uso de tecnologias digitais para tratamento de dados pelo Estado poderá levar a novas formas de promoção de violência institucional contra determinadas coletividades.

O enfoque na segurança da arquitetura democrática se voltará à estabilidade de processos democráticos sob a ótica da cibersegurança – como se estruturam redes que visam à desestabilização de eleições e governos, de que ferramentas lançam mão nestes esforços e quais suas conexões com outras formas de ameaça digital. De especial importância é, também, o foco na capacitação de indivíduos e da sociedade, sendo o indivíduo não capacitado frequentemente apontado como o “elo fraco” de qualquer sistema de cibersegurança.

Finalmente, o enfoque no preparo tecnológico, inclusive o investimento em pesquisa e desenvolvimento de soluções de cibersegurança, permitirá construir um pano de fundo para a análise dos problemas levantados: um quadro dos esforços de inserção do país como ator regional ou global na área, seu investimento em tecnologias da informação, estrutura de defesa cibernética e ecossistema institucional relativo à cibersegurança.

1.2 Ataques e ameaças cibernéticas e vulnerabilidades exploradas

Considerando a abordagem sistêmica da cibersegurança de que a trata a seção 1.1, as ameaças e ataques cibernéticos, bem como as vulnerabilidades exploradas por estas práticas, também precisam ser encaradas da mesma maneira. Incidentes de cibersegurança não se referem somente aos ataques ou falhas que levam à perda,

3 A criptografia pós-quântica busca uma resposta ao desafio apresentado pelo potencial aumento de capacidade computacional a partir da aplicação de tecnologias quânticas, o que tornaria algumas formas de criptografia de chaves públicas atualmente utilizadas vulneráveis a ataques. A criptografia pós-quântica não se refere a uma tecnologia determinada, mas a um conjunto possível de estratégias para manter a criptografia mesmo diante de computadores com capacidades quânticas. Um padrão de criptografia pós-quântica é atualmente discutido pelo *National Institute of Standards and Technology* (NIST) estadunidense, e o Departamento de Segurança Nacional (*Homeland Security*) do país emitiu memorando em 2021 recomendando ações internas para a adaptação de sistemas ao novo padrão, assim que publicado (GILES, 2019; NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY, 2017; U.S. DEPARTMENT OF HOMELAND SECURITY, 2021).

destruição, bloqueio ou acesso não autorizado às informações, sistemas, ou infraestruturas críticas, comprometendo os princípios CIA (confidencialidade, integridade, autenticidade e disponibilidade) e IAA (identificação, autenticação e acesso)⁴ (VAN DEN BERG, 2020, p. 32). Eles também se referem a comportamentos inseguros adotados por desenvolvedora/es e usuária/os de tecnologias e sistemas digitais (VAN DEN BERG, 2020), inclusive aqueles que possam afetar a segurança das estruturas democráticas, a proteção de dados pessoais e a própria coletividade – refletindo os enfoques de que tratamos anteriormente.

Os efeitos de incidentes de cibersegurança são variados, podem se dar em dimensão coletiva ou individual e ter impactos locais, nacionais ou mesmo transnacionais. No caso do Brasil, a maior parte dos ataques têm origem interna⁵. O principal alvo de ataques cibernéticos são empresas privadas, órgãos e entidades públicas, como os exemplos apresentados na seção 1.1 deste trabalho indicam. No entanto, há preocupação também por parte de organizações da sociedade civil voltadas para a proteção de direitos, que também relatam experiências de ataques (SHIRA; JANCZ, 2020, p. 5).

Em certos países da América Latina e do Caribe, a inexistência de políticas gerais e sistemáticas orientadas para cibersegurança impacta nos custos que ataques cibernéticos implicam para os estados locais (IZAGUIRRE OLMEDO; LEÓN GAVILÁNEZ, 2018). Os impactos da ausência de políticas públicas que centrem suas atenções inclusive na difusão de informação e formação de espaços educativos no tema de segurança cibernética não são sentidos apenas nos custos: vulnerabilidades originadas em tecnologias digitais expõem a segurança das pessoas em contextos não virtuais (e.g., roubos dos dispositivos físicos) (IZAGUIRRE OLMEDO; LEÓN GAVILÁNEZ, 2018).

Muitos dos ataques combinam diferentes técnicas para explorar as vulnerabilidades das redes e seu/suas usuária/os. Por exemplo, os ataques de *ransomware*, em que um *malware* é instalado

4 Boas práticas relacionadas à implementação desses princípios serão abordadas por nós na seção 3.2 deste trabalho.

5 51,93% dos incidentes reportados ao CERT.br de janeiro a dezembro de 2020 tiveram origem no Brasil (CERT.BR, [s.d.]).

para bloqueio das informações e sistemas de determinadas organizações, cujo acesso só é restaurado mediante pagamento de resgate ao agente malicioso, é originado frequentemente pelo acesso via práticas de *phishing*. As vulnerabilidades podem ser provocadas não só por ataques ativos, mas pela ausência da adoção de medidas de segurança simples, como evitar o uso de senhas pouco complexas e o resguardo contra a realização de downloads de arquivos infectados por vírus, somado ao fato do desconhecimento da forma de atuação de agentes maliciosos. Segundo relatório publicado pela ENISA (2022), os principais atores que exploram essas vulnerabilidades para prática de ataques são: atores apoiados por Estados, cibercriminosos, hackerativistas e hackers contratados por outras entidades privadas (p. 23).

Os impactos são múltiplos e podem refletir efeitos internos – como situações de elevado estresse diante do desconhecimento em como lidar com esse tipo de situação – e interrupção de atividades essenciais. O restabelecimento da infraestrutura, por sua vez, poderá levar a custos financeiros e sociais consideráveis, redução de competitividade, danos reputacionais, interrupção das operações ou/e serviços e riscos de privacidade e proteção de dados.

Cabe reiterar que, para além de problemas no âmbito organizacional, as preocupações em relação aos ataques e demais incidentes cibernéticos afetam várias dimensões interconectadas, como proteção de dados, salvaguardas de interesses financeiros, proteção de infraestruturas públicas e políticas e controle de fluxos de informação e comunicação (FICHTNER, 2018). 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. O cumprimento de obrigações, como prestação de contas, pode ser prejudicado pela interrupção das atividades.

Na tabela a seguir são ilustrados alguns dos principais tipos de ataques, as vulnerabilidades que dão ensejo ao ataque e suas potenciais consequências:

Tabela 1 – Tipos de ataques/ameaças cibernéticas

Problemas ⁶		
Tipos de ataques/ameaças	Vulnerabilidades	Consequências ⁷⁻⁸
Desinformação	Uso da arquitetura de plataformas digitais (principalmente plataformas sociais) para dispersão de desinformação, informações enganosas, ou informações maliciosas.	<ol style="list-style-type: none"> 1. Efeitos nos 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, como 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).

6 A tabela foi elaborada com base na taxonomia disponibilizada pela Cisco ([s.d.]) e na taxonomia apresentada no relatório da Ensina (2022), 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)

7 É de extrema importância destacarmos que as consequências, longe de serem exaustivas, são meramente exemplificativas, a fim de facilitarmos a compreensão dos múltiplos ataques e/ou ameaças.

8 A taxonomia de tipos de impactos apresentada no relatório da ENISA (2022, 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.

Problemas ⁶		
Tipos de ataques/ameaças	Vulnerabilidades	Consequências ⁷⁻⁸
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 vírus de dispositivos eletrônicos, softwares <i>worms</i> (“vermes”), que se multiplicam para atingir diferentes dispositivos; cavalos de Tróia (arquivos aparentemente normais, infectados por vírus) (ENISA, 2022).	<ol style="list-style-type: none"> 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 <i>spyware</i> (softwares de espionagem); 4. Compromete a operabilidade do sistema.
Estelionato de Dados (Phishing)	<p>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.</p> <p>Existem diferentes modalidades de phishing (ENISA, 2022):</p> <p>(i) smishing, i.e., phishing realizado por meio SMS (mensagens de textos enviadas ao celular);</p> <p>(ii) vishing, i.e., phishing realizado por meio de ligações telefônica (e.g., robô se passando por telefone da instituição bancária da pessoa “alvo” do golpe) ;</p> <p>(iii) spear phishing, bastante comum no Brasil⁹, 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;</p>	<ol style="list-style-type: none"> 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 chantagem a partir das informações obtidas, para manipulação de comportamentos; 3. Obtenção de benefícios financeiros, por meio de pagamentos ou transferências indevidas.

9 Trata-se do comum golpe em que o atacante se passa por um/a amigo/a ou familiar da pessoa “alvo” do ataque, para, por exemplo, solicitar transferência de quantias elevadas de dinheiro, alegando algum tipo de situação de emergência (cobrança de dívidas, questões de saúde, acidentes etc.).

Problemas ⁶		
Tipos de ataques/ameaças	Vulnerabilidades	Consequências ⁷⁻⁸
Estelionato de Dados (Phishing)	<p>(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);</p> <p>(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 (CASTELO BRANCO, 2021; FRAILE; MARCOS; YAGÜE, 2022).</p>	
Fraudes	<p>No Brasil, são bastante comuns as fraudes bancárias (seja por meio de falsificação de boletos, envio de cobranças indevidas).</p> <p>Se vale de ocultação de informações, mimetização de informações (arquivos, documentos) relevantes. A contrafação, portanto, é uma manifestação da fraude.</p> <p>Também se vale de informações públicas ou obtidas indevidamente para prática da fraude.</p>	<ol style="list-style-type: none"> 1. Prejuízos financeiros a determinada pessoa; 2. Uso indevido de dados; 3. Danos reputacionais a organizações.
Falsidade ideológica/Roubo de identidade	<p>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.</p>	<ol style="list-style-type: none"> 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 à danos à integridade física da pessoa); 3. Possíveis perdas financeiras da pessoa que teve a identidade roubada.

Problemas ⁶		
Tipos de ataques/ameaças	Vulnerabilidades	Consequências ⁷⁻⁸
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 ¹⁰ 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.	<ol style="list-style-type: none"> 1. Obtenção de informações e/ou dados; 2. Diante de ataques dessa natureza, há o impacto de aumento nos custos organizacionais de defesa (ENISA, 2022, p.11).
Reencaminhamento do sistema de nomes de domínio (DNS Tunneling)	Consiste em aproveitar a vulnerabilidade do DNS ¹¹ 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.

10 Linguagem cujos comandos são utilizadas para realizar buscas em bases de dados estruturadas relacionais.

11 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 próprios, por exemplo).

Problemas ⁶		
Tipos de ataques/ameaças	Vulnerabilidades	Consequências ⁷⁻⁸
Vazamento de Dados	Pode se valer das técnicas anteriores para vaziar informações disponibilizadas em determinada base de dados, ou de configurações erradas ou erros humanos, que levam à divulgação indevida da base.	<ol style="list-style-type: none"> 1. Violação de direitos fundamentais ou coletivos por meio do tratamento indevido ou discriminatório de dados; 2. Desvios nas finalidades; 3. Uso das informações indevidamente divulgada para prática de golpes, fraudes, ou outra das ameaçadas/ataques identificados nessa tabela.
Ataques a cadeias de suprimento	Combina um ou mais dos ataques anteriores para promover ataque à dois alvos, simultaneamente, i.e., um cliente e um fornecedor.	<ol style="list-style-type: none"> 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.

Todas as ameaças, e ataques listados impactam também a segurança das infraestruturas críticas. No setor de transporte europeu, por exemplo, o *ransomware* é 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 afetam inclusive a prestação de serviços de saúde, justiça e transporte público (que desempenham um papel essencial para exercício de outros direitos).

Ainda que as preocupações de segurança cibernética envolvendo áreas como fornecimento de água, transporte ou energia elétrica tragam para o debate preocupações relacionadas ao funcionamento da sociedade como um todo, o principal objetivo da

segurança cibernética nessas áreas deve seguir sendo a proteção das pessoas. Toma-se o exemplo do setor de transporte: conforme aponta relatório da ENISA (2023) em relação especificamente a este setor (e que pensa, majoritariamente, a Europa), parte significativa dos ataques é direcionada aos ativos de TI dos prestadores de serviços relacionados, e/ou respectivos fornecedores. Além disso, os ataques que ameaçavam os dados mantidos pela indústria de transporte representaram 21% dos ataques em 2021 e, mesmo com redução em 2022, o setor seguiu representativo (chegando a 9%, conforme relatório da ENISA, 2023). O mesmo relatório informa que as principais motivações se relacionavam à obtenção de vantagens financeiras (37%) e representavam ataques considerados, nos termos do documento, como cibercrimes – i.e., ataques que comumente envolvem o roubo e/ou venda de dados ou sequestro de dados mediante pedido de resgate. Os dados, ao lado de serviços, representam os principais “ativos” afetados pelos ataques, representando, respectivamente, 26% e 28% dos impactos físicos ou digitais, interpretados a partir das informações disponíveis sobre os ataques.

Por um lado, esses dados podem representar informações de natureza pessoal, de forma que a/os principais afetada/os sejam as pessoas titulares desses dados. Por outro lado, ainda que os dados alvo de ataques não tenham natureza pessoal, os reflexos de incidentes de segurança cibernética são sentidos na prestação do serviço público de transporte e na continuidade das operações, mesmo que a motivação do ataque não tenha sido a interrupção dos serviços, já que tratam-se de dados estratégicos para operação do sistema de transporte, seja ele público ou não – impactando, portanto, uma série de garantias e exercícios de direitos da população, que dependem do bom funcionamento do transporte. Por fim, trata-se de informações estratégicas para a sociedade em que opera a infraestrutura crítica, uma vez que são relevantes, por exemplo, para formulação de políticas públicas e tomadas de decisão pelo Estado. É o que ocorre na maioria dos ataques voltados ao setor rodoviário, onde o principal objetivo dos ataques envolvendo dados é a obtenção de dados de funcionários de instituições envolvidas na operação de transporte e usuária/os de serviço de transporte, seja ele coletivo ou público (ENISA, 2023,

p. 39 – ao tratar de ataques envolvendo plataformas voltadas para treinamento de pessoal e máquinas de compra de bilhetes). Ou seja, os principais afetados por incidentes de segurança cibernética sempre serão, ao fim e ao cabo, as pessoas.

Além da centralidade da proteção das pessoas na segurança das infraestruturas crítica, os ataques destinados ao setor de transporte oferecem um exemplo eloquente para evidenciar a necessária cooperação para elaborar e implementar estratégias de segurança cibernética. Considerando as análises feitas pela ENISA (2023) em relação ao setor de aviação, majoritariamente europeu, grande parte dos ataques cibernéticos nessa área são voltados a aeroportos, mais afetados por ataques de *ransomware* (p. 26). Impactos na operação dos aeroportos originados dos ataques aos seus sistemas cibernéticos têm reflexos internacionais. Ainda assim, a maior parte dos ataques são direcionados a roubo, sequestro ou venda de dados de clientes (dados pessoais) ou das próprias companhias aéreas (dados proprietários), evidenciando o risco sempre centrado nas pessoas de diferentes países e a prevalência da motivação financeira (e não *hacktivista*).

Portanto, é preciso que as autoridades de diferentes países e operadores de transportes (especialmente de aeroportos) estabeleçam mecanismos de cooperação para identificação dessas ameaças e compartilhar melhores práticas para mitigar riscos e reagir tempestivamente em caso de ataque.

Além disso, pode ter relação com o grande número de ataques apresentados na seção 1.1 o baixo custo para a sua realização, tornando ainda mais baixo pelas recentes evoluções tecnológicas em âmbito de inteligência artificial generativa – como o chatbot ChatGPT, capaz de redigir malware, e-mails de *phishing* para golpes online e *fake news* (BELLI; DA HORA, 2023) e a escalabilidade das ações maliciosas ou dos efeitos nocivos deixados pela exploração de vulnerabilidades.

Neste contexto, cabe ressaltar a existência e importância de iniciativas como o “Programa Internet + Segura”¹² do CGI.br e NIC.br (2017) que,

12 A plataforma institucional do programa pode ser acessada em: <https://bcp.nic.br/i+seg/>.

diante do posicionamento privilegiado das instituições em relação ao acesso às informações sobre fluxos das redes, buscam identificar os principais riscos de segurança cibernética no Brasil e “reduzir as vulnerabilidades e falhas de configuração presentes nos elementos das redes”, conforme informações disponíveis na plataforma. Também é objetivo do programa promover ações pedagógicas que ajudem a difundir os conhecimentos e a cultura de cibersegurança, para que, de forma geral, tenhamos protocolos de comunicação mais seguros.

Diante dos ataques mais comuns no Brasil (“negação de serviço, sequestro de prefixos e vazamento de rotas”, segundo plataforma institucional do programa), o programa identificou os principais eixos de ação para atender e esses objetivos. Trata-se de prioridades que dialogam, por exemplo, com as experiências relatadas por instituições da sociedade civil em oportunidades em que compartilharam experiências com incidentes (principalmente ataques de *ransomware*).

Tabela 2 – Tipos de ataque cibernético e medidas de mitigação

Problemas			
Tipos de ataques	Vulnerabilidades	Consequências	Medidas de mitigação identificadas pelo CGI.br e NIC.br
Sequestro de Prefixos (hijacking)	Assim como o vazamento de rotas, é voltado para o sistema de roteamento de rede de internet, e ocorre quando um agente malicioso (ou não, como nos casos de configuração errônea) utiliza o prefixo de outro endereço de outras redes, como forma de alterar o destino do tráfego da rede.	<ol style="list-style-type: none"> 1. Negação do serviço (sobrecarga do sistema, ou interrupção de sua operação); 2. Mudar o curso do tráfego de dados, para destinos ilegítimos para práticas maliciosas (acessos indevidos a informações); 3. Simulações de tráfego nas comunicações em rede; 4. Interrupção da internet para impactar o exercício de direitos como liberdade de expressão, associação e política, liberdade de manifestação artísticas. 	<ol style="list-style-type: none"> 1. Adoção de filtros de entrada

Problemas			
Tipos de ataques	Vulnerabilidades	Consequências	Medidas de mitigação identificadas pelo CGI.br e NIC.br
Negação do Serviço, ou <i>Denial-of-service attack</i> e Ataque Distribuído de Negação de Serviços, ou <i>Distributed-denial-of-service attack</i> (DDoS)	Consiste em indisponibilizar uma rede ou sistema sobrecarregando a conexão inundando-os com tráfegos de dados mal-intencionados.	<ol style="list-style-type: none"> 1. O sistema ou rede fica impossibilitado de atender às solicitações dos usuários, tornando-se inoperável; 2. Produção das mesmas consequências da interrupção dos serviços de internet; 3. Interrupção das atividades de determinada organização. 	<ol style="list-style-type: none"> 1. Configuração correta dos serviços (de acordo com notificações feitas aos responsáveis do IP pelo CGI.br).

É importante frisar também que o constante diálogo com instituições técnicas como CGI.br, CERT.br e NIC.br é essencial, diante do seu posicionamento excepcional para acessar informações sobre novas dinâmicas e ameaças à cibersegurança e boas práticas para lidar de maneira efetiva e eficiente com tais fenômenos. Neste sentido, diante do caráter internacional (conforme apresentado no próximo tópico), da multiplicidade de técnicas que podem ser combinadas a baixo custo para realização dos ataques e do constante avanço e novidades, uma abordagem multissetorial parece particularmente útil. Assim, a proximidade com atores de natureza diferente – comunidade técnica e acadêmica, setor privado, sociedade civil, movimentos sociais e organizações internacionais, além de governos – é fundamental para que a governança da cibersegurança seja eficiente e democrática e as respostas regulatórias para fortalecimento de cibersegurança sejam efetivas, atualizadas e aprimoradas constantemente.¹³

¹³ Isto é especialmente relevante diante da sofisticação dos ataques, que usam, por exemplo, modelos de aprendizado de máquina para replicar, automaticamente, as ameaças em escala, com baixos custos de reprodução.

1.3 O impacto da Inteligência Artificial na cibersegurança e da cibersegurança na Inteligência artificial

A inteligência artificial (IA) emergiu como uma força transformadora em vários setores, e uma área em que seu impacto é particularmente significativo é a segurança cibernética. À medida que o cenário digital se torna cada vez mais complexo e as ameaças cibernéticas se tornam mais sofisticadas, as organizações estão recorrendo a soluções baseadas em IA para reforçar suas defesas e proteger seus dados confidenciais. A IA oferece uma variedade de recursos que aprimoram as medidas de segurança cibernética, incluindo detecção avançada de ameaças, resposta em tempo real e análise de dados em escala (ANSARI et al., 2022).

No campo da segurança cibernética, a IA serve como um poderoso aliado, aproveitando algoritmos de aprendizado de máquina e automação inteligente para identificar, analisar e responder a ameaças com velocidade e precisão sem precedentes. Ao analisar grandes volumes de dados, os sistemas de IA podem detectar padrões, anomalias e indicadores comportamentais que indicam a presença de atividades maliciosas. Isso permite que as organizações se defendam proativamente contra ataques cibernéticos, evitando possíveis violações antes que causem danos significativos.

Além disso, os sistemas baseados em IA podem aprender e se adaptar continuamente às ameaças cibernéticas em evolução, fornecendo uma camada adicional de defesa. Esses sistemas podem evoluir seus modelos com base em novos dados e vetores de ataque emergentes, tornando-os cada vez mais resilientes e eficazes na identificação de ameaças anteriormente desconhecidas (YAMPOLSKIY; SPELLCHECKER, 2016). Com a IA, as organizações podem se afastar das abordagens tradicionais baseadas em regras para a segurança cibernética e adotar uma estratégia de defesa mais dinâmica e proativa.

No entanto, à medida que a IA se torna parte integrante da segurança cibernética, ela também levanta importantes considerações éticas e desafios de segurança. Garantir a justiça e a transparência dos algoritmos de IA, proteger a privacidade dos dados, proteger

contra ataques adversários e lidar com preconceitos são apenas algumas das questões complexas que precisam ser navegadas para aproveitar todo o potencial da IA, mantendo a confiança e a responsabilidade.

A inteligência artificial, com sua capacidade de imitar a inteligência humana e tomar decisões inteligentes, oferece um novo paradigma na identificação, mitigação e prevenção de ameaças cibernéticas. Ao alavancar algoritmos de aprendizado de máquina, técnicas de aprendizado profundo e recursos de análise de dados, os sistemas de IA podem analisar grandes quantidades de dados e detectar padrões que podem indicar atividades maliciosas. Isso permite que as organizações identifiquem e respondam a ataques cibernéticos em tempo real, reduzindo significativamente o tempo de resposta e minimizando os possíveis danos causados por tais ameaças (YAMPOLSKIY; SPELLCHECKER, 2016).

Um dos principais pontos fortes da inteligência artificial no combate a ataques cibernéticos reside em sua capacidade de se adaptar e aprender com os cenários de ameaças em evolução. As medidas tradicionais de segurança cibernética organizam padrões de ameaças conhecidas que são utilizados para identificar e bloquear atividades maliciosas e partir desta organização a inteligência artificial aprende como prevenir ou mitigar danos de forma ágil.

Por outro lado, os sistemas baseados em IA podem aprender e atualizar continuamente seus modelos com base em novos dados, permitindo detectar ameaças anteriormente desconhecidas e adaptar suas estratégias de defesa de acordo, em abordagem dinâmica. Aproveitando dados históricos e em tempo real, esses sistemas tornam-se cada vez mais eficazes na identificação de ameaças anteriormente desconhecidas e na detecção de anomalias sutis que podem passar despercebidas pelas medidas de segurança tradicionais.

Ao alavancar algoritmos de aprendizado de máquina e redes neurais profundas, os sistemas de IA podem analisar conjuntos de dados complexos, incluindo tráfego de rede, logs do sistema e comportamento do usuário, para identificar padrões anômalos e indicadores de possíveis ataques. Isso permite que as organizações

detectem e respondam a ameaças em tempo real, geralmente antes que ocorram danos significativos (GELUVARAJ; SATWIK; ASHOK KUMAR, 2019).

Além disso, os sistemas de detecção e prevenção de ameaças baseados em IA podem reduzir significativamente os falsos positivos, que costumam levar muito tempo para os analistas de segurança investigarem. Por meio de análise inteligente e correlação de eventos de segurança, os sistemas de IA podem priorizar e filtrar ameaças em potencial com precisão, permitindo que as equipes de segurança concentrem suas forças na análise dos casos.

A seguir, apresentamos alguns exemplos de ferramentas que têm sido desenvolvidas e aplicadas na interseção entre sistemas de IA e cibersegurança.

- **Darktrace:** Darktrace utiliza aprendizado de máquina e algoritmos de IA para detectar e responder a ameaças cibernéticas em tempo real. Sua tecnologia Enterprise Immune System analisa o tráfego de rede e o comportamento do usuário para identificar padrões anormais que podem indicar um possível ataque (DARKTRACE, [s.d.]).
- **Cylance:** A Cylance, agora parte da BlackBerry, utiliza IA e aprendizado de máquina para prevenir proativamente malware e ataques cibernéticos. Sua plataforma orientada por IA usa análise preditiva para detectar e bloquear arquivos e atividades maliciosas antes que possam causar danos (BLACKBERRY, [s.d.]).
- **IBM Watson for Cyber Security:** O IBM Watson for Cyber Security é uma plataforma baseada em IA que auxilia os analistas de segurança na detecção e investigação de possíveis ameaças. Ele analisa grandes quantidades de dados de segurança, incluindo logs, relatórios e inteligência de ameaças, para fornecer insights e recomendações para mitigação de ameaças (IBM, 2017).
- **SentinelOne:** O SentinelOne oferece uma plataforma de proteção de endpoint com IA que usa análise comportamental e aprendizado de máquina para detectar e prevenir malware e ameaças cibernéticas avançadas. Sua tecnologia responde de forma autônoma e mitiga ataques em tempo real (SENTINELONE, [s.d.]).

- **FireEye:** FireEye utiliza aprendizado de máquina e análise baseada em IA para detectar e responder a ameaças avançadas. Sua plataforma Helix combina IA com análise humana especializada para fornecer recursos abrangentes de detecção e resposta a ameaças (TRELLIX, [s.d.]).

Esses exemplos indicam que a inteligência artificial está sendo oferecida por empresas de segurança cibernética como ferramenta para aprimorar a detecção e a prevenção de ameaças. Eles mostram os recursos da IA na análise de grandes quantidades de dados, identificando anomalias e permitindo uma resposta em tempo real para combater ameaças cibernéticas em evolução. Porém, é importante destacar que a IA pode desempenhar também um facilitador de ciberataques, como abordaremos na próxima subseção.

1.3.1 Inteligência artificial como facilitador de ciberataques

Cabe destacar que, ao longo da última década, os ataques cibernéticos aumentaram exponencialmente não apenas em termos quantitativos, mas também no nível de sofisticação das ameaças. O futuro da segurança cibernética será impulsionado por uma nova classe de ataques cujo objetivo não é necessariamente roubar dados, mas sim manipulá-los ou alterá-los. A capacidade fundamental da IA de aprender e se adaptar dará início a uma nova era na qual ataques altamente personalizados e que imitam humanos são escaláveis (DIXON; EAGAN, 2019).

Particularmente, a IA pode acelerar os ciberataques em três dimensões: velocidade, escala e sofisticação. No que diz respeito à velocidade, o processo humano de desenvolvimento e implementação de estratégias de ciberataques, que às vezes leva meses, pode ser reduzido a dias, horas ou até automatizado em poucos minutos. Da mesma forma, assim que sistemas de IA começarem a descobrir estratégias efetivas de invasão informática, eles serão capazes de explorá-las em uma escala simplesmente inconcebível até poucos anos.

Enfim, os ciberataques assistidos por IA abrem as portas para estratégias extremamente sofisticadas além daquelas que podem ser concebidas pela mente humana sem ajuda. Exatamente como as análises estatísticas de IA podem revelar relações entre variáveis

para apoiar a ciberdefesa, elas podem ser usadas para identificar vulnerabilidades que os melhores especialistas humanos podem nunca ter reconhecido. Neste contexto, a chamada “IA ofensiva” – código de ataque altamente sofisticado e malicioso – permite que os cibercriminosos realizem ataques direcionados em velocidade e escala sem precedentes enquanto passam despercebidos pelo radar das ferramentas de detecção tradicionais (MIT TECHNOLOGY REVIEW INSIGHTS, 2021).

Cabe frisar que ciberataques baseados em IA não são um conceito futuro hipotético. Todos os blocos de construção necessários para o uso de IA ofensiva já existem: malware altamente sofisticado, criminosos motivados financeiramente – e implacáveis – dispostos a usar todos os meios possíveis para aumentar seu retorno sobre o investimento e projetos de pesquisa de IA de código aberto que fornecem informações altamente valiosas disponíveis no domínio público.

A seguir, apresentamos alguns exemplos de ataques que têm sido potencializados pelo uso de sistemas de IA com capacidades ofensivas.

- **Deepfakes:** os Deepfakes têm grande potencial para distorcer a realidade de muitos indivíduos para fins nefastos. Um dos abusos mais populares envolvem o uso de técnicas de IA para criar ou manipular conteúdo de áudio e visual para que pareçam autênticos. Uma combinação de “aprendizagem profunda” e “mídia falsa”, os deepfakes são perfeitamente adequados para uso em futuras campanhas de desinformação porque são difíceis de diferenciar imediatamente do conteúdo legítimo, mesmo com o uso de soluções tecnológicas (CIANCAGLINI et al., 2021). Devido ao amplo uso da internet e das mídias sociais, os deepfakes podem atingir milhões de pessoas em diferentes partes do mundo em velocidades sem precedentes. Em janeiro de 2020, o FBI alertou que a tecnologia deepfake já havia chegado ao ponto em que personas artificiais poderiam ser criadas e passar por testes biométricos (MIT TECHNOLOGY REVIEW INSIGHTS, 2021).

- Adivinhação de senha com suporte de IA. Os cibercriminosos estão empregando ML para melhorar os algoritmos para adivinhar as senhas dos usuários. Com o uso de redes neurais e Generative Adversarial Networks (GANs), os cibercriminosos podem analisar vastos conjuntos de dados de senhas e gerar variações de senhas que se ajustassem à distribuição estatística. No futuro, isso levará a possibilidade de adivinhar senhas com maiores chances (CIANCAGLINI et al., 2021).
- Personificação humana em plataformas de redes sociais. IA pode ser usada para imitar o comportamento humano, por exemplo, enganando com sucesso os sistemas de detecção de bots em plataformas de mídia social. Por meio dessa representação com suporte de IA, os cibercriminosos podem monetizar o sistema malicioso para gerar fluxos e tráfego fraudulentos para aumentar artificialmente as visualizações e consequente monetização de conteúdos e contas específico (CIANCAGLINI et al., 2021).

1.4 Caráter tipicamente internacional e multidimensional

O sistema internacional, *lato sensu*, é moldado pelo conjunto de atores institucionais estatais e não-estatais tomando decisões das mais variadas que se refletem desde na alteração dos fluxos de petróleo às alternativas a serem adotadas face à mudança climática, até as perspectivas de abertura ou fragmentação da Internet (DRAKE; CERF; KLEINWÄCHTER, 2016; KREMER; MÜLLER, 2014). Nesse viés, o aumento exponencial de usuários de Internet e do valor essencial da conectividade não somente para acessar serviços, mas pra o pleno gozo de direitos humanos (BELLI; HADZIC, 2022) contribui para a ampliação do fluxo informacional no ciberespaço¹⁴ e possibilita o surgimento de um novo campo de batalha diferente dos meios tradicionais (CLARKE, RICHARD A.; CLARKE, ROBERT K., 2015). Este fluxo informacional, por sua vez, se dá em meio a um protocolo de informação padrão, compartilhado internacionalmente.

14 “[...] cyberspace is a global domain within the information environment whose distinctive and unique character is framed by the use of electronics and the electromagnetic spectrum to create, store, modify, exchange, and exploit information via interdependent and interconnected networks using information communication technologies” (KUEHL, DANIEL T., 2009, p. 24).

Conscientes da crescente transformação digital e da ampla gama de efeitos de tal fenômeno, alguns autores destacam que a capacidade cibernética se apresenta como uma força híbrida, utilizada na camada informacional, em que existem as ações dos sistemas econômicos e políticos, e no âmbito físico, em que os mecanismos cibernéticos podem causar danos às estruturas físicas (SOUZA, 2021) e chegam até a ser incluídos em um novo tipo de guerra híbrida, particularmente evidente desde o conflito ucraniano (BELLI, 2022b; CAFÉ DA MANHÃ, 2022). Assim, as consequências das ameaças e riscos cibernéticos não se limitam à camada informacional, podendo ocasionar também efeitos sociais devastadores uma vez que podem comprometer o acesso às infraestruturas críticas do país, impactar o funcionamento de mercados, a provisão de serviços e até o bom funcionamento do processo democrático. No mesmo sentido, é importante frisar que a cibersegurança é um compromisso coletivo essencial e sua falta pode ter um impacto considerável para diferentes áreas (política, econômica, social, de segurança ou militar) e setores (setor público, privado, entidades civis, dentre outras) dentro da sociedade brasileira.

Dessa forma, é necessário que a construção de Estratégias Nacionais de Cibersegurança e que os Marcos de Cibersegurança e Soberania Digital sejam baseados numa visão sistêmica da cibersegurança que permita a cooperação entre os diferentes agentes da sociedade. A construção desta abordagem precisa ser feita a partir do nosso contexto, para que possamos chegar a uma governança de cibersegurança capaz de tutelar os riscos e ameaças enfrentadas pelo Brasil a nível nacional e internacional e garantir aos usuários das redes interconectadas o exercício dos direitos individuais e o desfrute de sua liberdade na esfera digital (OAS; GLOBAL PARTNERS DIGITAL, 2022).

1.4.1 Uma perspectiva multidimensional e multissetorial

Vale ressaltar que a cibersegurança se caracteriza pelo caráter multidimensional (BELLI, 2021b) e se apresenta como um desafio a todos os integrantes e usuários do sistema digital, em que se pode observar os níveis de impactos nos diferentes setores e áreas da sociedade.

Tradicionalmente, a cibersegurança foi fundamentada exclusivamente como uma estratégia de defesa militar ou segurança nacional (CALDERARO; CRAIG, 2020) em decorrência das ameaças internas ou externas do país. Podemos chamar este o paradigma hegemônico da cibersegurança. Tal escolha por uma resposta ofensiva (de certa forma, 'bélica') às inseguranças que surgem diante da mobilização de tecnologias e sistemas digitais reflete uma opção política que prejudica, principalmente, as pessoas: quem deveria ser o centro da proteção acaba sendo a maior vítima, ao se tornarem alvos das capacidades cibernéticas desenvolvidas para a defesa do Estado e terem direitos humanos vulnerabilizados (LIAROPOULOS, 2015).

Assim, compartilhamos do entendimento de que a esfera de proteção, assim como da participação, não deve se limitar à área de defesa militar, devido à multidimensionalidade dos ciberataques e das ameaças envolvidos. Isto posto, idealmente, uma política de cibersegurança que dê conta desta multidimensionalidade contará com a participação ativa tanto de setores públicos quanto de setores privados, sociedade civil, comunidade técnica e acadêmica. Isto traduz o que Liaropoulos (2015) descreve como uma conceitualização "positiva" da cibersegurança, ou seja, aquela que é "percebidas como o conjunto de políticas e práticas que protegem e capacitam as pessoas a exercerem seus direitos de forma livre e segura" (idem, p. 19).

Os governos estão cada vez mais interessados no desenvolvimento de Estratégias Nacionais de Cibersegurança (ENCs) capazes de abordar de maneira integrada e eficiente toda gama de questões. De acordo com a Organização dos Estados Americanos, a elaboração de uma ENC é vista como a principal ferramenta para lidar com as ameaças cibernéticas e construir medidas altamente desejáveis para preveni-las (OAS; GLOBAL PARTNERS DIGITAL, 2022). No Brasil, nossa ENC atual é abrangida pela Política Nacional de Segurança da Informacional (PNSI), cujo caráter monosssetorial contrasta com o movimento por uma abordagem mais holística das preocupações relacionadas ao tema¹⁵.

15 Na próxima seção deste trabalho, voltaremos a estes documentos, com a devida atenção. No entanto, para esta seção, que falamos do caráter multissetorial da cibersegurança, vale a menção

Dessa forma, e tendo em vista a abrangência da cibersegurança, é de suma importância que o país desenvolva, seja através de políticas públicas de incentivo aos atores privados, seja através de parcerias público-privadas (KALISZ, 2022), ações capazes de integrar os diferentes setores e áreas, incluindo instituições de ensino e produção de conhecimento científico. No entanto, é importante que não se restrinja a estas ações, uma vez que a participação popular (seja por meio de mobilizações sociais, seja por meio de instituições formais da sociedade civil) é imperativa diante da responsabilidade social compartilhada na adoção de comportamentos digitais mais seguros.

Neste viés, é imperativo o estabelecimento de uma Agência Nacional de Cibersegurança (ANC) responsável para atuar na coordenação, implementação e fiscalização do arcabouço normativo e das estratégias desenvolvidas em prol da prevenção, segurança e proteção do ciberespaço (vide, na seção 4, a proposta de Marco de Cibersegurança e Soberania Digital). Tal órgão deve desempenhar uma função de coordenação parecida à função do CGSI, porém ampliada a todas as dimensões da cibersegurança (ao invés de se concentrar somente na segurança da informação) e deve ser fortalecida por um comitê multissetorial capaz de assessorar a Agência de forma permanente.

A criação de um Comitê Multissetorial de Cibersegurança e de uma Rede Nacional de Cibersegurança, como órgãos complementares da ANC, também é imprescindível para garantir a diversidade dos setores na participação das pautas relacionadas ao tema, a contínua alimentação da ANC com os conhecimentos mais atualizados, bem como a maximização da efetividade e capilaridade da implementação e conformidade com os padrões de cibersegurança.¹⁶ A composição do Comitê Multissetorial de Cibersegurança poderia basear-se no modelo do Conselho Nacional de Proteção de Dados Pessoais e da Privacidade¹⁷ (CNPd), órgão consultivo da Autoridade Nacional de Proteção de Dados (ANPD), enquanto a estrutura da Rede Nacional de Cibersegurança poderia basear-se

a este caráter para dialogar com uma necessária atualização, proposta ao final da seção 2.

16 Veja-se a seção 4: Conclusão: uma proposta de Marco de Cibersegurança e Soberania Digital.

17 Ver <https://www.gov.br/anpd/pt-br/cnpd-2>.

no modelo do *European Cybersecurity Competence Centre and Network*.¹⁸ O papel da Rede, especificamente, consistiria no estabelecimento de uma estrutura estável capaz de apoiar a inovação, o desenvolvimento (e cocriação) e a implementação de soluções de cibersegurança, promovendo a soberania digital e coordenando a comunidade de centros de pesquisa em cibersegurança e as equipes de resposta a incidentes de segurança informática do país. Assim, é necessário que o modelo europeu seja tomado apenas como ponto de partida (mas não de chegada) para que a composição da Rede possa dar conta de toda a pluralidade do contexto brasileiro.

Dessa forma, além de ser uma autoridade reguladora completa, a ANC desempenharia também uma função de ponto focal facilitando não somente interação e cooperação com outras agências de cibersegurança – p.e. a *European Union Agency for Cybersecurity* (ENISA) ou a *Cyberspace Administration of China* (CAC) etc. – ou de coordenação temática de cibersegurança ao nível nacional, mas também estimulando a realização de parcerias multissetoriais nacionais e internacionais. Este tipo de parcerias parece extremamente útil para incentivar investimentos em pesquisas técnicas e científicas, capacitação de especialistas em cibersegurança e, sobretudo, educação digital e conscientização da sociedade sobre a cibersegurança.

Portanto, o alinhamento de esforços é essencial e deverá se dar tanto de forma multissetorial, como a partir de uma abordagem capaz de tomar em conta o caráter transnacional da cibersegurança, tendo em vista o funcionamento das tecnologias digitais, baseado em protocolos de comunicação de dados cujos arranjos são compartilhados por diferentes países.

1.4.2 Uma perspectiva Internacional

As decisões tomadas pelos Estados no exercício de seus poderes soberanos podem desencadear, e frequentemente desencadeiam, uma série de efeitos colaterais a nível internacional. Pense-se, por exemplo, nos sistemas de segurança

¹⁸ Ver https://cybersecurity-centre.europa.eu/index_en.

nacional cibernética estadunidenses, que se tornaram particularmente conhecidos e estudados por causa das revelações de Edward Snowden, exatamente há uma década, cuja consequência direta foi o enfraquecimento não somente da proteção de dados e privacidade de milhões de indivíduos ao redor do mundo, mas também uma redução da segurança e da confiança na tecnologia digital *lato sensu* e uma ataque direto à soberania nacional alheia¹⁹ (ROUSSEFF, 2013).

Assim, uma perspectiva internacional parece necessária para considerar as evoluções constantes de um ecossistema digital no âmbito do qual cada componente é inevitavelmente afetado pelos efeitos externos das escolhas dos outros, sejam tais escolhas políticas e legislativas voltadas à regulação das tecnologias digitais, seja por causa de ações e decisões tomadas por atores não-estatais como empresas, consórcios ou até grupos de hackers (BELLI, 2016, p. 318–323). Apesar de, no Brasil, os ataques mais comuns terem origem interna (CERT.BR, [s.d.]), grande parte dos ataques cibernéticos manifestam-se de forma transfronteiriça. Assim, a tutela da cibersegurança deve ser tratada pelos Estados como preocupação de dimensão simultaneamente nacional e internacional em que se tenha ampla participação não somente estatal, mas também das instituições não-governamentais para construir estratégias, mecanismos de governança e marcos regulatórios que sejam eficientes e efetivos.

No campo do estudo teórico das Relações Internacionais, o desenvolvimento da cibersegurança se concentra principalmente na defesa nacional e na militarização, conforme explicam as três

19 Como foi destacado de forma contundente pela antiga Presidenta Dilma Rousseff em sua fala de abertura da Assembleia Geral da ONU de 2013 “Como tantos outros latino-americanos, lutei contra o arbítrio e a censura e não posso deixar de defender de modo intransigente o direito à privacidade dos indivíduos e a soberania de meu país. Sem ele – direito à privacidade – não há verdadeira liberdade de expressão e opinião e, portanto, não há efetiva democracia. Sem respeito à soberania, não há base para o relacionamento entre as nações. Estamos, senhor presidente, diante de um caso grave de violação dos direitos humanos e das liberdades civis; da invasão e captura de informações sigilosas relativas as atividades empresariais e, sobretudo, de desrespeito à soberania nacional do meu país. [...] Imiscuir-se dessa forma na vida de outros países fere o Direito Internacional e afronta os princípios que devem reger as relações entre eles, sobretudo, entre nações amigas. Jamais pode uma soberania firmar-se em detrimento de outra soberania. Jamais pode o direito à segurança dos cidadãos de um país ser garantido mediante a violação de direitos humanos e civis fundamentais dos cidadãos de outro país. Pior ainda quando empresas privadas estão sustentando essa espionagem.” (ROUSSEFF, 2013).

principais teorias da área, quais sejam: o Realismo²⁰, o Liberalismo²¹ e o Construtivismo²². Apesar destas teorias tradicionais de relações internacionais conseguirem correlacionar o desenvolvimento da cibersegurança com a capacidade militar e defesa nacional, elas possuem pouco impacto prático no desenvolvimento da capacidade cibernética dos Estados.

Calderaro e Craig (2020) avaliam que o embasamento da cibersegurança em estratégias fundadas na militarização é ultrapassado. Defendem, por sua vez, que estas sejam substituídas pela capacidade de produção de conhecimento científico e técnico em cibersegurança no país. Como destacaremos na próxima seção, o aprimoramento das competências da população por meio de treinamento e capacitação é também condição essencial para o fortalecimento – ou até a construção – da soberania digital.

Tanto para países do Sul Global, quanto para países do “Norte”²³, existem evidências de que o investimento na produção de conhecimento científico e técnico é um fator determinante na influência das estratégias nacionais de desenvolvimento em diversas dimensões, inclusive no aprimoramento da economia e riquezas (TÖDTLING; LEHNER; TRIPPL, 2006). Isso é aplicável também no contexto dos

20 Conforme a Teoria do Realismo, os Estados que operam no sistema internacional possuem como fundamento resposta às ameaças ou riscos à segurança por meio de construção de esforços militares (RID; MCBURNEY, 2012 apud CALDERARO; CRAIG, 2020).

21 A Teoria do liberalismo traz a ideia de que Estados democráticos sofrem mais pressão no âmbito de investimentos da cibersegurança, devido aos apelos da população que elegeu seu representante, em comparação aos Estados autoritários. Um segundo fator relevante diz respeito sobre a estabilidade do país. Há autores que defendem a ideia de que guerras civis reduzem o investimento governamental em cibersegurança, pois todos os esforços foram concentrados na retomada da estabilização do país (STEWART, FRANCES; HUANG, CINDY; WANG, MICHAEL, 2000).

22 A Teoria do Construtivismo defende que as Organizações Intergovernamentais (Intergovernmental Organization – IGO) são essenciais para a construção de normativas de cibersegurança, uma vez que podem definir parâmetros de comportamentos, a nível internacional, aceitáveis para os Estados. Assim sendo, quanto maior o número de adesão de Estados às normas governamentais internacionais de cibersegurança, maior será a cooperação entre tais agentes para cumprir tais normativas da comunidade internacional e realizar trocas entre si. Outra ideia defendida pelos construtivistas reside no poder de prestígio, ou seja, os Estados buscam capacidades militares como forma de status, e, tal fator pode se espelhar também quando se trata da capacidade cibernética.

23 O uso da terminologia de Norte e Sul Global se alinha a uma visão pós-colonial que marca a “reafirmação da subalternidade [e] não permite que a diferença colonial seja esquecida, sendo possível verificar posições de subalternidade em relação ao sistema internacional, à dinâmica econômica, às expressões culturais, às estruturas acadêmicas e aos sistemas de pensamento” (BALLESTRIN, 2020). Os conceitos vêm sendo usados, por exemplo, em discussões a respeito de países emergentes, como no bloco dos BRICS, e processos de cooperação Sul-Sul.

estudos de cibersegurança, em que a difusão e aprimoramento do conhecimento exerce um papel primordial para garantir a liderança no campo da inovação e domínio da defesa (PAARLBERG, 2004). Além disso, nos países do Sul Global, o fortalecimento de capacidades figura de maneira preeminente como estratégia de administração contra desastres (GAILLARD; MERCER, 2013).

O conhecimento científico e técnico se manifesta em formatos variados, circula por meios formais e informais e é impactado pelas condições institucionais para o seu florescimento e fluxo (EDQUIST, 2006; LUNDVALL, 2007). A produção de conhecimento, seja por meio de pesquisa e desenvolvimento, seja por meio de treinamento e divulgação, possui relevantes impactos nos diferentes pilares da capacidade cibernética determinada pela UIT (legal, técnico, organizacional e capacitação) (ITU, [s.d.]).

A produção de artigos científicos é considerada como um fator relevante para a evolução na seara legal do país em relação ao desenvolvimento de políticas de cibersegurança. No mais, vários estudos demonstram que a falta de investimento e incentivo à pesquisa e produção de conhecimentos científicos e técnicos nos países do Sul Global é o principal responsável pelo atraso no desenvolvimento da capacidade cibernética destes países (CALDERARO; CRAIG, 2020).

Dessa forma, alinhando-se as evidências apresentadas a uma visão situada no contexto brasileiro, é importante o investimento em políticas públicas de incentivo à pesquisa e inovação na área de cibersegurança para estimular o desenvolvimento da capacidade cibernética. Isto significa não apenas o incentivo às instituições de pesquisa científica, mas o apoio – inclusive com recursos econômicos dedicados – à formação de um sistema de inovação em torno dessas tecnologias, com efetivas conexões entre os agentes do sistema.

Essa compreensão parte de uma perspectiva a respeito da política de cibersegurança como componente do posicionamento do Estado no cenário internacional, mas também como detentor e principal impulsionador da soberania digital nacional (BELLI; JIANG, 2023). Tecnologias relacionadas à cibersegurança têm caráter estratégico, devido aos desdobramentos multifacetados

já apresentados nas seções anteriores, e o alinhamento de uma nação à vanguarda tecnológica significa, neste campo, potencialmente um fator diferenciador entre soberania e vulnerabilidade, entre dependência e autonomia.

Assim, a política de cibersegurança, especialmente em países em desenvolvimento, deve levar em conta a necessidade de construção de sistemas de inovação autônomos em torno destas tecnologias estratégicas, o seu direcionamento à realização de valor público e missões sociais de grande alcance e estar inserida em um conjunto de políticas verticais e horizontais, implícitas e explícitas, facilitadoras da formação de sistemas de inovação e adaptadas ao contexto do país (CASSIOLATO; LASTRES, 2005; MAZZUCATO, 2018; MAZZUCATO; RYAN-COLLINS, 2022).

2 SOBERANIA DIGITAL E CIBERSEGURANÇA

A soberania digital refere-se à capacidade de uma dada entidade para exercer agência e capacidade regulatória sobre dados e infraestruturas digitais²⁴ (BELLI, 2021a, 2023b; 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 de 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, 2023). 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.

O assunto torna-se cada vez mais importante, à medida que a tecnologia avança e mais das nossas sociedades, economias e democracias são conduzidas online e dependentes das tecnologias digitais (BELLI; GUGLIELMI, 2022). Ao examinar este debate, é preciso destacar que os últimos anos confirmaram que a transformação digital, enormemente acelerada pela recente pandemia, nos traz enormes oportunidades, mas, se não enxergarmos, entendermos e dominarmos as tecnologias que facilitam essa transformação, a digitalização se torna uma “bomba-relógio”, na

24 Aqui o termo “infraestrutura digital” é utilizado para se referir a qualquer bem físico e lógico, ou seja, todos os tipos de hardware e software que suportam produtos e serviços digitais, em vez de apenas infraestruturas físicas que fornecem conectividade. Como tal, as infraestruturas digitais incluem também aplicações de protocolo e software que facilitam as comunicações digitais, tal como é geralmente entendido nos Estudos de Ciência e Tecnologia.

melhor das hipóteses, e uma sentença de colonização digital, na pior (AVILA PINTO, 2018; BELLI, 2023a; COULDRY; MEJIAS, 2019).

No entanto, para evitar o excesso de protecionismo e autoritarismo, as medidas de soberania digital e de cibersegurança devem ser enquadradas utilizando um pensamento sistêmico e uma abordagem centrada no ser humano, tendo claramente em mente quais são os riscos que se pretende evitar e como, mas também a que tipo de efeitos colaterais estas medidas podem conduzir e como mitigá-los.

Assim, o Brasil, como qualquer país, precisa urgentemente de uma estratégia de soberania digital, seja em sua política externa ou interna, para voltar a ser ator protagonista do próprio futuro digital e retomar seu papel de liderança nas políticas digitais não somente ao nível regional e no Sul Global, mas até global. Como destacaremos nas próximas seções, a soberania digital tem uma conexão íntima com a cibersegurança.

2.1 Como nasceu e como se popularizou o conceito de soberania digital?

Recentemente o conceito de soberania digital se tornou uma pauta europeia, ganhando popularidade e uma conotação menos negativa. Assim, desde 2020, ele é abordado no sentido de promoção da autonomia estratégica de controle sobre infraestruturas digitais (VON DER LEYEN, 2020). Esse debate popularizou enormemente o conceito e se tornou necessário diante da postura extremante imprevisível – e potencialmente danosa – da administração Trump no que diz respeito à tecnologia digital.

Neste sentido, quando o antigo presidente dos EUA, Donald Trump, começou a adotar ordens executivas como armas econômicas, para proibir o uso de software estadunidense pela chinesa Huawei e ameaçar bloquear o TikTok, a maioria dos países europeus percebeu sua dependência tecnológica e os riscos que tal situação determina (JIANG, 2019). Pela primeira vez nos últimos 30 anos as lideranças Europeias se deram conta de que eles mesmos são enormemente vulneráveis por sua falta de autonomia estratégica em âmbito tecnológico (MICHEL, 2021).

Porém o discurso sobre o conceito de soberania digital começa oficialmente em 2011, com a proposição da Organização de Cooperação de Xangai²⁵, uma organização intergovernamental liderada por China e Rússia que, em 2011, elaborou um Código Internacional de Conduta para Segurança da Informação, atualizado em 2015. O documento reafirma que “a autoridade para regular questões de política pública relacionadas à Internet é um direito soberano dos Estados” e estabelece o compromisso de “não usar as tecnologias de informação e comunicação e as redes de informação e comunicação para realizar atividades contrárias à tarefa de manter a paz e a segurança internacionais” (FMPRC, 2011).

Tal cenário se torna extremamente relevante com as revelações de Edward Snowden, depois das quais os países do bloco BRICS foram os primeiros a adotar medidas concretas para reafirmar sua soberania face às revelações de abuso de tecnologia para espionagem e atentado à soberania alheia. Os Russos introduziram a localização de dados e a construção do famoso “Runet”, o segmento autônomo de Internet russo (DAUCÉ; MUSIANI, 2021). Os chineses adotaram planos de informatização e cibersegurança e criaram a Administração Chinesa do Ciberespaço. A Índia proibiu as práticas de *zero rating*, ou seja, os aplicativos patrocinados (entre os quais havia principalmente redes sociais estadunidenses implicadas nas revelações de Snowden), consagrando a neutralidade da rede – talvez esta tenha sido a medida que mais fez pela soberania digital da Índia (BELLI, 2021a, 2021c).

A maioria dos observadores naquela época perceberam a iniciativa indiana como uma grande vitória para a liberdade expressão e para os consumidores, mas na verdade um dos principais impactos da adoção dessa política foi a preservação do potencial do ecossistema digital nacional, da concorrência e da inovação

25 A Organização de Cooperação de Xangai, geralmente conhecida como *Shanghai Cooperation Organization*, (SCO), é uma organização intergovernamental voltada para a cooperação política, econômica e de segurança. Abrange três quintos do continente euroasiático, 40% da população mundial e mais de 20% do PIB global. Ver <http://eng.sectscsco.org>.

local, ou seja, o fortalecimento da soberania no sentido de auto-determinação digital. Proibindo o patrocínio de somente alguns aplicativos dominantes – o que acontece na maioria dos países do mundo – os indianos evitaram que os dados da população fossem concentrados somente por algumas plataformas dominantes e permitiram que as *startups* indianas fossem acessíveis em pé de igualdade para todos os usuários. Essas *startups* agora são gigantes e a Índia está vivendo uma *belle époque* da inovação (PARSHEERA, 2020), passando a ser o terceiro lugar com mais *startups* do mundo (CHOUDHURY; SHARMA; JAIN, 2019; SORENSEN, 2022). Os indianos entenderam extremamente bem o valor da soberania digital.

2.2 Quais são os elementos fundamentais da soberania digital?

A soberania digital é um assunto multidimensional (BELLI, 2023a; COUTURE, 2020). Refere-se à capacidade de exercer poder e controle sobre infraestruturas digitais e dados e implica ser apto a entender os efeitos – positivos e negativos – que cada escolha tecnológica determina. Neste sentido, é essencial ter uma visão sistêmica para entender como os diferentes elementos dos ecossistemas digitais se inter-relacionam e como desenvolver, usar e regular a tecnologia ao invés de ser regulado por ela (BELLI; JIANG, 2023).

Seria ingênuo pensar que, tomando as revelações de Snowden como referência, ao longo da última década a situação evoluiu de maneira radicalmente diferente. Em julho 2020, no celebre caso Schrems II²⁶, o Tribunal de Justiça Europeu decidiu anular o “*Privacy Shield*”, mecanismo que permitia o fluxo transatlântico de dados entre a União Europeia (UE) e os Estados Unidos (EUA), com o fundamento de que o sistema de vigilância estadunidense torna impossível garantir a proteção de dados pessoais exigida pelo Regulamento Geral de Proteção de Dados da União Europeia (BELLI; DONEDA, 2021).

26 Ver Caso C-311/18 *Data Protection Commissioner v Facebook Ireland Limited and Maximilian Schrems*, dito “Schrems II”.

Precisamos, portanto, considerar três dimensões fundamentais da soberania digital para construir nossa visão estratégica. Primeiramente, soberania digital é autodeterminação²⁷, no sentido mais puro desse direito fundamental. Determinar livremente seu desenvolvimento econômico, político, social e cultural.

Assim, a soberania digital é essencial para escolher e organizar independentemente o desenvolvimento de uma Nação. Porém, nas últimas décadas, pouquíssimos governos tiveram uma postura consciente, estratégica e coordenada ao definir suas políticas de educação, pesquisa, de desenvolvimento industrial, de expansão de suas infraestruturas digitais e de governança de dados para fortalecer a soberania digital. O Brasil precisa urgentemente dessa postura, sem que se torne uma justificativa para protecionismo, mas como pilar fundamental do desenvolvimento nacional.

Esta dimensão coincide com a noção de “Boa Soberania Digital” que se baseia na ideia de que qualquer entidade (não apenas o Estado) pode ser soberana digitalmente enquanto for capaz de compreender o funcionamento da tecnologia digital e utilizá-la para seu próprio benefício e progresso, inclusive criando novas tecnologias. Nessa perspectiva, portanto, a soberania digital é

27 O direito à autodeterminação desempenha um papel fundamental para permitir aos indivíduos gozarem dos seus direitos humanos inalienáveis e, por este motivo, está consagrado como primeiro artigo tanto da Carta das Nações Unidas como dos Pactos Internacionais de Direitos Humanos. De acordo com estes três instrumentos de direito internacional, os Estados concordaram que “todos os povos têm direito à autodeterminação” e que “em virtude desse direito, são livres de determinar o seu estatuto político e de prosseguir o seu desenvolvimento econômico, social e cultural”. Embora a autodeterminação seja geralmente discutida na sua dimensão externa, ou seja, a independência territorial e política em relação aos atores externos, é essencial salientar que, neste trabalho, estamos a referir-nos à dimensão interna da autodeterminação, ou seja, o direito de determinar e prosseguir livremente o seu desenvolvimento econômico, social e cultural, inclusive através da escolha, desenvolvimento e adopção independente das tecnologias digitais. Tal concepção é também corroborada pelo direito fundamental à “autodeterminação informativa” como expressão do direito humano a ter e desenvolver uma personalidade, reconhecido pela primeira vez pelo Supremo Tribunal alemão, no caso do Censo de 1983. É importante salientar que o direito fundamental ao livre desenvolvimento da personalidade é formalmente reconhecido internacionalmente. O artigo 22 da Declaração Universal dos Direitos do Homem afirma que “todas as pessoas têm direito à realização dos direitos necessários à sua dignidade e ao livre desenvolvimento da sua personalidade”, enquanto o Pacto Internacional dos Direitos Económicos, Sociais e Culturais consagra este princípio fundamental relativo ao direito de todas as pessoas à educação e à participação na vida pública. Em particular, os signatários do Pacto concordaram que o direito à educação “será dirigido ao pleno desenvolvimento da personalidade humana e ao sentido da sua dignidade [...] e permitirá que todas as pessoas participem efetivamente na sociedade” (Artigo 13.1). Além disso, o livre desenvolvimento da personalidade é explicitamente considerado como fundamental para o exercício do direito fundamental de “participar na vida cultural [e] usufruir dos benefícios do progresso científico e das suas aplicações” (Artigo 15). Ver Belli et al. (2017; 2019).

uma função da compreensão e do empoderamento pela tecnologia. Apesar de não possuir uma estratégia explícita de soberania digital, o Brasil oferece exemplos interessantes de como esta concepção de soberania digital já existe e pode ser construída, seja adotando tanto uma abordagem *top-down* ou *bottom-up*.

No primeiro caso, infraestruturas digitais públicas podem ser criadas e gerenciadas pelo estado, como o “sistema de pagamento Pix”²⁸ (BCB, [s.d.]) que permitiu ao Brasil se emancipar da total dependência de atores estrangeiros (as empresas Visa e MasterCard no que diz respeito aos pagamentos eletrônicos). No caso das iniciativas *bottom-up*, cabe destacar a existência de iniciativas de redes comunitárias²⁹, que permitem a comunidades locais construir sua própria infraestrutura de acesso à Internet e gerenciá-la como um bem comum, ou também iniciativas de cooperativismo de plataforma (GROHMANN, 2021), que permitem a grupos de trabalhadores e desenvolvedores se associarem para fornecer serviços digitais.

Uma segunda dimensão da soberania digital, particularmente relevante para este trabalho, é a cibersegurança, nas suas diferentes camadas. Ser soberano significa ser capaz de controlar e proteger suas próprias infraestruturas críticas, suas redes eletrônicas,

28 É importante enfatizar que, antes do Pix, a única opção disponível para processar pagamentos eletrônicos instantâneos em tempo integral no Brasil era utilizar as redes das gigantes estrangeiras de pagamentos eletrônicos Visa e Mastercard, que cobram uma taxa de 3% em cada transação, além de centralizar a coleta de dados de todos os seus usuários (CHRISTL, 2017). Esses pontos são a principal razão pela qual o desenvolvimento de infraestruturas digitais públicas como o Pix é enormemente relevante do ponto de vista de uma boa soberania digital. Portanto, estimular uma infraestrutura pública de pagamento digital doméstica é fundamental para alcançar três objetivos: simplificação e democratização dos pagamentos, redução da concentração de mercado e dados e emancipação da dependência de intermediários estrangeiros, e fornecimento de uma visão única sobre a economia nacional para o Banco Central do Brasil (em vez de para dois atores estrangeiros), revertendo assim uma tendência que caracteriza o Sul Global e que muitos estudiosos têm definido como “colonialismo de dados” (COULDRY; MEJIAS, 2019).

29 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, 2018a), 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, 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 moradores de favelas 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.

seus bancos de dados e as infraestruturas políticas que permitem a governança do País. Cada uma dessas camadas é vulnerável a ataques e tais ataques são perpetrados com frequência basicamente cotidiana no Brasil.

Nossas infraestruturas críticas estão sendo digitalizadas e automatizadas para incrementar sua performance, mas, com frequência, sem a menor consideração dos riscos que a falta de cibersegurança produz. Como destacamos na introdução deste trabalho, exemplos de ataques hackers derrubando empresas, tribunais, municípios e ministérios são superabundantes. Até o bom funcionamento democrático depende da capacidade das instituições de exercer controle sobre a estrutura política do País, que se tornou intimamente interconectada com tecnologias digitais.

As ameaças extremamente tangíveis que surgem de redes sociais nos demonstram o quanto é flexível e porosa a fronteira entre online e off-line e o quanto é necessário garantir o controle democrático das infraestruturas digitais para assegurar a (ciber) segurança e a soberania nacional. Uma democracia, uma economia e uma sociedade constantemente vulneráveis não podem ser chamadas de digitalmente soberanas.

Em terceiro lugar, a soberania digital é soberania sobre dados pessoais e críticos, sendo capaz de explorá-los economicamente, estrategicamente e tecnologicamente, ao invés de oferecer esses ativos valiosos para atores estrangeiros sem entender seu verdadeiro valor. Assim, continuamos a proclamar que os dados são o “petróleo do Século XXI” (PALMER, 2006) – metáfora muito pouco correta conceitualmente, porém bem apropriada economicamente –, mas de fato entregamos uma concessão para explorar essa riqueza *ad infinitum* para as mesmas pouquíssimas empresas estrangeiras implicadas nas revelações de Snowden de 2013.

Na verdade, no Brasil, e na maioria dos países do Sul Global, a enorme maioria dos usuários de Internet são, na verdade, usuários de redes sociais, que estão entre os pouquíssimos aplicativos subsidiados nas franquias dos planos de internet móvel. Essa situação leva os usuários mais pobres, ou seja, a enorme maioria de usuários, a usar principalmente redes sociais nos próprios *smartphones*

porque são as únicas percebidas como “de graça”. Na verdade, o usuário e o País todo pagam com seus dados e sua soberania digital.

Não é de se maravilhar que os internautas brasileiros passam em média 4 horas por dia em redes sociais e 95% deles usam sua conexão principalmente em aplicativos de mensageria instantânea, como destaca o IBGE (2018), e que os aplicativos Facebook e WhatsApp – ambos patrocinados no âmbito de ofertas de *zero rating* – são os mais instalados nos *smartphones* brasileiros (IDEC; INSTITUTO LOCOMOTIVA, 2021). Não é de se maravilhar também que os lucros bilionários realizados pelas *big tech* nos últimos anos não são devidamente tributados, considerando que o insumo (dados) é extraído globalmente, porém é processado e gera renda e inovação – e informações altamente estratégicas – em servidores estrangeiros e com esquema de erosão fiscal e transferência de lucros altamente questionáveis (ACTIONAID, 2020).³⁰

O Brasil, porém, não é condenado a ser uma colônia digital. Na verdade, foi até um precursor da soberania digital, com as políticas da primeira administração Lula sobre software livre. Por anos o Brasil foi uma referência mundial, oferecendo uma visão diferente de como o software podia ser enxergado como ferramenta libertadora e de empoderamento, ao invés de um instrumento de extração de dados e de colonização digital.

O software livre foi abandonado em 2016 pela administração Temer, que resolveu contratar a empresa Microsoft para digitalizar a administração pública. Hoje, é muito difícil voltar à soberania digital, mas não é impossível. Em vários casos, já existe legislação que poderia ajudar enormemente se fosse simplesmente aplicada. A regulamentação do Marco Civil da Internet pode, e deveria, ser aplicada para proibir as práticas de *zero rating* (BELLI, 2018b). Além de consagrar a autodeterminação informativa, a Lei Geral de Proteção de Dados (LGPD) estabelece mecanismo para regular as transferências de dados internacionais e a interoperabilidade entre

30 Uma pesquisa da ActionAid Internacional de 2020 revelou que vinte países em desenvolvimento podem estar perdendo até US\$ 2,8 bilhões em receita tributária do Facebook, Alphabet Inc. (empresa controladora do Google) e Microsoft devido a falhas em regras tributárias globais. Particularmente, Índia, Indonésia, Brasil, Nigéria e Bangladesh são os estados com as maiores “lacunas fiscais” dessas três empresas (ACTIONAID, 2020).

serviços. Infelizmente, até hoje, nenhum dos dois foi regulamentado pela Autoridade competente.

Por fim, para plena realização de soberania digital – bem como da cibersegurança – é essencial uma forte ação de capacitação e treinamento multigeracional, almejando não somente as novas gerações, mas também aquelas que, apesar de já terem concluído as etapas de educação do nível básico (sobretudo considerando as negações ao direito à educação que caracterizam a realidade brasileira), nunca foram preparadas para os desafios da tecnologia digital. E pior: não foram apresentadas à lógica de funcionamento das novas ferramentas e sistemas, para que possam cocriar tecnologias mais adequadas aos múltiplos contextos locais e para que possam estar preparadas para as rápidas transformações e combinações de ameaças de que falamos na seção 1.2.

Tal falta de preparação e conhecimento crítico da população geral cria uma enorme vulnerabilidade em termos de cibersegurança e impossibilita a criação de uma Nação digitalmente soberana. Neste sentido, o Brasil precisa de uma estratégia séria de soberania digital baseada em um papel central da cibersegurança, do pensamento sistêmico, de investimentos estratégicos e, sobretudo, do fortalecimento dos recursos humanos, inclusive modernizando radicalmente suas políticas educacionais³¹. Além disso, o Brasil precisa atualizar currículos escolares e investir na formação, capacitação, pesquisa e desenvolvimento, de forma que não sejam valorizadas apenas competências e habilidades – que não devem se confundir com construção de conhecimento³². Aprender a programação de software livre, por exemplo, deveria ser parte dos currículos de ensino básico³³. As políticas elaboradas nos últimos anos e que tentaram abordar o assunto, no entanto, não dão conta destes desafios, conforme veremos a seguir.

31 Ver seção 2.2.1.

32 Este desafio se torna particularmente complexo diante das novas políticas públicas em curso na educação nos últimos anos, como a Reforma do Ensino Médio, que institui os itinerários formativos.

33 Interessante notar que, dentre os currículos que referência disponibilizados pelo Centro de Inovação para Educação Brasileira (CIEB), não há qualquer referência à software livre – conforme buscas realizadas na plataforma que disponibiliza os currículos – cf <https://curriculo.cieb.net.br/buscar/software%20livre>. O CIEB foi um dos principais institutos responsáveis pela elaboração de documentos que instruíram a Política Inovação Educação Conectada (PIEC) que pensa na incorporação de recursos educacionais digitais na educação básica.

2.2.1 A necessária modernização da política educacional para um país digitalmente soberano

A educação precisa ser enxergada como alicerce fundamental para a criação e fortalecimento da soberania digital, bem como o fomento da cultura em cibersegurança. Assim, uma política educacional voltada à construção da soberania digital precisa considerar pelo menos quatro dimensões fundamentais.

Primeiramente, acesso significativo à conectividade. Isso implica acesso não discriminatório e universal à Internet, possibilidade de usar dispositivos apropriados (sendo impossível por exemplo trabalhar e desenvolver tecnologia somente usando um smartphone com acesso móvel limitado) e volume de dados apropriado. Em segundo lugar, acesso significativo a aplicativos de software. Isso envolve educação digital com enfoque especial na programação, uso e desenvolvimento de software livre e aberto.

Em terceiro lugar, acesso significativo a conteúdo educacional. Isso implica criar exceções apropriadas aos direitos autorais para permitir o 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, parece necessário considerar os riscos que tecnologias digitais (tais como plataformas de educação a distância) não auditadas devidamente podem gerar para o pleno gozo dos direitos individuais e a soberania digital nacional lato sensu.

No Brasil, atualmente, contamos com três políticas principais que, em âmbito federal, pensam os atravessamentos das tecnologias digitais com as práticas educacionais (em nível básico e superior): a política de garantia de acesso à internet para fins educacionais (Lei 14.172/2021), a política de inovação e educação conectada (Lei 14.180/2021) e a política nacional de educação digital (Lei 14.533/2023). É preciso que estas políticas sejam complementadas, para que possamos avançar na consolidação da soberania digital do País.

A Lei 14.172/2021, por exemplo, foi elaborada para dar assistência aos diferentes entes federativos no acesso à Internet para continuidade das atividades educacionais. A política, porém, pensava na garantia da conectividade somente para o período da pandemia,

sem levar em consideração todas as desigualdades sociais que ficaram em evidência ao longo da crise sanitária. As desigualdades materiais, relativas à conexão (e também 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 “acesso” (IDEC; INSTITUTO LOCOMOTIVA, 2021)), reforçam outros processos discriminatórios e de dominação em curso no país, que marcam a educação pública. Nos parece, porém, que os aprendizados da pandemia não serviram para reforçar o acesso à educação, por meio da instituição de políticas que, em âmbito federal, garantissem o apoio à conectividade não só em momentos de crise, mas sim enquanto reconhecimento de um direito de toda a população.

A política traz respostas pontuais ao cenário de acesso e permanência, desconsiderando toda a realidade concreta de injustiças sociais e exacerbação de *digital divides* que persistem para além da pandemia. Além disso, ela limita o uso de internet para fins educacionais à educação básica – e não enfrenta a necessária garantia de acesso e educabilidade das diferentes gerações em relação aos novos desafios e lógicas incorporadas por tecnologias digitais. É possível ainda que haja problemas de soberania dos dados, uma vez que empresas internacionais (art. 5º) também poderiam prestar o serviço de acesso à conexão e que a prestação dos serviços de internet era condicionada ao fornecimento de dados pessoais dos beneficiários da política (art. 4º), sem muitas previsões com relação às obrigações procedimentais para o tratamento desses dados.

A Lei 14.180/2021, que institui a PIEC (Política de Inovação e Educação Conectada), por sua vez, aborda a incorporação de recursos digitais nas práticas pedagógicas. Baseada em um modelo importado da Holanda (CIEB, 2021), a política se alinha às reformas educacionais, frequentemente criticadas pelo caráter marcadamente neoliberal dos últimos anos, como a uniformização dos currículos a partir da Base Nacional Comum Curricular e a Reforma do Ensino Médio (que valoriza a técnica, no lugar do pensamento crítico ou autonomia e pluralidade na construção de conhecimento). Para além de reproduzir a atuação comum de importação de fundamentos conceituais não necessariamente adaptáveis e

úteis no contexto brasileiro, a política não enfrenta os desafios que são introduzidos pela incorporação de novas tecnologias.

Por exemplo, conforme apresentam Rizzini, Araújo e do Couto (2022), o fechamento das escolas públicas durante a pandemia levou ao aumento da exposição de crianças e adolescentes a violências (inclusive, violência sexual) mediadas pelo uso de tecnologias digitais. Este tipo de preocupação poderia ser incorporado pela política (que se valeu da experiência pandêmica para elaboração), que é silente em relação aos efeitos colaterais que podem ser produzidos pelo ensino a distância. Além disso, a PIEC também se mostra insuficiente para apoiar a construção da soberania digital, ao propor a adoção de currículos construídos de maneira verticalizada, reforçando o distanciamento da sociedade em relação aos temas de tecnologias digitais, ao invés de embasar a aprendizagem em aplicação concreta de conceitos a exemplos e situações próximos do público-alvo, portanto dificultando sua apreensão crítica.

Este ano, também entrou em vigor a Política Nacional de Educação Digital (Lei 14.533/2023), cujas previsões dialogam com a Lei de Diretrizes e Bases da Educação Nacional. A política estabelece como seus objetivos (art. 2º) “inclusão digital”, “educação digital escolar”, “capacitação e especialização digital” e pesquisa e desenvolvimento em TICs. A política apresenta elementos importantes, como a separação entre educação e capacitação (de habilidades e competências digitais), que são frentes distintas as quais não podem ser confundidas sob risco de cairmos em uma abordagem tecnicista da educação digital³⁴. Também está presente o componente multigeracional, já que a educação escolarizada (em nível básico) é apenas um dos eixos pelos quais as ações da política devem passar, mas não o único, considerando o geral despreparo de todas as gerações no que diz respeito ao entendimento do funcionamento de tecnologias digitais e os efeitos de tais tecnologias.

Para estimular o aprimoramento e atualização constante das políticas educacionais, nos parece preciso avançar em relação ao diálogo multissetorial capaz de enfrentar as múltiplas preocupações de

³⁴ Por exemplo, uma abordagem que seja pautada somente em preocupações do campo da segurança da informação, reproduzindo uma visão sobre a cibersegurança que, conforme falamos na seção 1, já foi superada.

cibersegurança e à instituição de mecanismos para garantir outras dimensões da soberania digital, como a autodeterminação (inclusive autodeterminação informativa sobre os dados pessoais) e a participação popular no desenvolvimento de novos sistemas e tecnologias digitais.

Iniciativas como o *prato feito*, voltada para difusão de informação em cuidados digitais, da Rede Transfeminista de Direitos, demonstram como a educação para o uso mais seguro de tecnologias digitais pode ser feita a partir de referências e urgências próprias, com linguagem alinhada a outras urgências do país, favorecendo o “rompimento da lógica de mercado, nos ajudando a transformar nossa relação pessoal com a tecnologia em algo mais saudável, potencializando redes e serviços que prezam e compartilham dos mesmos valores que os nossos”, como aponta o site da iniciativa (REDE TRANSFEMINISTA DE CUIDADOS DIGITAIS, [s.d.]). Outra iniciativa que merece destaque são os cursos oferecidos pelo Núcleo de Tecnologia do MTST (Movimento dos Trabalhadores sem Teto), que, baseados na metodologia desenvolvida por Paulo Freire nos círculos de cultura voltados para alfabetização de adultos, conduz as práticas educativas em programação a partir da centralidade da experiência prática e criação de resultados concretos ao final do curso (como desenvolvimento de aplicações com importância prática para a comunidade atendida pelos cursos, por exemplo) (MTST, [s.d.]).

O papel de organizações sociais e políticas 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).

Convencidos da existência de um enorme capital de criatividade e talento no País, acreditamos que a adoção de políticas capazes de promover a soberania digital possa permitir – em tempos razoavelmente breves – que o Brasil se torne não somente um exportador de tecnologia, mas uma liderança mundial. Neste sentido, é necessário enxergar brasileiras e brasileiros não somente como consumidores, mas como criadores da tecnologia do futuro.

2.2.2 A conexão entre soberania digital e Inteligência artificial

A história da Inteligência Artificial (IA) no Brasil é uma jornada marcada por avanços e contribuições significativas. Nos anos 1960 e 1970, o país começou a explorar os conceitos fundamentais da IA, com instituições renomadas como o Instituto Nacional de Pesquisas Espaciais (INPE) e a Universidade de São Paulo (USP) desempenhando papéis de destaque nessa área. Nesse período, pesquisadores pioneiros como Ney Moura Brasil desenvolveram estudos inovadores em lógica fuzzy e redes neurais artificiais, estabelecendo as bases para o desenvolvimento da IA no Brasil.

À medida que a computação avançava e novas tecnologias surgiam, a IA ganhou visibilidade nas décadas seguintes. Nos anos 1980, o Ministério da Ciência e Tecnologia criou o Programa de Informática na Educação (PROINFO), que impulsionou a aplicação da IA na educação. Já nos anos 1990, instituições acadêmicas como a Universidade Federal do Rio Grande do Sul (UFRGS) e a Universidade de Campinas (UNICAMP) estabeleceram grupos de pesquisa dedicados à IA, contribuindo para avanços em áreas como visão computacional, processamento de linguagem natural e aprendizado de máquina.

Com o avanço das tecnologias de computação e a crescente demanda por soluções inteligentes, a IA continuou a se expandir no Brasil nos anos 2000. Empresas e startups nacionais começaram a investir em aplicações de IA nos setores de saúde, finanças, logística e atendimento ao cliente, impulsionando o crescimento e a adoção da tecnologia em diferentes áreas da sociedade.

Porém é importante frisar que, apesar do terreno fértil destacado anteriormente, o país não pode ser definido como realmente soberano em termos de IA enquanto os dados da população brasileira são concentrados principalmente em um número muito limitado de plataformas de redes sociais, patrocinadas por meio dos supramencionados planos de *zero rating*; e enquanto as infraestruturas digitais essenciais pelo desenvolvimento da IA, em termos de hardware e software, não desenvolvidas nacionalmente, mas

são principalmente fornecidas por provedores estrangeiros que detêm, em última instância, o controle sobre tais infraestruturas.

Para estimular um uso sustentável da IA e a soberania digital no âmbito da qual a IA seja desenvolvida e usada no interesse público brasileiro, não é simplesmente necessário garantir que a IA seja regulada³⁵. É necessário também que o acesso à IA seja democratizado, e que os diferentes elementos que compõem os sistemas de IA sejam estudados, entendidos e desenvolvidos no Brasil (BELLI, 2023), evitando a exclusão digital e promovendo a inclusão de todos os segmentos da sociedade. Somente essa situação pode permitir que seja mantida a capacidade individual e coletiva de exercer agência e controle sobre os sistemas de IA.

Nesse sentido, a colaboração entre o setor público, o setor privado, a academia e a sociedade civil se torna crucial para enfrentar esses desafios e explorar ao máximo os benefícios da IA, implementando uma visão de soberania digital compartilhada. Através da criação de parcerias estratégicas, é possível reunir os conhecimentos e recursos de diferentes atores, estimulando a troca de ideias e impulsionando a inovação no campo da IA. O estímulo à pesquisa e ao desenvolvimento também desempenha um papel fundamental nesse contexto. Investimentos contínuos em pesquisas de ponta, incentivos à formação de grupos de trabalho e colaborações interdisciplinares podem impulsionar a criação de soluções inovadoras e fortalecer a competitividade do Brasil no cenário global da IA.

Além disso, é essencial investir na capacitação de profissionais especializados em IA, impulsionando não apenas o desenvolvimento tecnológico, mas também o avanço econômico do país. Por meio de programas de educação e treinamento, é possível formar uma força de trabalho qualificada e preparada para atuar nos mais

35 A construção de um ambiente regulatório adequado é um passo fundamental para o impulso da IA no Brasil. Regulamentações claras e atualizadas são necessárias para garantir a ética, a segurança e a transparência no uso da tecnologia, além de promover a confiança tanto dos usuários quanto dos desenvolvedores de soluções de IA. Essas regulamentações devem ser elaboradas em diálogo com todos os setores envolvidos, de forma a considerar diferentes perspectivas e necessidades. No Brasil, o avanço da Inteligência Artificial (IA) tem despertado a necessidade de estabelecer um marco regulatório que oriente seu desenvolvimento e uso responsável. Nesse sentido, a discussão sobre o marco regulatório da IA tem ganhado relevância e está em andamento no país.

diversos setores que se beneficiam da IA. Isso inclui áreas como saúde, finanças, indústria, agronegócio e serviços, que estão cada vez mais incorporando soluções baseadas em IA para melhorar a eficiência operacional, otimizar processos e impulsionar a inovação. Ao formar novos profissionais especializados em IA, o Brasil fortalecerá sua base de conhecimento e estimulará a geração de empregos qualificados. A atualização e requalificação dos profissionais já inseridos no mercado de trabalho também desempenham um papel fundamental nesse contexto. Com a rápida evolução da IA, é importante que os profissionais estejam atualizados sobre as mais recentes tecnologias, ferramentas e práticas, a fim de se adaptarem às demandas do mercado e contribuírem de forma efetiva para o avanço da IA no país.

A capacitação de profissionais em IA não apenas impulsiona o avanço tecnológico e econômico, mas também estimula a inovação e a criação de soluções que atendam às necessidades e desafios específicos do Brasil. Ao desenvolver uma força de trabalho especializada e atualizada, o país poderá aproveitar ao máximo os benefícios da IA, impulsionando a produtividade, a eficiência e o crescimento em diversos setores. Dessa forma, ao investir na capacitação de profissionais em IA, o Brasil estará não apenas se preparando para enfrentar os desafios e aproveitar as oportunidades da era da IA, mas também construindo uma base sólida para impulsionar o desenvolvimento econômico sustentável e promover a competitividade no cenário global.

2.3 Qual é a conexão entre soberania digital e cibersegurança

A discussão sobre soberania digital se justapõe enormemente – até englobar – às políticas, mecanismos de governança e iniciativas destinadas a promover a cibersegurança e a moldar a transformação digital. De fato, a adoção de tecnologias digitais pode facilitar enormes avanços a serem postos ao serviço das pessoas, mas também pode ser armada contra indivíduos, empresas e Estados-nação. Nesta perspectiva, parece natural considerar a enorme e constantemente crescente sobreposição entre soberania digital e segurança cibernética.

A elevação da soberania digital e da cibersegurança a uma prioridade nacional e a elaboração e implementação conjuntas de políticas e ações destinadas a reforçá-las parece ser a opção mais desejável, uma vez que incorpora a soberania digital e a cibersegurança na concepção e execução de programas de transformação digital. No entanto, é importante salientar que as abordagens existentes tanto em relação à cibersegurança como à soberania digital oferecem alguns exemplos reveladores de como a implementação de políticas e projetos de cibersegurança e soberania digital – mesmo os mais bem intencionados – pode tornar-se disfuncional e contraproducente ou mesmo perigosa quando faltam uma visão a longo prazo, fortes salvaguardas e mecanismos de monitoramento sólidos (BELLI; GUGLIELMI, 2022).

Como destacado precedentemente, é importante notar que tanto a soberania digital como a cibersegurança são itens multidimensionais, uma vez que existem vários fatores que contribuem para a sua realização. Do micro ao macro, a soberania digital e a cibersegurança sobrepõem-se no seu objetivo final de assegurar a capacidade de controlar os próprios dados, incluindo tanto os dados pessoais, quanto informações importantes que revelam o funcionamento de uma organização ou sistema de infraestruturas críticas. Nesta perspectiva, para promover o desenvolvimento seguro e utilizar redes, sistemas e bases de dados digitais, protegendo-os contra ciberataques e outras formas de ameaças digitais, é essencial estabelecer uma vasta gama de medidas, incluindo mecanismos de avaliação e certificação de riscos, regulamentação específica, normas técnicas e sistemas de monitoramento, bem como processos de desenvolvimento de capacidades, cooperação e governação e esquemas de financiamento seguros e bem concebidos.

Criticamente, para alcançar a soberania digital, as nações e quaisquer entidades devem investir no seu próprio desenvolvimento digital. Isto inclui investimentos estratégicos no desenvolvimento de capacidades, investigação, desenvolvimento e manutenção de infraestruturas digitais robustas e atualização contínua da força de trabalho, *hardware* e *software*. Claramente, seria ingênuo pensar que o reforço da cibersegurança e da soberania digital poderia ser alcançado sem uma instituição dedicada, capaz de supervisionar

adequadamente a implementação da regulamentação da cibersegurança e soberania digital ao mesmo tempo que coordena com as partes interessadas nacionais e internacionais para facilitar a cooperação *multistakeholder* mais fluida e harmoniosa (BELLI, 2016).

Um grande desafio para as políticas de soberania digital e de cibersegurança é considerar os efeitos externos que elas podem implantar, tanto no que diz respeito à fragmentação da Internet como à proteção dos direitos humanos. Isto significa que os esforços para afirmar a soberania digital e garantir a cibersegurança devem ser sempre planejados e executados no contexto de uma avaliação de impacto bem estruturada, capaz de identificar e mitigar os riscos e as externalidades negativas. Nesta perspectiva, para além da instituição de um regulador forte e independente de cibersegurança e soberania digital, é essencial planejar um sólido desenvolvimento de capacidades e investimentos para aprimorar os recursos humanos e financeiros, que são vitais para o sucesso tanto da soberania digital, como das estratégias de cibersegurança.

3 CIBERSEGURANÇA NO BRASIL: MAPEAMENTO E ANÁLISE CRÍTICA DO ARCABOUÇO NORMATIVO VIGENTE

Nesta seção, abordamos instrumentos normativos brasileiros no nível federal que envolvem medidas de cibersegurança, *lato sensu*, com o objetivo de identificar os principais pontos de avanço em relação à Política Nacional de Segurança da Informação e à E-ciber. Nossa finalidade é propor ajustes que podem contribuir ao aprimoramento da efetividade da política nacional, e retomar as medidas necessárias para a promoção da segurança das pessoas e seus direitos como valor central, em interlocução com o atual arranjo político de cibersegurança do País.

Antes de analisar propriamente as normas, é interessante repisar o que foi abordado na introdução deste artigo: a cibersegurança no Brasil, bem como em qualquer outro País, é um ecossistema com múltiplas dimensões. Tal multidimensionalidade impõe a adoção de um mecanismo de governança e de um arcabouço normativo capazes de considerar os diversos setores da sociedade e iniciativas existentes sobre o tema de forma harmônica, para garantir a cibersegurança de maneira eficiente e efetiva.

Nesta perspectiva, é preciso que haja um alinhamento na estratégia nacional por meio de um marco normativo que traga padrões mínimos para os níveis operacionais, organizando suas dimensões e estabelecendo os princípios, o sistema de governança e formas de cooperação entre os diferentes setores. Diante das novas movimentações do atual governo e na proposição de normas que passam pela responsabilização por comportamentos em plataformas digitais³⁶, e com o fim da vigência da E-Ciber em 2023 (de que trataremos a seguir), temos a oportunidade de redesenhar os arranjos atuais. Podemos repensar os caminhos que queremos dar à cibersegurança no País, centrados na proteção das pessoas,

36 Aqui, fazemos referência ao Pacote Pela Democracia, que contempla projetos em diferentes eixos. Sobre os projetos do governo em relação à desinformação, cf GALF (2023).

na garantia de direitos humanos, na sustentabilidade e na soberania digital.

Hoje, no Brasil, a cibersegurança é organizada de forma setorizada, de acordo com as políticas, definições e critérios de cada órgão público, em cada um dos Poderes do Estado. No Poder Executivo Federal, o Decreto nº 9.637/2018, implementa a Política Nacional de Segurança da Informação e Governança da Informação (PNSI) no âmbito da Administração Pública Federal. No arranjo herdado do último governo, esta Política se desdobra em outros documentos, abrangendo a referida ENC do Brasil. Diante de suas previsões, a PNSI favorece uma indesejada compartimentação da regulação de cibersegurança no País, como passaremos a abordar.

O decreto da PNSI trata, principalmente, da dimensão da segurança da informação como algo abrangente que engloba (artigo 2º): a área da “segurança cibernética”, da “defesa cibernética”, da “segurança física e de proteção de dados”, além de “ações para assegurar a disponibilidade, integridade, confidencialidade e autenticidade das informações”. Ao incorporar a segurança cibernética como dimensão da segurança da informação, a política adota uma abordagem conceitualmente questionável, sendo a segurança a informação tipicamente categorizada como uma dimensão da cibersegurança, não o contrário. Outrossim, esta abordagem limita-se à reprodução da ultrapassada visão da cibersegurança reduzida à adoção de princípios CIA e IAA na condução de suas atividades em sistemas ou com tecnologias digitais: elementos importantes, porém insuficientes, quando não acompanhados das demais dimensões necessárias para frear e obstaculizar de maneira completa e sistêmica as ameaças e ataques já explorados na seção 1.2.

O decreto prevê dois instrumentos para a implementação de sua política, a Estratégia Nacional de Segurança da Informação (E-Ciber), nossa ENC, e os planos nacionais. No que se refere à Estratégia Nacional de Segurança da Informação, o decreto prevê que a E-Ciber seja elaborada à semelhança de seus princípios, com os seguintes blocos de enfoque temático (artigo 6º): (i) a segurança cibernética, (ii) a defesa cibernética, (iii) a segurança das infraestruturas críticas; (iv) a segurança das informações sigilosas; e (v) a proteção contra vazamento de dados.

Por outro lado, os planos nacionais são responsáveis por promover o detalhamento das ações estratégicas, o planejamento, a coordenação de atividades, bem como o detalhamento das atribuições de responsabilidade, os cronogramas, as análises de riscos e as ações de contingência que forneçam o resultado programado. Esse arranjo fomenta a compartimentalização da visão da cibersegurança adotada pela política vigente, que destaca, por exemplo, a dimensão das infraestruturas críticas, que conta com Plano próprio, definido no Decreto 9.573/2018, recentemente atualizado pelo Decreto 11.200/2022 (BRASIL, 2022), cujos princípios e objetivos não abrangem soberania digital, direitos fundamentais e proteção das pessoas (e dos dados que lhe dizem respeito) diante da afetação das principais infraestruturas críticas. Essa visão hiper-setorial contribui para a fragmentação da regulamentação, desconsidera o caráter dinâmico das ameaças e a multiplicidade de combinações de técnicas de ataques, abordados na seção 1.2, e perpetua uma vulnerabilidade sistêmica devida à falta de interconexão e coordenação entre as dimensões que compõem a cibersegurança.

Apesar de não detalhar os controles relacionados à segurança da informação, a norma traça um guia para os órgãos públicos federais estabelecerem os princípios da segurança da informação, definirem as obrigações a serem implementadas e criarem uma estrutura de governança da informação³⁷.

Especial destaque à criação, no âmbito federal, do Comitê Gestor da Segurança da Informação³⁸, que tem a função de assessorar o Gabinete Institucional da Presidência da República, órgão responsável pela coordenação da PNSI, nas atividades relacionadas à segurança da informação. Sua composição, claramente inspirada pelo *xitong* de cibersegurança chinês³⁹, envolve a participação de

37 Este assunto será tratado nos pormenores em um trabalho dedicado de iminente publicação.

38 Ver o Capítulo V do Decreto Nº 9.637, de 26 de dezembro de 2018.

39 O "xitong" é uma estrutura administrativa tipicamente chinesa, destinada a estabelecer um mecanismo dedicado à coordenação de todas as administrações públicas afetadas por uma área política específica, como ministérios, autoridades reguladoras, instituições financeiras públicas etc. Seu objetivo é lidar com a complexidade de uma administração multifacetada em um Estado gigantesco, podendo assim coordenar e regular setores específicos de forma eficiente. A China estabeleceu um xitong de cibersegurança em 2014,

todos os Ministérios que compõem o Governo, além do próprio Gabinete, da Casa Civil, da Controladoria Geral da União, da Secretaria do Governo da Presidência da República, da Advocacia Geral da União, do Banco Central e da Autoridade Nacional de Proteção de Dados (artigo 10). Ante o exposto, resgatando-se o debate acerca da necessidade e relevância da integração e cooperação de entes diversos (precisamente, entre o poder público, o setor empresarial, a sociedade e as instituições acadêmicas), visão inclusive alavancada como um dos princípios da PNSI (artigo 3º, inciso XV), defronta-se com a criação de um Comitê cuja composição é monosssetorial, apenas com a representatividade do Poder Público.

Após essa iniciativa, o Poder Executivo elaborou o Decreto nº 10.748/2021, que regulamenta o disposto no artigo 15, inciso VIII, da PNSI, e o Decreto nº 10.222/2020, conhecido como “E-Ciber”, que dá densidade à política de segurança da informação correspondente ao módulo “segurança cibernética”, estabelecido na PNSI, e detalha quais ações estratégicas devem ser implementadas pelos órgãos da Administração Federal, de acordo com suas competências.

Atendendo às disposições estabelecidas pelo PNSI e pela “E-Ciber”, diferentes Agências Reguladoras formalizaram seus programas de segurança da informação. Apesar de fornecerem aprendizados que podem ser aproveitados para a proposição de um novo Marco regulatório, a ausência de diálogo entre as medidas favorece uma visão compartimentada pelos diferentes setores.

Tal diálogo parece necessário considerando a atual heterogeneidade das abordagens setoriais adotadas pelas diferentes agências brasileiras, entre as quais se destacam: (i) a ANATEL (Agência Nacional de Telecomunicações), através da Resolução nº 740/2020, que aprova o Regulamento de Segurança Cibernética aplicada ao setor de telecomunicações, e do Ato nº 77/2021, que estabelece

junto com a Administração Chinesa do Ciberespaço (a famosa Cyberspace Administration of China, também conhecida como CAC) e uma Central Commission for Cybersecurity and Informatization (CCCI). No sistema chinês, o xitong é diretamente conectado à presidência da República e o Presidente encabeça também a CCCI. Ver BELLI (2022a, p. 18-19). Cabe também destacar que, desde 2014, os países do bloco BRICS compartilham periodicamente informações e boas práticas sobre suas abordagens de cibersegurança, no âmbito do BRICS Working Group on Security in the use of ICTs. Ver BELLI (2021a, 2021b).

requisitos de segurança cibernética para equipamentos para telecomunicações; (ii) a ANEEL (Agência Nacional de Energia Elétrica), via Resolução Normativa nº 964, que dispõe sobre a política de segurança cibernética a ser adotada pelos agentes do setor de energia elétrica; (iii) a ANAC (Agência Nacional de Aviação Civil), por meio da Instrução Normativa nº 128 de 2018, com redação atualizada pela Instrução Normativa nº 173 de 2021 e do Manual de Segurança Cibernética na Aviação Civil, editado em setembro de 2021; e (iv) a ANTT (Agência Nacional de Transportes Terrestres), através da Resolução 5854/2019, que regulou a Política de Segurança da Informação e Comunicações (PoSIC) da Agência.

Apesar de não se tratar de agência reguladora, o Banco Central (BACEN), autarquia federal, atualizou a Resolução nº 4658/18 via Resolução nº 4893/21, agora em vigor, para dispor sobre a política de segurança cibernética e sobre os requisitos para a contratação de serviços e processamento e armazenamento de dados e de computação em nuvem a serem observados pelas Instituições autorizadas a funcionar pelo BACEN. No que se refere aos meios de pagamentos, foi editada a Resolução nº 85/202, com o mesmo objeto e finalidade.

Outras duas autarquias, ligadas ao Ministério da Economia, também regulamentaram a segurança cibernética em seus setores, a Superintendência de Seguros Privados (SUSEP), via Circular nº 638 de 2021, e a Comissão de Valores Mobiliários (CVM), através da Instrução Normativa 35/2021 (capítulo XII, que trata sobre a segurança da informação), alterada pela Resolução nº 134, de 2022.

Cabe frisar que a elaboração de regulamentações setoriais pelos órgãos supracitados representa um avanço muito positivo, testemunhando da relevância crescente da preocupação com cibersegurança pelas administrações públicas brasileiras e dos progressos realizados nos últimos anos. Porém, o sistema de governança existente parece extremamente minimalista, para usar um eufemismo, é inapto a garantir uma coordenação eficiente entre administrações, setor privado e terceiro setor.

Considerado quanto exposto nas precedentes seções, particularmente no que diz respeito à necessária natureza multissetorial, multidimensional e internacional da cibersegurança, não nos parece possível que o Comitê Gestor da Segurança da Informação, na sua atual configuração de única instância de coordenação, permita a promoção de ações regulatórias conjuntas e a elaboração e implementação de políticas coordenadas e, sobretudo, capazes de estabelecer uma interação multissetorial permanente coletando *inputs* dos vários setores afetados e envolvendo-os ativamente na educação e *compliance*.

Para além deste sistema de governança monosssetorial e desta regulação compartimentada e setORIZADA (e não sistêmica), cabe lembrar a existência de outras leis tangentes que devem ser respeitadas e promovidas pelo Executivo Federal. São elas: a Lei Geral de Proteção de Dados (Lei nº. 13.709/2018), que prescreve regras sobre a segurança de dados nos artigos 6º, 44, 46, 47, 48 e 49, o Marco Civil da Internet (Lei nº. 12.695/2014), que regula a segurança da internet nos artigos 3º, V, 9º, § 2º, III, 10, § 4º, 13 e 15, e a Convenção de Budapeste, ratificada pelo Brasil em 2001 e transformada no Projeto de Decreto Legislativo Projeto de Decreto Legislativo nº 255/2021, incorporada ao ordenamento jurídico pátrio em abril de 2023 por meio do Decreto n. 11.491, cujo objetivo é facilitar a cooperação internacional para o combate ao crime cibernético. Não há, nas duas principais bases do arranjo normativo de cibersegurança vigente, o necessário diálogo com estas legislações (considerando a contemporaneidade das produções normativas).

3.1 Críticas gerais acerca das principais bases normativas federais

A normativa federal (PNSI) denuncia avanços significativos face à preocupação contundente relativa à cibersegurança e à soberania digital. É fundamental um texto normativo que uniformize e direcione a estruturação de um programa matricial de segurança da informação nas suas mais plurais dimensões. No entanto, em que pesem os progressos observados, o que se verifica são

regulamentações ainda restritas a uma visão tradicional e, conforme já asseverado, insuficiente. Elucidam-se na sequência os principais aspectos que merecem críticas.

Antes de tecer críticas substanciais à política implementada pela PSNI, é interessante apontar para a imprecisão terminológica utilizada ao se referir à “segurança da informação” como termo amplo abrangente e equivalente à ideia de “cibersegurança”. Os termos não são sinônimos, o que pode levar a uma abordagem confusa que pode causar um tratamento inadequado do tema, limitando-o a questões relacionadas à segurança da informação, deixando de fora outras dimensões, mencionadas na primeira sessão, além de colocar a informação como centro de proteção, quando o valor central da regulação deve ser a proteção dos indivíduos e do Estado, nas suas componentes democrática, econômica e social.

A reflexão que se faz organiza-se a partir de três eixos centrais, quais sejam, (i) regulatório, ante a inobservância de uma atuação multissetorial; (ii) material, haja vista a incompletude das dimensões atreladas à segurança da informação alcançadas pela norma, bem como omissão correlata ao protagonismo dos indivíduos nesse contexto; e (iii) integrativo, de modo a formar um corpo normativo coeso e integrado, seja quanto ao aspecto terminológico, seja quanto aos agentes atuantes.

Conforme explorado em oportunidade pretérita, embora a PNSI tenha firmado como pilar principiológico a integração e a cooperação multissetorial (artigo 3º, inciso XV), a conformação do Comitê Gestor da Segurança da Informação denota postura díspar. Reitera-se: envolveram-se exclusivamente entidades públicas, desconsiderando outros setores importantes para produção normativa regulatória, tais como a sociedade civil, empresas privadas, instituições acadêmicas e comunidade técnica.

Podemos destacar que uma abordagem compartimentada e monosssetorial produz estratégias, regulações, instituições e ações que, necessariamente, não se beneficiam de experiências e contribuições dos demais setores envolvidos e, portanto, têm uma qualidade – seja na elaboração ou na implementação

– necessariamente mais limitada e fragmentada. Tal falta de coordenação, consulta e cooperação⁴⁰ multissetorial reduz a eficiência e efetividade das estratégias regulatórias e configura uma vulnerabilidade sistêmica adicional e frequentemente explorada. O valor por trás da proposta de se construir uma compreensão sistêmica da cibersegurança está em prover uma abordagem para o estudo da cibersegurança que dê conta dessa complexidade.

Nessa trilha, por mais que possamos (e devamos) questionar o caráter efetivamente democrático do processo de participação de diferentes setores da sociedade na elaboração da E-ciber, frisa-se que seu texto foi submetido à consulta pública antes da sua aprovação e publicação. A E-Ciber menciona a necessidade de aprimoramento do arcabouço legal sobre segurança cibernética enquanto um dos eixos de atuação e, portanto, tal orientação poderia inspirar a realização de medidas de participação de diferentes atores (e.g., “universidades, institutos, centros de pesquisa e setor privado”, E-Ciber, item 2.3.10, bem como da sociedade civil, movimentos sociais, entidades de classe, entidades estudantis, trabalhadores das bases) para explorar o conteúdo de um marco normativo para segurança das pessoas na realização de atividades em que o poder público se vale de meios digitais (inclusive, atividades de disponibilização de dados) e que considere as especificidades locais, sem olvidar dos riscos de eventual fragmentação da regulamentação do tema.

Sobre o último eixo passível de crítica, destaca-se que as normas federais analisadas carecem de coesão textual, conceitual e estrutural quando introduzidas no contexto de outras diretrizes e leis do nosso ordenamento jurídico que abordem temas correlatos. Ilustrativamente, cita-se a ausência de correlação normativa com a Lei nº. 13.709/2018, Lei Geral de Proteção de Dados, que, além de

40 Essa combinação configura a dita governança multissetorial “em 4C” cujo objetivo é elaborar e implementar estratégias regulatórias efetivas. Dessa forma, a concertação inicial permite analisar um determinado problema e identificar as melhores práticas; a cooperação ajuda a desenvolver uma estrutura modelo por meio de uma abordagem participativa; a consulta permite aperfeiçoar tal modelo em virtude de uma pluralidade e diversidade de contribuições examinando as diferentes dimensões afetadas do instrumento normativo proposto; por fim, a coordenação entre as partes envolvidas permite assegurar uma aplicação correta e eficaz da ferramenta regulatória. Ver BELLI (2016, p. 82).

regulamentar o tratamento de dados pessoais, nos meios físicos e digitais, pelas pessoas físicas e jurídicas privada e pública (art. 1º) – dimensão da segurança da informação –, introduz a figura do encarregado pelo tratamento de dados (art. 5º, inciso VIII), não incluído nos textos legais analisados, e cria a Autoridade Nacional de Proteção de Dados (ANPD), conforme disposto no artigo 55-A.

Por fim, insta salientar que o Decreto que regulamenta a Estratégia Nacional de Cibersegurança no Brasil tem vigência prevista para o quadriênio 2020-2023, pelo que, com o seu fim, ao final deste ano, a sociedade brasileira terá a oportunidade de debater essa abordagem, trazendo uma nova roupagem para a regulação de cibersegurança.

Expostas as críticas aos textos normativos analisados, cabe considerar uma de suas omissões. Nesse sentido, na contramão de um perfil repressivo, uma política de incentivos fiscais em prol da implementação de medidas mínimas de segurança da informação – com especial enfoque na cibersegurança – nas organizações merece ser avaliada pelo governo⁴¹. Para a compreensão das vantagens e desvantagens associadas à ação, seriam necessários estudos para a definição de critérios objetivos para classificação da elegibilidade das empresas a serem contempladas pelo benefício fiscal, de quais seriam os requisitos mínimos de segurança a serem perseguidos (de forma que sejam efetivos e atualizados) e as estratégias para a condução das auditorias, inclusive periódicas, nesses ambientes. Nada obstante, em que pesem os benefícios reflexos na cultura das organizações, na medida em que seriam estimuladas a capacitar colaboradores, investir e implementar controles de segurança, impõe-se uma avaliação criteriosa sobre o impacto da medida aos cofres públicos (a renúncia às receitas pode afetar o orçamento público e eventualmente comprometer áreas prioritárias).

41 A título ilustrativo, sem tecer críticas, cita-se o Projeto de Lei nº 4, de 2022, de iniciativa do Senador Izalci Lucas (PSDB/DF), que pretende permitir o desconto de créditos relativos a valores investidos em programas de adequação à Lei nº 13.709/2018 (“LGPD”) da base de cálculo da Contribuição para os Programas de Integração Social (PIS) e de Formação do Patrimônio do Servidor Público (PASEP), da Contribuição para o Financiamento da Seguridade Social (COFINS), da Contribuição para os Programas de Integração Social e de Formação do Patrimônio do Servidor Público incidente na Importação de Produtos Estrangeiros ou Serviços (PIS/PASEP-Importação) e a Contribuição Social para o Financiamento da Seguridade Social devida pelo Importador de Bens Estrangeiros ou Serviços do Exterior (COFINS-Importação). (BRASIL; SENADO FEDERAL, 2022).

3.2 Medidas de cooperação internacional e de homogeneização de práticas

Evidenciados os riscos aos quais se está exposto em uma sociedade em rede, em ambiente de relações e transações transfronteiriças, muitas das quais digitalizadas sem preocupação séria por questões de cibersegurança, é recomendável que os atores públicos e privados cooperem na identificação e implementação das soluções regulatórias mais eficientes, eficazes e efetivas.

Neste sentido, uma governança multisetorial almeja oferecer as bases para que as partes interessadas busquem (i) integrar boas práticas, estruturas e padrões delineados por entidades especializadas; (ii) capacitar e certificar seus colaboradores, determinadas áreas internas, projetos ou as próprias empresas e entidades de forma geral; (iii) seguir códigos de conduta – que poderão ser elaborados tanto internamente, pelas próprias organizações, mas que idealmente, deveriam ser definidos no âmbito de uma abordagem corregulatória, associando entidades de classe, legislativo e outros setores interessados; (iv) avaliar a contratação de seguros voltados à gestão de riscos cibernéticos; (v) adotar regulamentos e cláusulas-tipo (padronizadas) para harmonizar a regulação da cibersegurança; e (vi) estabelecer regras corporativas vinculativas.

Nesta seção, trabalharemos as principais medidas de cooperação e adoção de boas práticas, necessárias para dar conta do caráter internacional da cibersegurança.

3.2.1 Normas e padrões internacionalmente reconhecidos como referências

Em face das possibilidades plurais concernentes às duas primeiras alternativas sugeridas como boas práticas, dedicar-se-á, na sequência, a uma breve explanação e cotejo entre os seus principais referenciais. Destarte, elencam-se a seguir os padrões e estruturas de maior relevo em razão de respectivas popularidade e enfoque:

Tabela 3 – Padrões de cibersegurança

Padrão	Considerações gerais
<p>ISO/IEC 27.001 (International Organization for Standardization)</p>	<p>Com sua primeira versão publicada em 2005, a ISO/IEC 27001 representa uma Norma de Gestão de Segurança da Informação (SGSI) baseada em risco. Trata-se de documento que alcança todos os tipos de organizações⁴² e que prescreve uma série de controles passíveis de serem aplicados tanto nas empresas, de modo integral, quanto em segmentos específicos dessas, conforme a respectiva delimitação do escopo. Sobreleva o papel de liderança e a demanda de comprometimento da Alta Direção (ISO, 2013). Esse material poderá ser utilizado e aplicado com o fim de (i) formular requisitos e objetivos de segurança da informação; (ii) garantir a conformidade com leis e regulamentos; (iii) garantir uma gestão de risco econômica; (iv) guiar uma estruturação de processo de implementação e gerenciamento de controles que garanta o atendimento de objetivos de segurança específicos; (v) fornecer informações relevantes sobre políticas, diretivas, padrões e procedimentos de segurança da informação para parceiros comerciais e outras organizações com as quais se mantém qualquer interação operacional ou comercial; e (vi) representar instrumento de avaliação do grau de aderência e <i>status</i> das atividades de gerenciamento de segurança da informação na organização (ISO, 2005).</p>
<p>NIST Cybersecurity Framework (CSF) (National Institute of Standards and Technology)</p>	<p>Este Guia dedica-se ao aperfeiçoamento da gestão de riscos de segurança cibernética em infraestruturas críticas⁴³, embora possa ser utilizado por organizações de outros setores ou pela sociedade. Assim como a ISO 27.001, também permite aplicação por escopos delimitados (como, por exemplo, apenas para a entrega de serviços críticos). Foca nos efeitos da segurança nas dimensões físicas, cibernéticas e de pessoas.</p> <p>O material subdivide-se em três partes: (i) “Estrutura Básica”, que consiste em funções simultâneas e contínuas de identificar, proteger, detectar, responder e recuperar; (ii) “Níveis de Implementação de Estrutura”, que variam entre parcial (Nível 1), risco informado (Nível 2), reproduzível (Nível 3) e adaptável (Nível 4); e (iii) “Avaliação de Estrutura”, que pode ser utilizada para descrever o estado atual ou desejável de atividades específicas. Esse referencial NIST poderá ser utilizado para (i) a realização de uma avaliação básica das práticas de segurança cibernética; (ii) a elaboração ou melhoria de um programa de segurança cibernética; (iii) informar os <i>stakeholders</i> sobre os requisitos de segurança cibernética; (iv) decisões de compras; (v) identificação de oportunidades para referências informativas, sejam elas novas ou revisadas; (vi) autoavaliação de riscos; e (vii) como metodologia para proteção da privacidade e das liberdades civis.</p>

42 Exemplificativamente, citam-se as organizações comerciais, as sem fins lucrativos e as governamentais.

43 Conforme definição do *US Patriot Act*, de 2001, infraestruturas críticas são “sistemas e ativos, sejam eles físicos ou virtuais, tão vitais para os Estados Unidos que a incapacidade ou destruição de tais sistemas e ativos teria um impacto debilitante sobre a segurança econômica nacional, saúde e segurança pública nacional, ou na combinação de qualquer uma dessas áreas” (42 U.S.C § 5195c(e)).

Padrão	Considerações gerais
<p>NIS 2.0, Diretiva (UE) 2022/2555 do Parlamento Europeu e do Conselho</p>	<p>A Diretiva vislumbra a identificação de medidas capazes de promover um elevado nível comum de segurança cibernética na União Europeia. Embora vigente, os Estados-membros da UE terão até 17 de outubro de 2024 para implementar suas disposições, por meio de transposição dos dispostos normativos em leis nacionais.</p> <p>O texto normativo revogou a Diretiva (UE) 2016/1148 (conhecida na denominação e acrônimo inglês “Directive on Security of Network and Information Systems across the EU” ou “NIS Directive”), que promoveu progressos significativos no âmbito da ciber resiliência e cooperação a nível da União, conquanto, permitiu aplicações muito diversas a nível nacional relativas às obrigações de cibersegurança e de notificação de incidentes. Face à fragmentação do mercado interno, e no intuito de superar a vulnerabilidade da prestação de serviços transfronteiriços e o nível de ciber ⁴⁴, ao: (i) criar mecanismos de cooperação entre as autoridades desses Estados; (ii) atualizar (e alargar) lista de setores e atividades sujeitas aos deveres relativos à cibersegurança; e (iii) uniformizar diretrizes de supervisão e execução para os Estados-membros.</p> <p>Vislumbrando a proteção de sistemas de redes e informação, nos meios digitais e físicos, estabelecem-se como medidas de gestão dos riscos de cibersegurança mínimas (art. 21.2): (i) políticas e procedimentos de segurança dos sistemas da informação, de análise de risco, para avaliação da eficácia das medidas de gestão de riscos, e relativos à criptografia e cifragem (caso se aplique); (ii) tratamento de incidentes; (iii) continuidade das atividades por meio da gestão de <i>backups</i>, recuperação de desastres e gestão de crises; (iv) segurança da cadeia de suprimentos; (v) segurança na aquisição, desenvolvimento e manutenção dos sistemas de rede e de informação, com o tratamento e a divulgação de vulnerabilidades; (vi) práticas básicas de ciber-higiene e formação em cibersegurança; (vii) segurança dos recursos humanos, com políticas de controle de acessos e gestão de ativos; e (viii) implementação de soluções de autenticação multifator ou contínua, comunicações seguras (voz, vídeo e texto), bem como sistemas seguros de comunicações de emergências na entidade, caso aplicável.</p>

Conforme exposto, os três modelos⁴⁵ representam padrões e estruturas amplamente utilizados como referências ao nível nacional e internacional, por organizações públicas e privadas. Não obstante estes modelos sejam desenvolvidos por entidades diferentes (uma organização internacional de natureza técnica, uma agência nacional, e uma organização intergovernamental supranacional)

44 Considerando 5 da Diretiva (UE) 2022/2555 do Parlamento Europeu e do Conselho.

45 A título informativo, faz-se menção à proposta de regulamento europeu intitulado “Cyber Resilience Act”, sobre os requisitos horizontais de cibersegurança para produtos digitais e serviços auxiliares (COMISSÃO EUROPEIA, [s.d.]).

e tenham abrangências diversas, apresentam várias semelhanças que nos permitem identificar quais sejam os principais pontos que merecem atenção dos reguladores e dos regulados. Os principais pontos de convergência e até justaposição são: (i) uma abordagem baseada em risco; (ii) a preocupação com a estruturação de sistemas de gestão da segurança da informação alinhados aos objetivos, visão e missão do negócio; (iii) o objetivo de promover a cibersegurança *lato sensu*, aumentando a confiança na economia digital, reforçando a resiliência de infraestruturas e mantendo a segurança individual no ambiente digital; (iv) a inclusão de lista de controles de segurança a serem estruturados e implementados em camadas; e (v) a ênfase na melhoria contínua por meio de monitoramento, avaliação de desempenho dos controles implementados e atualização de políticas e procedimentos relacionados à segurança cibernética.

Compreendido o cenário de estruturação de um Sistema de Gestão da Segurança da Informação (SGSI), aborda-se a seguir a segunda boa prática sugerida na introdução desta seção: o envolvimento de colaboradores capacitados e certificados nas atividades tanto de gestão da segurança da informação, quanto de risco. Nesta perspectiva cabe reiterar que a capacitação e a educação multigeracionais devem representar uma preocupação constante e prioritária de qualquer sistema voltado a encarar os desafios da cibersegurança de maneira séria e sólida.

Assim, as experiências dos modelos de certificação existentes são particularmente interessantes porque, além de preparar os profissionais para a gerência e a implementação de controles de segurança em organizações, impulsionam a imagem das empresas e a confiança de partes interessadas. O benefício da capacitação certificada é, portanto, duplo: não somente o aprimoramento das competências individuais, mas também da confiança das pessoas – físicas e jurídicas – cujas competências são certificadas. Os treinamentos e cursos de capacitação existentes deveriam, portanto, ser considerados como modelos de treinamentos que podem ser adaptados à população geral, com o intuito de incrementar as capacidades e o engajamento individual no fortalecimento da cibersegurança.

Iniciativas que corroboram essas premissas são o Regulamento (UE) 2019/881 do Parlamento Europeu e do Conselho, de 17 de abril de 2019, relativo à ENISA (Agência da União Europeia para a Cibersegurança) e à certificação da cibersegurança das tecnologias da informação e comunicação, e a recente criação de uma Rede Centro Europeu de Competência em Cibersegurança, juntamente com a Rede de Centros Nacionais de Coordenação, cujo objetivo é trabalhar em conjunto para reforçar a soberania tecnológica europeia através do investimento conjunto em projetos estratégicos de cibersegurança⁴⁶. Pelo texto, no intuito de se assegurar o bom funcionamento do mercado intrabloco e alcançar um nível alto de cibersegurança, de ciber-resiliência e de confiança, pondera-se acerca da relevância de sistemas de certificação europeus atentarem à garantia de que produtos, serviços e processos por eles aprovados sejam satisfatórios na proteção da disponibilidade, autenticidade, integridade e confidencialidade dos dados tratados, em todas as fases de respectivo ciclo de vida⁴⁷. Tal visão é complementada pelo reconhecimento explícito da importância de investimentos consideráveis em pesquisa e desenvolvimento que reflitam os valores de cibersegurança a serem embutidos nas novas tecnologias.

Embora a normativa ainda não seja uma disposição reproduzida de forma uníssona em outros territórios, algumas certificações despontam. Atualmente, as certificações mais reconhecidas nacional e internacionalmente – excepcionando-se aquelas de nicho, como, por exemplo, relativas à privacidade e à proteção de dados, que não foram contempladas no estudo haja vista o recorte temático do presente ensaio –, são:

46 Em 8 de junho de 2021, foi publicado o Regulamento (UE) 2021/887 do Parlamento Europeu e do Conselho, de 20 de maio de 2021, que cria o Centro Europeu de Competências Industriais, Tecnológicas e de Investigação em Cibersegurança e a Rede de Centros Nacionais de Coordenação. O Centro Europeu de Competência em Cibersegurança (ECCC), juntamente com a Rede de Centros Nacionais de Coordenação (NCCs), é a nova estrutura da Europa para apoiar a inovação e a política industrial em segurança cibernética. O ECCC desenvolverá e implementará, com os Estados-Membros, a indústria e a comunidade tecnológica de cibersegurança, uma agenda comum para o desenvolvimento tecnológico e para a sua ampla implantação em áreas de interesse público e nas empresas, em particular nas PME.

47 Arts. 1º, caput; 46, 2; e Considerando 75, do Regulamento (UE) 2019/881 do Parlamento Europeu e do Conselho, de 17 de abril de 2019.

Tabela 4 – Certificações, por entidade certificadora e indicação

CERTIFICAÇÃO	ENTIDADE CERTIFICADORA	INDICAÇÃO
<u>CISSP</u> (Certified Information Systems Security Professional)	(ISC) ²	Profissionais com atuação em posições de gerência/liderança na área da segurança da informação (exige alguns requisitos, como experiência).
<u>CISM</u> (Certified Information Security Manager)	ISACA ⁴⁸	Profissionais com atuação em posições de gerência/liderança na área da segurança da informação.
<u>CRISC</u> (Certified in Risk and Information Systems Control)	ISACA	Profissionais com atuação em posições de gerência/liderança na área da segurança da informação.
<u>COBIT 5 e COBIT 2019</u> (Control Objectives for Information and Related Technology)	ISACA; PEOPLECERT; APMG	Profissionais com atuação em posições de gerência/liderança na área da tecnologia da informação e outros (foco em governança de TI).

As certificações supracitadas contemplam estruturas similares, passíveis de implementação em camadas. Entretanto, especial menção se faz em relação à CISSP, que exige alguns requisitos de formação e experiência prática prévia.

Ante o exposto, no esforço de apresentar os principais controles de segurança atrelados a todos os modelos indicados, citam-se como primordiais: (i) organização estrutural e documental da segurança da informação; (ii) inventário e gestão de ativos, com implementação de controles de segurança físicos e lógicos; (iii) controle de acessos físicos e digitais à informação – incluindo-se, por óbvio, gestão de identidade e classificação da informação; (iv) criptografia e realização de cópias de segurança (*backup*); (v) enfoque na segurança dos processos de recursos humanos e da cadeia de suprimentos, bem como daqueles relentes aos sistemas e redes (aquisição, desenvolvimento e manutenção); (vi) segurança na comunicação (redes e transferências de informações); (vii) gestão de incidentes de segurança da informação, com realização de testes, monitoramento e relatórios com as lições aprendidas; e (viii) conscientização de colaboradores e terceiros por meio de treinamentos, simulações e testes e investimentos

48 Information Systems Audit and Control Association.

na certificação de profissionais ou na contratação desses. Não se deve olvidar que nem todas as organizações demandam a implementação completa desses controles. A criticidade e sensibilidade das atividades desenvolvidas e das informações tratadas serão elementos norteadores na estruturação dos sistemas de gestão de segurança cibernética.

3.2.2 Seguro cibernético

Dentro de uma perspectiva multissetorial, uma ferramenta passível de ser utilizada com o potencial de conformar condutas e direcionar, portanto, comportamentos mais seguros em um ambiente cujos riscos estão incorporados no cotidiano é o seguro cibernético.

Esse tipo de seguro projeta-se à cobertura de perdas e responsabilidade de terceiros decorrentes de incidentes de segurança no ambiente digital, como violações à privacidade, proteção de dados e outros ataques. Dentre os custos compensatórios inclusos, citam-se aqueles para notificação e monitoramento de vítimas, investigações forenses e campanhas de relações públicas enveredadas à restauração da confiança na organização. Embora esse ensaio não tenha a pretensão de realizar uma análise profunda desta ferramenta, convém desenvolver sumariamente algumas considerações relevantes acerca dessa opção e de seus impactos no contexto estudado.

Pela visão tradicional – e dominante –, a concepção de seguro é baseada na ideia de um contrato cujo objeto é o risco. Esse acordo refletirá duas dimensões: por um lado, (i) a “transferência de risco”: uma relação *inter partes* na qual o segurado (contratante) paga um prêmio e, em contrapartida, recebe uma garantia contra riscos; e, por outro, (ii) a “distribuição de riscos”, na qual a seguradora celebra vários contratos similares com a garantia de riscos relativamente homogêneos, promovendo a diluição de perdas entre os vários atores (TALESH; FILHO, 2023, p. 79). Como salvaguarda na gestão de riscos, caberia à seguradora, *prima facie*, auditar a organização (segurada) de forma global e mais exaustiva *ex ante* (idem, 2023, p. 77), prevenindo-se, desta maneira, não somente os riscos alcançados pelas tratativas, mas igualmente a inadimplência.

Haja vista a capacidade (ou a tentativa) de alterar comportamentos em busca da mitigação de riscos – sejam eles derivados da falibilidade institucional, humana ou tecnológica –, entende-se que as seguradoras atuam como reguladoras – inclusive com vantagens comparadas ao governo, na medida em que, no âmbito privado, acessam com exclusividade dados privilegiados das organizações auditadas (idem, 2023, p. 82)⁴⁹. Potencialmente, a partir da capacidade de antever sinistros e de mensurar os níveis de maturidade da organização face aos controles de privacidade, proteção de dados e segurança da informação, há a possibilidade de ofertar valores de contraprestação adequados e proporcionais que, muito além de ampliar as perspectivas negociais pela cadência de custos – quanto menor for o risco da atividade desenvolvida e mais controles forem implementados, menor a quantia do prêmio a ser pago –, os segurados são incentivados a aprimorar o cenário mapeado na sua organização, clara manifestação da influência no seu comportamento de risco (BARRY; DOYLE; ERICSON, 2003).

A redução eficiente de risco impacta positivamente na possibilidade de minoração de valores dos prêmios, na maior participação competitiva das seguradoras no mercado, no controle das perdas e em um ambiente físico e cibernético mais seguro e sustentável. Contudo, tal conclusão perfaz-se apenas idealmente. A despeito da abordagem anterior, nem sempre as seguradoras estão alinhadas aos valores e interesses da sociedade. A maximização dos lucros e a redução dos custos é crucial para tais atores, cuja lógica pode não estar alinhada com o interesse público. Ademais, na promoção dos valores – inclusive normativos – que lhes sejam próprios, por vezes alguns aspectos da interpretação legal são negligenciados, enfraquecendo tais determinações ao apresentar novos contornos – afastando-se assim do êxito no exercício do papel regulatório complementar e do interesse público (cf. três casos empíricos explorados, ver TALESH; GONÇALVES FILHO, 2023). Outro aspecto merecedor de atenção

49 Considerando a complexidade atual das relações sociais e assimetria regulatória entre o setor regulado, de um lado, e usuários e regulador, do outro, notadamente, temas que envolvem tecnologia digital, que as seguradoras podem se tornar grandes aliadas na regulação de cibersegurança, já que elas possuem melhores condições de conseguir maiores informações sobre a atividade regulada, diminuindo o problema da assimetria informacional, e, por consequência, são mais capazes de realizar o gerenciamento do risco e moldar o comportamento dos usuários, se comparadas as possibilidades do Estado.

são os conjuntos de dados que embasam as avaliações de riscos das seguradoras, fontes que podem ser altamente incompletas e imprecisas, haja vista a ausência de metodologia predefinida e homogêneas. A respectiva definição de critérios e métricas pulverizada nas seguradoras evidencia a premente necessidade de elaboração de padrões metodológicos aplicáveis aos atores de mercado à autoridade reguladora.

Outro aspecto nesse contexto é a “tecnologização dos seguros”. Nessa trilha, a utilização de tecnologias e *big data* pelas seguradoras, na visão de Talesh e Cunningham (2021), poderiam torná-las mais eficazes enquanto reguladoras, seja na prevenção, na detecção ou na resposta aos riscos de segurança cibernética, *inter alia* aplicando algumas das técnicas de IA destacadas na secção 0 deste trabalho. Entretanto, consoante pesquisa empírica encabeçada pelos autores, os resultados práticos não refletem esse cenário. Verificou-se primordialmente uma alta competitividade para o ingresso e a manutenção no mercado – no qual os recursos tecnológicos são orquestrados com o condão de aumentar lucros, e não para realização de auditorias – e uma “relutância” em premiar os “bons cidadãos cibernéticos”, não oferecendo incentivos a esses segurados, por exemplo, com a minoração dos valores dos prêmios, ou com a exclusão da cobertura de seguro daqueles que não estão dispostos a implementar medidas de segurança cibernética. Outrossim, constatou-se uma baixa aderência na aquisição de ferramentas e serviços adicionais de gerenciamento de risco cibernético e controle de danos, seja em razão do alto custo, seja pelo descrédito de sua ocorrência (TALESH; CUNNINGHAM, 2021, p. 1010-1015).

Preocupação de igual relevância é a utilização de bases de dados de qualidade questionável associada às técnicas de *Big Data* e IA, face aos resultados escaláveis, de fato prejudicando os benefícios em termos de eficiência promovidos pela tecnologia. Neste sentido, é desejável não somente que os elementos aptos a permitir a avaliação do risco sejam integrados em arcabouço normativo sobre cibersegurança, mas, também, que seja adotada regulamentação específica voltada a padronização de conteúdo e de formato das informações necessárias para que uma autoridade reguladora

(ou uma seguradora) possa efetivamente avaliar a conformidade de cada entidade com as melhores práticas (e ferramentas) de cibersegurança e, portanto, sua exposição ao risco.⁵⁰

Por fim, para o funcionamento desse arcabouço regulatório é imprescindível a coordenação com a criação de uma Agência Reguladora Nacional de Cibersegurança, promovendo a contribuição de diversos atores, públicos e privados, que operam nesse ecossistema. Caberá a entidade pública supervisionar a intervenção das empresas privadas no setor impedindo que os interesses públicos sejam sobrepostos pelos privados. É igualmente importante que o Estado determine a estrutura regulatória a ser seguida pelas entidades privadas, distanciando-se, portanto, de um modelo de comando e controle, aproximando-se dos modelos de metarregulação. Dessa forma, reduzindo as incertezas jurídicas correlatas, a Agência deverá: (i) identificar os perfis das organizações e conformar as boas práticas de cibersegurança a serem implementadas; (ii) estabelecer critérios de avaliação, prevenção e mitigação de riscos (de acordo com os perfis predeterminados); (iii) definir responsabilidades de cada ator envolvido – inclusive no que diz respeito à educação de treinamentos –; (iv) determinar as métricas para avaliar o cumprimento de responsabilidades específicas, dentre outras especificidades pertinentes; e (v) elaborar o modelo relativo a execução e a periodicidade das auditorias – documentais e *in loco* – dos atores do setor.

Em vista disso, a utilização dos seguros como instrumento para conformar as condutas dos segurados, buscando mais segurança no ciberespaço, está alinhada com o modelo de governança proposto neste estudo, embora deva ser considerada como um mero complemento, ao invés que um substituto de um sistema multissetorial encabeçado pelo Estado. Nessa trilha, cabe ao Estado delimitar os meios dessa atuação, considerando as externalidades do uso do seguro como instrumento regulatório no setor, principalmente, adotando especial cuidado para que não se desconsidere interesses e objetivos públicos, o que poderia fragilizar a soberania

50 A padronização e tais elementos normativos bem como dos requisitos formais e substanciais para demonstrar compliance poder facilitar enormemente elaboração de avaliações da maturidade do nível de cibersegurança – os chamados *cyber scores* – de entidades específicas. Veja por exemplo o *Cyber Score* <https://www.cyberscores.io/pt/>

digital do Estado. Assim, superando os obstáculos postos em cena, os seguros (são) tornar-se-ão um excelente instrumento complementar – e não alternativo – em um programa de mitigação de riscos cibernéticos.

3.3 Convenção de Budapeste

A busca por um cenário de segurança cibernética homogênea nas organizações e que garanta a implementação de (boas) práticas mínimas é uma necessidade cogente face ao mercado global. Ampliando-se o escopo e a abrangência de respectiva assertiva, reflete-se acerca dessa possível uniformização também em matéria penal há mais de duas décadas. Em vista disso, não se deve olvidar a Convenção do Conselho da Europa sobre o Crime Cibernético, conhecida como Convenção de Budapeste⁵¹, que é o primeiro tratado internacional dedicado ao combate ao cibercrime e foi oficialmente assinada pelo Brasil, que se tornou parte da Convenção no fim de 2021 (BRASIL; SENADO FEDERAL, 2021). A Convenção foi, então, incorporada ao ordenamento jurídico pátrio em abril de 2023 por meio do Decreto n. 11.491 de 2023 (BRASIL; PRESIDÊNCIA DA REPÚBLICA, 2023).

A Convenção abriu assinaturas em 2001 e entrou em vigor em 2004. Foi o primeiro tratado internacional a focar explicitamente no cibercrime. O texto vislumbra facilitar a cooperação internacional no âmbito criminal – portanto, entre Estados e organizações privadas – e uniformizar os procedimentos atrelados à persecução penal. Atualmente, o texto é ratificado por 68 países (“Budapest Convention – Cybercrime”, [s.d.]) e é utilizado como guia orientativo para as produções legislativas de outros 158 países (MINISTÉRIO DA JUSTIÇA E SEGURANÇA PÚBLICA, 2021).

De cariz técnico, a Convenção propõe, sob o aspecto material, a criminalização das seguintes condutas: acesso ilegítimo, interceptação ilegítima, interferência em dados e sistemas, uso abusivo de dispositivos, falsidade e burla informática, exploração sexual infantil por meios digitais (infelizmente definida como “pornografia infantil”), violação de direitos de autor e de direitos conexos. O

51 A versão em português da Convenção pode ser acessada no site do Conselho da Europa (2001).

tratado fornece também elementos úteis para caracterizar situações mais complexas de responsabilidade, quais sejam, tentativa de crime e cumplicidade, responsabilidade de pessoas jurídicas e sanções (art. 2º a 13).

Pela perspectiva processual, mencionam-se eventuais ações coercitivas e instrumentais para a persecução penal de crimes em ambiente transfronteiriço digital – como, por exemplo, busca e apreensão de dados informáticos armazenados (art. 19), coleta de dados de tráfego em tempo real (art.20) e interceptação de dados de conteúdo (art. 21) –, de competência jurisdicional (art.22) e, finalmente, estabelece mecanismos de cooperação entre Estados (art. 23 a 35).

A base principiológica para a cooperação internacional, de forma geral, sustenta-se na extradição, no auxílio mútuo – e amplo (art. 25, 1) –, na informação espontânea, na confidencialidade e restrição da utilização de informações em outras investigações ou procedimentos não comunicados, coroados com a disponibilização de um ponto de contato “24/7” (24 horas por 7 dias da semana) intitulado por profissional técnico e célere, promovendo-se, dessa maneira, a garantia de uma assistência imediata a investigações ou procedimentos.

Há críticas cabíveis ao texto da Convenção, em especial relentes à proteção de dados pessoais em matéria criminal e à justaposição de ordenamentos jurídicos plurais e dotados de diferentes níveis de maturidade face aos desafios impostos pelo ciberespaço. Além disso, cabe salientar que a Convenção de Budapeste tem sido alvo de críticas constantes por causa da postura excessivamente rígida no que diz respeito às infrações aos direitos autorais e conectados. Tais infrações, consideradas tipicamente como um comportamento ilícito de área cível, são, porém, criminalizadas pela Convenção, que obriga as partes assinantes a integrar essa mesma abordagem.

Apesar da existência de evidentes críticas, a participação do sistema estabelecido pela Convenção nos parece útil, oferecendo, além de um marco modelo para a regulação de cibercrimes, um sistema capaz de estreitar relações internacionais de maneira particularmente eficiente e harmonizar conceitos, a criminalização de condutas e os instrumentos para o respectivo combate.

4 CONCLUSÃO: UMA PROPOSTA DE MARCO DE CIBERSEGURANÇA E SOBERANIA DIGITAL

Como destacamos ao longo deste trabalho, a cibersegurança é um assunto complexo, cuja governança e cuja regulação nos obrigam a pensar e atuar de maneira sistêmica, para elaborar e implementar soluções que sejam ao mesmo tempo democráticas, eficientes e efetivas. Tal abordagem sistêmica é indissociavelmente conectada à discussão sobre soberania digital, que se tornou essencial para garantir o desenvolvimento sustentável do País. Ambas as discussões são extremamente urgentes e a falta de propostas concretas sobre como estruturá-las é flagrante.

Neste sentido o objetivo deste trabalho é fornecer ao leitor as chaves essenciais para abordar o debate, entender as diferentes dimensões - não somente temáticas e jurídicas, mais também nacionais e culturais - que caracterizam as pautas analisadas, para conseguir formar uma opinião de maneira crítica e informada. Um debate público amplo, inclusivo, e multissetorial capaz de identificar o melhor caminho para o Brasil se tornar um País ciberseguro e digitalmente soberano, é extremamente urgente. Em 2023, a falta de um Marco de Cibersegurança, de uma Agência Nacional de Cibersegurança, e de um sistema capaz de preservar a cibersegurança nas suas diferentes dimensões e promover a soberania digital não é aceitável.

Para contribuir de maneira proativa ao desenvolvimento de um debate público urgente sobre esses temas essenciais pelo futuro do Brasil, esse trabalho se conclui com uma proposta inicial para um Marco de Cibersegurança e Soberania Digital, voltada a promover um ambiente digital seguro e sustentável e capaz de traduzir o enorme conhecimento gerado pelos *stakeholders* brasileiros em políticas públicas e ações concretas pelo desenvolvimento do País.

De forma tangencial, porém não menos importante, dentre as proposições relativas à flexibilização do perfil repressivo dos modelos regulatórios sobre a matéria, destaca-se a necessidade de se promover uma reflexão acerca de eventual política de incentivos

fiscais em prol da implementação de medidas preventivas de segurança da informação – com especial enfoque na cibersegurança – nas organizações.

Consciente do enorme desafio representado pela criação de um novo marco regulatório e de um novo sistema de governança, nossa proposta é intencionalmente principiológica, adotando uma abordagem “minimalista”, considerando que a melhor forma para detalhar os pontos essenciais analisados ao longo deste trabalho e apresentados em forma de sugestão normativa nesta seção seja um debate público aberto, inclusivo e democrático.

4.1 Proposta de Marco de Cibersegurança e Soberania Digital

Art. 1 A finalidade desta lei é a proteção e promoção da cibersegurança e da soberania digital do País fundamentadas no pleno respeito dos direitos fundamentais garantidos pela Constituição da República Federativa do Brasil.

Art. 2 Esta lei visa garantir a segurança dos indivíduos, dos sistemas digitais, das infraestruturas de acesso, das infraestruturas críticas, dos bancos de dados e dos aplicativos, bem como a capacidade das autoridades nacionais de regular essas tecnologias digitais no Brasil.

Art. 3 **Princípios.** A disciplina da cibersegurança e a promoção da soberania digital baseiam-se nos seguintes princípios:

- I. O respeito aos direitos fundamentais.
- II. O pleno exercício da autodeterminação, nas suas diferentes concepções.
- III. A segurança.
- IV. A soberania nacional.
- V. A visão abrangente e sistêmica da cibersegurança.
- VI. A educação como alicerce fundamental para o fomento da cultura em cibersegurança e o fortalecimento da soberania digital.
- VII. A articulação entre as diferentes dimensões e atores da segurança cibernética.

- VIII. A cooperação internacional.
- IX. O desenvolvimento econômico e tecnológico e a inovação.
- X. A livre iniciativa, a livre concorrência e a defesa do consumidor.
- XI. O pleno exercício da cidadania pelas pessoas naturais.

Art. 4 **Definições.** Para os propósitos desta lei:

- I. “Cibersegurança” se refere ao conjunto de normas, medidas e práticas utilizadas para garantir a proteção de sistemas digitais e bancos de dados de acesso não autorizado, uso, divulgação, interrupção, modificação ou destruição, bem como a proteção de usuários de sistemas digitais e de titulares de dados.
- II. “Soberania digital” se refere à capacidade do País de desenvolver a competência e literacia digital de sua população, e garantir a cibersegurança, o desenvolvimento sustentável, e a regulação efetiva de sua própria infraestrutura digital.
- III. “Tecnologias digitais” se referem a sistemas digitais, infraestruturas de acesso, infraestruturas críticas, bancos de dados e aplicativos.
- IV. “Sistema digital” se refere a quaisquer sistemas de computadores, redes eletrônicas ou dispositivos que são usados para processar, armazenar ou transmitir dados.
- V. “Infraestrutura de acesso” se refere a qualquer infraestrutura, e seus componentes, que seja instrumental para a provisão do acesso à Internet.
- VI. “Infraestrutura crítica” se refere a qualquer infraestrutura, e seus componentes, que seja instrumental para a provisão de águas, energia, transporte, comunicações, finanças, biossegurança e bioproteção e defesa.
- VII. “Banco de dados” se refere a qualquer coleção de informações estruturadas e armazenadas eletronicamente em um sistema digital.
- VIII. “Aplicativo” refere-se a qualquer tipo de software concebido para desempenhar um conjunto de tarefas específicas para executar determinados trabalhos.
- IX. “Dado estratégico” se refere a qualquer informação sobre o funcionamento de infraestruturas críticas.

- X. “Agente de cibersegurança” se refere à pessoa física ou jurídica responsável pela correta implementação dos padrões de cibersegurança.
- XI. “Cibercrime” se refere ao acesso não autorizado, uso, divulgação, interrupção, modificação ou destruição de sistemas digitais, redes e dados.

Art. 5 Estratégia Nacional de Cibersegurança e Soberania Digital.

A União deverá desenvolver, implementar e atualizar periodicamente uma Estratégia Nacional de Cibersegurança e Soberania Digital que inclua medidas para proteger os indivíduos usuários de sistemas digitais, os sistemas digitais, as infraestruturas de acesso, as infraestruturas críticas, os bancos de dados, e os aplicativos no País. A estratégia deverá incluir disposições para desenvolvimento de educação multigeracional, em plena sinergia com a Política Nacional de Educação Digital, estabelecimento e fortalecimento de capacidades técnicas e operacionais, gestão de riscos, resposta a incidentes, cooperação ao nível nacional e internacional e definição de papéis e responsabilidades.

Art. 6 Soberania digital. O objetivo da soberania digital é desenvolver a capacidade da população de entender o funcionamento das tecnologias digitais, participar do desenvolvimento de tais tecnologias,, e manter a capacidades das autoridades nacionais de regula-las, promovindo um ecossistema digital sustentável no Brasil. Consideram-se como eixos da soberania digital:

- I. A Autodeterminação informativa. A capacidade individual e coletiva de exercer controle sobre os dados pessoais e os dados públicos será promovida por meio de ações de formação, educação, treinamento, pesquisa e desenvolvimento.
- II. O acesso significativo à conectividade. A acesso não discriminatório e universal à Internet deverá ser garantido, junto com a possibilidade de usar dispositivos apropriados e volume de dados apropriados.
- III. O acesso significativo e o desenvolvimento de software. O uso e o desenvolvimento de aplicações de software, inclusive em formato livre e aberto, serão incentivados e facilitados, para contribuir ao desenvolvimento de bens públicos e infraestruturas publicas digitais.

- IV. O acesso à conteúdo educacional aberto. O uso de material educacional produzido com fundos públicos deverá ser permitido e tal material consolidado em repositórios públicos de conteúdo educacional aberto facilmente acessíveis para qualquer indivíduo.
- V. A promoção de bens comuns digitais e bens públicos digitais. A pesquisa e o desenvolvimento de bens comuns digitais, estabelecidos organizados e gerenciados de forma cooperativa, e bens públicos digitais, estabelecidos organizados e gerenciados pelos poderes públicos, será promovido e apoiado.
- VI. A formação digital. A regulamentação específica deve estabelecer espaços de formação continuada para professora/es das redes públicas de ensino, em que possam, principalmente, compartilhar as experiências educativas em cibersegurança, como forma de fomentar construção de conhecimento coletivo sobre as tecnologias digital.
- VII. As tecnologias de educação seguras e soberanas. Aplicativos de educação deverão ser auditáveis e auditadas para garantir o pleno gozo dos direitos dos usuários, particularmente no que diz respeito a segurança da informação e proteção de dados pessoais.
- VIII. O compartilhamento ágil de informações em segurança cibernética. As empresas fornecedoras de sistemas digitais deverão informar prontamente ao Centro de Prevenção, Tratamento e Resposta a Incidentes Cibernéticos do Governo, CTIR-Gov, e disponibilizar as informações claras e acessíveis, em modelo a ser definido pela Agência Nacional de Cibersegurança. As empresas também deverão desenvolver e manter páginas web em seus sites oficiais voltadas para disseminação de informações em segurança cibernética.

Art. 7 **Garantia da soberania digital**. Impulsionados pela Agência Nacional de Cibersegurança, os poderes públicos deverão buscar a consolidação da soberania digital. Para tal finalidade, regulamentação a ser definida pela autoridade nacional deve estabelecer medidas para:

- I. Especificar os padrões de cibersegurança;
- II. Definir o mecanismo de certificação de segurança para garantir que tecnologias digitais atendam aos padrões de segurança nacionais e não representem riscos para a soberania digital;
- III. Garantir a educação digital intergeracional e crítica para que tecnologias sejam desenvolvidas e usadas da maneira mais segura no Brasil;
- IV. Fomentar investimentos em pesquisa e desenvolvimento e implementação de novas tecnologias e soluções de segurança cibernética;
- V. Especificar as modalidades de criação de sistemas digitais nacionais, inclusive promovendo o desenvolvimento de infraestrutura de acesso e crítica, quando tais infraestruturas necessitem estar sob controle direto do País;
- VI. Definir o regime de proteção de dados estratégicos, inclusive os casos de armazenamento de tais dados dentro das fronteiras do país, incluindo a regulamentação da coleta, uso e armazenamento de dados pessoais;
- VII. Garantir a cooperação multissetorial ao nível nacional e internacional no pleno respeito da soberania digital; e
- VIII. Manter e fomentar a criação local de espaços de associativismo, para participação popular de usuária/os de tecnologias digitais nas formulações da regulação complementar a esta legislação, estimulando a permanente atualização da concepção da cibersegurança.

Art. 8 **Padrões de Cibersegurança.** Esta lei estabelece requisitos mínimos para garantir a cibersegurança. Estes requisitos são baseados nas melhores práticas internacionais e deverão ser especificados em padrões de cibersegurança regularmente revisados e atualizados pela Agência Nacional de Cibersegurança.

- I. Os padrões de cibersegurança devem ser estabelecidos, implementados e divulgados em cooperação com todas as agências reguladoras interessadas. A plena sinergia entre os setores interessados é garantida por meio do Comitê Multissetorial de Cibersegurança da Agência Nacional de Cibersegurança e do Comitê Gestor da Segurança da Informação do Gabinete de Segurança Institucional.

- II. Além da indicação dos elementos formais e substanciais essenciais para garantir a cibersegurança os padrões devem especificar também quais informações devem ser divulgadas e em qual formato para demonstrar a conformidade com os padrões de cibersegurança e para permitir a avaliação do nível de maturidade de cibersegurança.

Art. 9 **Os Agentes de cibersegurança** são responsáveis pela implementação dos padrões que deverão ser especificados pela Agência Nacional de Cibersegurança em coordenação com as agências nacionais responsáveis pela regulamentação de setores específicos. A garantia da cibersegurança baseia-se na:

- I. Responsabilidade: Cada agente de cibersegurança é responsável pela correta implementação dos padrões de cibersegurança estabelecidos nesta lei. Isso inclui a obrigação de atualizar periodicamente as medidas implementadas.
- II. Identificação e avaliação de riscos: Cada agente de cibersegurança é responsável pela identificação e avaliação de riscos para a segurança cibernética e pela tomada das medidas necessárias para mitigá-los.
- III. Monitoramento. Cada agente de cibersegurança é responsável por avaliar a conformidade das medidas técnicas e organizacionais com os padrões de cibersegurança definidos pela Agência Nacional de Cibersegurança. Monitoramento inclui auditorias regulares e inspeções, bem como a utilização de ferramentas de verificação automatizadas.
- IV. Testes regulares: Cada agente de cibersegurança é responsável pela realização de testes regulares para verificar a eficácia das medidas de segurança implementadas.
- V. Treinamento: Cada agente de cibersegurança é responsável pela organização de medidas voltadas ao treinamento de funcionários sobre os padrões e as melhores práticas de cibersegurança.
- VI. Educação e conscientização: a Agência Nacional de Cibersegurança e o Ministério da Educação são responsáveis pela definição de políticas educacionais efetivas voltadas ao aprimoramento e modernização da educação digital e conscientização sobre os riscos e as medidas de cibersegurança.

- VII. **Contratos com terceiros:** qualquer contrato voltado a regular o uso de tecnologias digitais deve incluir cláusulas de segurança cibernética em contratos com terceiros, incluindo provedores de serviços e fornecedores, sendo o agente de cibersegurança responsável pela inclusão de tais cláusulas antes da formalização do negócio jurídico.
- VIII. **Documentação:** Cada agente de cibersegurança é responsável pela documentação das medidas de cibersegurança implementadas e pela manutenção dos registros das auditorias e testes realizados.
- IX. **Disponibilidade de recursos:** qualquer fabricante, provedor ou operador de tecnologias digitais deve garantir que haja recursos disponíveis para lidar com incidentes de segurança cibernética, incluindo pessoal treinado e equipamentos.
- X. **Conformidade:** Cada agente de cibersegurança é responsável pela garantia da conformidade com os padrões de cibersegurança estabelecidos, incluindo a criação de processos aptos a implementar efetivamente as medidas técnicas e organizacionais definidas pela Agência Nacional de Cibersegurança.

Art. 10 **Certificação de Cibersegurança.** O governo deverá estabelecer um programa de certificação para tecnologias digitais. A certificação deverá indicar que as tecnologias digitais foram avaliadas e que estão em conformidade com os padrões de cibersegurança estabelecidos por esta lei e a regulamentação da ANC. A regulamentação sobre Certificação de Cibersegurança deve incluir as seguintes disposições:

- I. **Objetivo:** A regulamentação deve estabelecer o objetivo de garantir a segurança dos sistemas e dados digitais através do estabelecimento de um programa de certificação de cibersegurança.
- II. **Responsabilidade:** A regulamentação deve estabelecer que as organizações e indivíduos são responsáveis por garantir a segurança dos sistemas e dados digitais e, portanto, estão sujeitos ao programa de certificação.
- III. **Critérios de certificação:** A regulamentação deve estabelecer os critérios de certificação que as organizações e indivíduos

devem cumprir para serem certificados. Esses critérios devem ser baseados em melhores práticas internacionais e devem incluir requisitos para a segurança dos sistemas e dados, gestão de riscos e incidentes, privacidade e proteção de dados.

- IV. Processo de certificação: A regulamentação deve estabelecer o processo de certificação, incluindo a documentação necessária, os procedimentos de avaliação e as autoridades responsáveis pela certificação.
- V. Validade da certificação: A regulamentação deve estabelecer a validade da certificação, incluindo a frequência da renovação e os requisitos para manter a certificação válida.
- VI. Sanções: A regulamentação deve estabelecer as sanções aplicáveis às organizações e indivíduos que não cumprirem os critérios de certificação ou que não renovem a certificação.
- VII. Transparência: A regulamentação deve estabelecer mecanismos para garantir a transparência do processo de certificação, incluindo a publicação de listas de organizações e indivíduos certificados.
- VIII. Conformidade: A regulamentação deve estabelecer mecanismos para garantir a conformidade com os requisitos de certificação, incluindo a criação de órgãos reguladores e a designação de autoridades responsáveis pela aplicação das regras.
- IX. A regulamentação sobre certificação de cibersegurança deve ser adaptada ao contexto do país, considerando as necessidades e especificidades de cada setor econômico.

Art. 11 **Resposta a Incidentes de Cibersegurança.** A Agência Nacional de Cibersegurança estabelece o sistema de resposta a incidentes de cibersegurança para responder a incidentes de cibersegurança. O sistema estabelece uma plataforma de comunicação permanente e segura entre as redes de gestão de incidentes existentes, inclui disposições para investigação de incidentes, gerenciamento de incidentes e recuperação de incidentes, e favorece a cooperação multissetorial.

- I. Plano de resposta a incidentes: Cada agente de cibersegurança é responsável pela definição do plano de resposta a incidentes de cibersegurança, incluindo procedimentos para identificar, investigar e responder a incidentes de cibersegurança.

- II. Notificação de incidentes: Cada agente de cibersegurança é responsável pela notificação de cada incidente de cibersegurança que possa acarretar risco ou dano relevante à Agência Nacional de Cibersegurança num prazo de máximo de 2 dias.
- III. Cooperação: A Agência Nacional de Cibersegurança estabelece o sistema de cooperação multissetorial entre as organizações, pessoas e autoridades responsáveis pela resposta a incidentes de cibersegurança.
- IV. Capacitação: A Agência Nacional de Cibersegurança publica e atualiza anualmente os padrões de cibersegurança, baseados nas melhores práticas internacionais.
- V. Testes: A Agência Nacional de Cibersegurança regulamenta as medidas de realização de testes regulares de capacidades de resposta a incidentes de cibersegurança.
- VI. Conformidade: A Agência Nacional de Cibersegurança estabelece os mecanismos para garantir a conformidade com os requisitos de resposta a incidentes de cibersegurança.

Art. 12 **Cibercrime**. Esta lei dá suporte ao combate ao cibercrime, incluindo acesso não autorizado, uso, divulgação, interrupção, modificação ou destruição de dados e tecnologias digitais. As penalidades para crimes cibernéticos devem ser proporcionais à gravidade do crime e podem incluir multas, prisão e/ou confisco de ativos.

- I. O objetivo de combater o cibercrime é a proteção dos cidadãos e das organizações públicas e privadas contra crimes cibernéticos.
- VII. Responsabilidade de investigação e processamento: As autoridades competentes têm a responsabilidade de investigar e processar casos de cibercrime.
- VIII. Cooperação Internacional: As autoridades competentes participam de mecanismos para cooperação internacional no combate ao cibercrime, incluindo a troca de informações e a realização de operações conjuntas, no pleno respeito das obrigações internacionais.
- IX. Conformidade: As autoridades competentes devem estabelecer mecanismos para garantir a conformidade com as regras de combate ao cibercrime, incluindo a criação de órgãos responsáveis pela aplicação das regras.

Art. 13 **Proteção de dados estratégicos e dados sensíveis.** A Agência Nacional de Cibersegurança deve estabelecer regulamentos de proteção de dados estratégicos e sensíveis para garantir que tais dados sejam tratados de maneira consistente com os padrões de cibersegurança definidos nesta lei. Tais regulamentos devem ao menos estabelecer:

- I. Classificação de dados: A regulamentação deve estabelecer critérios claros para classificar os dados estratégicos e sensíveis, de forma compatível com a legislação em vigor, e estabelecer medidas de segurança apropriadas para cada tipo de dado.
- II. Segurança da informação: A regulamentação deve especificar medidas de segurança da informação para garantir a efetiva confidencialidade, integridade e disponibilidade dos dados estratégicos e sensíveis.
- III. Controle de acesso: A regulamentação deve estabelecer mecanismos efetivos para controlar o acesso aos dados estratégicos e sensíveis, incluindo autenticação forte, autorização de acesso e registro de auditoria.
- IV. Gerenciamento de incidentes: A regulamentação deve estabelecer procedimentos para gerenciamento de incidentes de cibersegurança cibernética, incluindo a detecção, investigação, contenção, recuperação e análise pós-incidente.
- V. Conformidade: A regulamentação deve estabelecer mecanismos para garantir a conformidade com as regulamentações de segurança de dados, incluindo a criação de órgãos reguladores e a designação de responsáveis pela aplicação das regras.
- VI. Responsabilidade: A regulamentação deve estabelecer a responsabilidade de cada organização em proteger os dados estratégicos e sensíveis, incluindo a obrigação de implementar medidas de segurança adequadas e de notificar incidentes de cibersegurança às autoridades competentes.
- VII. Educação, conscientização e treinamento: A regulamentação deve incluir medidas para educar, conscientizar e treinar funcionários sobre as melhores práticas para proteger os dados estratégicos e sensíveis.

Art. 14 **Educação multigeracional, conscientização e treinamento.** A regulamentação deve estabelecer o objetivo de garantir que a população inteira esteja educada e consciente sobre os riscos de cibersegurança e as medidas de proteção disponíveis, e deve prever que entidades públicas e privadas forneçam treinamento regular para seus funcionários sobre ciberseguranças.

- I. Currículo de Educação em Cibersegurança. A educação em cibersegurança deve ser incluída no currículo escolar e universitário, e os seus temas geradores devem ser buscados a partir das urgências de cada comunidade educacional, e poderão incluir temas como a educação sobre as ameaças cibernéticas e as melhores práticas para se proteger contra tais ameaças, estimulando a cocriação de programas de segurança cibernética e cuidado digital por parte da população interessada.
- II. Programas de Conscientização. A regulamentação deve estabelecer a criação de programas de formação de consciência crítica em relação às tecnologias e ameaças digitais, bem como oficinas práticas para a população em geral, incluindo campanhas de conscientização direcionadas às diferentes faixas etárias, eventos educacionais, e estimulando parcerias com atores da área da educação e associativo.
- III. Responsabilidade das empresas. A regulamentação deve estabelecer a responsabilidade das empresas de educar e avaliar os conhecimentos de seus funcionários e conscientizar clientes sobre cibersegurança. De forma complementar, a regulamentação deve garantir que a população esteja educada sobre a responsabilidade de empresas na promoção da cibersegurança;
- IV. Conformidade. A regulamentação deve estabelecer mecanismos para garantir a conformidade com as políticas educacionais e conscientização de cibersegurança, incluindo a criação de secretaria especializada em educação digital no âmbito do Ministério da Educação.
- V. Participação da comunidade. A regulamentação deve estabelecer mecanismos para envolver a comunidade no esforço de educação e conscientização, incluindo parcerias com grupos comunitários, organizações não governamentais e

movimentos sociais. As parcerias podem ter como objetivo práticas educativas voltada para construção de tecnologias digitais, para promoção e reforço da soberania digital.

- VI. Continuidade. A regulamentação deve estabelecer a necessidade de continuidade na educação e conscientização de cibersegurança para garantir que a população esteja sempre atualizada e ciente de todo o conhecimento acumulado necessário para produção das tecnologias digitais.
- VII. Fornecimento de materiais. A regulamentação poderá contar com programas de fornecimento de materiais necessários para a prática educativa em segurança cibernética, considerando especialmente o uso de material em acesso livre.
- VIII. Parágrafo Único. A execução da regulamentação deverá destinar parte do seu orçamento para estabelecimento e/ou fomento à programas de educação digital, voltados para o estímulo à soberania digital da população brasileira, e que contemplem os eixos de ação apresentados.

Art. 15 **Execução da lei pela Agência Nacional de Cibersegurança.** A Agência Nacional de Cibersegurança deve ter como objetivo garantir a segurança cibernética no país através da regulamentação e supervisão de atividades relacionadas à cibersegurança.

- I. Autoridade: A agência reguladora deve ser uma entidade independente, com autoridade para regular e supervisionar as atividades relacionadas à cibersegurança no país.
- II. Funções: As funções da agência reguladora incluem a elaboração de regulamentos para a execução das políticas relacionadas à cibersegurança em âmbito federal, a supervisão e a fiscalização das atividades relacionadas à cibersegurança, a investigação de violações e a aplicação de sanções e a coordenação com outras agências.
- III. Composição: A agência reguladora deve ser composta por especialistas em cibersegurança, incluindo representantes do governo, setor privado e setor acadêmico. A estrutura interna da agência é composta por:

§ 1º Conselho Diretor, órgão máximo de direção;

§ 2º Comitê Multissetorial de Cibersegurança;

§ 3º Rede Nacional de Cibersegurança;

§ 4º Corregedoria;

§ 5º Ouvidoria;

§ 6º Órgão de assessoramento jurídico próprio;

§ 7º Unidades administrativas e unidades especializadas necessárias à aplicação do disposto nesta lei.

- IV. Financiamento: A agência reguladora deve ter recursos financeiros suficientes para cumprir suas funções de maneira independente.
- V. Transparência: A agência reguladora deve ser transparente em suas decisões e ações, publicando relatórios periódicos, fornecendo informações detalhadas sobre o processo de elaboração e de implementação de suas regulamentações e atividades de supervisão, e a participação dos demais setores da sociedade em suas atividades.
- VI. Cooperação Internacional: A agência reguladora deve trabalhar em cooperação com agências reguladoras internacionais para garantir a conformidade com regulamentações internacionais e para trocar informações e melhores práticas.
- VII. Interação e coordenação com outras agências: A agência reguladora deve trabalhar em conjunto com todas as outras agências governamentais representadas no Comitê Multissetorial de Cibersegurança, para garantir que as políticas e regulamentações de cibersegurança sejam implementadas de forma coerente e eficaz.

Art. 16 Comitê Multissetorial de Cibersegurança. O Comitê Multissetorial de Cibersegurança assiste a Agência Nacional de Cibersegurança e garante a plena sinergia com o Comitê Gestor da Segurança da Informação.

- I. Composição do comitê multissetorial: O comitê deve ser composto por representantes de diferentes setores, incluindo todas as agências reguladoras, setor privado, setor acadêmico, setor de tecnologia, movimentos sociais e outras organizações

da sociedade civil. O comitê atua em sinergia com o Comitê Gestor da Segurança da Informação, integrando parte de seus membros. O objetivo da composição do comitê é garantir que as perspectivas de diferentes setores sejam consideradas na implementação da cibersegurança e a atividade da Agência Nacional de Cibersegurança seja organizada em total sinergia com as outras agências reguladoras.

- II. Grupos de trabalho. Para facilitar a execução de suas tarefas e a interação e coordenação com outras agências, o Comitê Multissetorial de Cibersegurança estabelece grupos de trabalho coordenados por membros do Comitê. Os grupos de trabalho podem incluir membros da Rede Nacional de Cibersegurança e podem ser criados com intuito de suportar o Comitê Gestor da Segurança da Informação.
- III. Identificação de ameaças e vulnerabilidades: O comitê deve realizar estudos e consultas anuais voltadas à análise de risco e identificação das principais ameaças e vulnerabilidades à cibersegurança no país.
- IV. Desenvolvimento de estratégias de cibersegurança: Com base na análise de risco, o comitê deve desenvolver estratégias para abordar as principais ameaças e vulnerabilidades identificadas.
- V. Divulgação de medidas de cibersegurança: As medidas de cibersegurança devem ser divulgadas em todos os setores, incluindo governo, setor privado, sociedade civil e setor acadêmico. Essas medidas podem incluir a criação de regulamentações por agências específicas, programas de treinamento, programas de conscientização e mecanismos de cooperação entre setores.
- VI. Monitoramento e avaliação: O comitê deve monitorar e avaliar regularmente a eficácia das medidas de segurança.
- VII. Responsabilidade e conformidade: A regulamentação deve estabelecer mecanismos para garantir a conformidade com as regras de cibersegurança, incluindo a criação de órgãos reguladores e a designação de autoridades responsáveis pela aplicação das regras.

- VIII. Participação da comunidade: A implementação deve incluir mecanismos para envolver a comunidade nacional, incluindo parcerias com grupos comunitários e organizações não-governamentais.
- IX. Continuidade: A implementação deve ser contínua, com atualizações regulares para garantir que a cibersegurança esteja sempre atualizada e adaptada às novas ameaças e vulnerabilidades.
- Art. 17 **Rede Nacional de Cibersegurança.** A Rede Nacional de Cibersegurança assiste a Agência Nacional de Cibersegurança.
- X. Composição da Rede Nacional de Cibersegurança. Integra a Rede Nacional de Cibersegurança qualquer entidade cujo objetivo seja a pesquisa, desenvolvimento ou a atuação no âmbito da cibersegurança e seja reconhecida como tal pelo Comitê Multissetorial de Cibersegurança.
- XI. Disseminação de boas práticas. A Rede Nacional de Cibersegurança promove a disseminação das mais recentes práticas, produtos e serviços de cibersegurança.
- XII. Estímulo à pesquisa. A Rede Nacional de Cibersegurança indica áreas de pesquisa de cibersegurança urgentes que necessitem de investimento.
- XIII. Coleta e atualização de conhecimentos. A Rede Nacional de Cibersegurança favorece a coleta e sistematização de pesquisa sobre cibersegurança para favorecer uma visão geral atualizada da cibersegurança pelas partes interessadas.
- XIV. Promoção da colaboração nacional. A Rede Nacional de Cibersegurança promove e facilita a colaboração entre pesquisadores, representantes da indústria, profissionais e órgãos públicos a nível estadual e federal.
- XV. Intercâmbios internacionais. A Rede Nacional de Cibersegurança promove intercâmbios entre membros nacionais e entidades voltadas ao fortalecimento da cibersegurança em nível internacional.
- XVI. Divulgação. A Rede Nacional de Cibersegurança apoia o Comitê Multissetorial de Cibersegurança na elaboração de estudos e divulgação de informações sobre cibersegurança.

XVII. Grupos de trabalho. Para facilitar a execução de suas tarefas, a Rede Nacional de Cibersegurança estrutura-se em grupos de trabalho coordenados pelo Comitê Multissetorial de Cibersegurança.

BIBLIOGRAFIA

- ACTIONAID. **\$2.8bn 'tax gap' exposed by ActionAid research reveals tip of the iceberg of 'Big Tech's big tax bill' in the global south.** Disponível em: <<https://actionaid.org/news/2020/28bn-tax-gap-exposed-actionaid-research-reveals-tip-iceberg-big-techs-big-tax-bill-global>>. Acesso em: 3 mar. 2023.
- ANSARI, M. F. et al. **The Impact and Limitations of Artificial Intelligence in Cybersecurity: A Literature Review.** Rochester, NY, 1 set. 2022. Disponível em: <<https://papers.ssrn.com/abstract=4323317>>. Acesso em: 7 jun. 2023.
- AVILA PINTO, R. Digital sovereignty or digital colonialism? New tensions of privacy, security and national policies. **Sur – International Journal on Human Rights**, v. 27, n. jul, p. 15-27, 16 jul. 2018.
- BALLESTRIN, L. **O sul global como projeto político.** Disponível em: <<https://www.horizontesaosul.com/single-post/2020/06/30/o-sul-global-como-projeto-politico>>. Acesso em: 7 mar. 2023.
- BARRY, D.; DOYLE, A.; ERICSON, D. **Insurance as governance.** [s.l.] University of Toronto Press, 2003.
- BARTOLOMÉ, M. Redes sociais, desinformación, cibersoberanía y vigilancia digital: una visión desde la ciberseguridad. **Revista de Estudios en Seguridad Internacional**, v. 7, n. 2, p. 167-185, 1 dez. 2021.
- BCB. **Pix.** Disponível em: <<https://www.bcb.gov.br/estabilidadefinanceira/pix>>. Acesso em: 7 jun. 2023.
- BELLI, L. **De la gouvernance à la régulation de l'Internet.** Paris: Berger-Levrault, 2016.
- BELLI, L. et al. **Community networks: The internet by the People, for the People.** Rio de Janeiro: FGV Direito Rio, 2017.
- BELLI, L. **Network self-determination: When building the Internet becomes a right.** **IETF Journal**, 28 mar. 2018a. 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, L. Neutralidade da rede, zero-rating e o Marco Civil da Internet. Em: **Governança e regulações da internet na América Latina.** Rio de Janeiro: FGV Direito Rio, 2018b. p. 175-204.
- BELLI, L. BRICS Countries to Build Digital Sovereignty. Em: BELLI, L. (Ed.). **CyberBRICS: Cybersecurity Regulations in the BRICS Countries.** Cham: Springer International Publishing, 2021a. p. 271-280.
- BELLI, L. CyberBRICS: A Multidimensional Approach to Cybersecurity for the BRICS. Em: BELLI, L. (Ed.). **CyberBRICS: Cybersecurity Regulations in the BRICS Countries.** Cham: Springer International Publishing, 2021b. p. 1-33.
- BELLI, L. Cybersecurity Policymaking in the BRICS Countries: From Addressing National Priorities to Seeking International Cooperation. **The African Journal of Information and Communication**, v. 28, 2021c.

- BELLI, L. New Data Architectures in Brazil, China, and India: From Copycats to Innovators, towards a post-Western Model of Data Governance. **Indian Journal of Law and Technology**, v. 18, n. 2, p. 1-58, 2022a.
- BELLI, L. Rússia também ataca Ucrânia pela internet; entenda a ciberguerra. **Folha de S. Paulo**, 26 fev. 2022b.
- BELLI, L. **Brasil precisa reconstruir sua soberania digital**. **Estadão**, 1 mar. 2023a. Disponível em: <<https://www.estadao.com.br/politica/blog-do-fausto-macedo/brasil-precisa-reconstruir-sua-soberania-digital/>>. Acesso em: 3 mar. 2023
- BELLI, L. **Exploring the Key AI Sovereignty Enablers (KASE) of Brazil, towards an AI Sovereignty Stack**. Rochester, NY, 31 maio 2023b. Disponível em: <<https://papers.ssrn.com/abstract=4465501>>. Acesso em: 13 jun. 2023.
- BELLI, L.; DA HORA, N. **ChatGPT: o que anima e o que assusta na nova inteligência artificial**. Disponível em: <<https://www1.folha.uol.com.br/tec/2023/01/chatgpt-o-que-anima-e-o-que-assusta-na-nova-inteligencia-artificial.shtml>>. Acesso em: 7 mar. 2023.
- BELLI, L.; DONEDA, D. **“Rede Limpa”ou segurança da informação? China Hoje**, 24 fev. 2021. Disponível em: <<http://www.chinahoje.net/rede-limpaou-seguranca-da-informacao/>>. Acesso em: 3 mar. 2023.
- BELLI, L.; GUGLIELMI, G. J. **L’État digital**. Paris: Berger-Levrault, 2022.
- BELLI, L.; HADZIC, S. **Community Networks as Enablers of Human Rights**. Rio de Janeiro: FGV Direito Rio, 2022.
- BELLI, L.; JIANG, M. **Digital Sovereignty in the BRICS Countries**. Cambridge, UK: Cambridge University Press, 2023.
- BELLI, L.; JORGE, S.; RAMOS, B. **Building Community Network Policies: A Collaborative Governance towards Enabling Frameworks**. Rio de Janeiro: FGV Direito Rio, 2019.
- BLACKBERRY. **Cylance Is BlackBerry Cybersecurity**. Disponível em: <<https://www.blackberry.com/us/en/products/cylance-endpoint-security/cylance-is-blackberry-cybersecurity>>. Acesso em: 7 jun. 2023.
- BRASIL. **Decreto n. 10.222/20**, 5 fev. 2020. Disponível em: <https://www.planalto.gov.br/ccivil_03/_ato2019-2022/2020/decreto/d10222.htm>. Acesso em: 2 mar. 2023.
- BRASIL. **Decreto n. 11.200/22**, 15 set. 2022. Disponível em: <https://www.planalto.gov.br/ccivil_03/_ato2019-2022/2022/decreto/D11200.htm>. Acesso em: 2 mar. 2023.
- BRASIL; SENADO FEDERAL. **Projeto de lei n. 4 de 2 de fevereiro de 2022**. Disponível em: <<https://www25.senado.leg.br/web/atividade/materias/-/materia/151507>>. Acesso em: 12 jun. 2023.
- BRIDI, S.; GREENWALD, G. **Documentos revelam esquema de agência dos EUA para espionar Dilma**. Disponível em: <<http://g1.globo.com/fantastico/noticia/2013/09/documentos-revelam-esquema-de-agencia-dos-eua-para-espionar-dilma-rousseff.html>>. Acesso em: 1 mar. 2023.

- BROWN, I. et al. *Cybersecurity for Elections: A Commonwealth Guide on Best Practice*. 2020.
- CAFÉ DA MANHÃ. **O que os ataques digitais da Rússia à Ucrânia mostram sobre a guerra cibernética**. Folha de S. Paulo, , 28 fev. 2022. Disponível em: <<https://www1.folha.uol.com.br/podcasts/2022/02/o-que-os-ataques-digitais-da-russia-a-ucrania-mostram-sobre-a-guerra-cibernetica-ouca-podcast.shtml>>. Acesso em: 3 mar. 2023.
- CALDERARO, A.; CRAIG, A. J. S. Transnational governance of cybersecurity: policy challenges and global inequalities in cyber capacity building. **Third World Quarterly**, v. 41, n. 6, p. 917-938, 2 jun. 2020.
- CARAMANCION, K. M. 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, p. 49, 12 abr. 2022.
- CASSIOLATO, J. E.; LASTRES, H. M. M. Sistemas de inovação e desenvolvimento: as implicações de política. **São Paulo em Perspectiva**, v. 19, n. 1, p. 34-45, mar. 2005.
- CERT.BR. **Incidentes Reportados ao CERT.br -- Janeiro a Dezembro de 2020**. Disponível em: <<https://cert.br/stats/incidentes/2020-jan-dec/top-cc.html>>. Acesso em: 2 mar. 2023.
- CESARINO, L. Como vencer uma eleição sem sair de casa: a ascensão do populismo digital no Brasil. **Internet & Sociedade**, v. 1, n. 1, 16 fev. 2020.
- CGI.BR; NIC.BR. **Por uma Internet mais segura**. Disponível em: <<https://bcp.nic.br/i+seg/>>. Acesso em: 7 jun. 2023.
- CHOUDHURY, S. P.; SHARMA, S.; JAIN, S. **Three Waves: Tracking the Evolution of India's Startups**. **Knowledge at Wharton**, 5 nov. 2019. Disponível em: <<https://knowledge.wharton.upenn.edu/article/three-waves-tracking-evolution-indias-startups/>>. Acesso em: 3 mar. 2023.
- CHRISTL, W. How Companies Use Personal Data Against People. Automated Disadvantage, Personalized Persuasion, and the Societal Ramifications of the Commercial Use of Personal Information. 10 out. 2017.
- CIANCAGLINI, V. et al. **Malicious Uses and Abuses of Artificial Intelligence**. The Hague: Trend Micro Research; UNICRI; EC3, 6 dez. 2021. Disponível em: <https://www.europol.europa.eu/cms/sites/default/files/documents/malicious_uses_and_abuses_of_artificial_intelligence_europol.pdf>.
- CIEB. **Marco conceitual: Escola Conectada**: Materiais de referência. São Paulo: Centro de Inovação para a Educação Brasileira, 2021. Disponível em: <<https://cieb.net.br/wp-content/uploads/2021/07/Marco-Conceitual-Escola-Conectada.pdf>>.
- 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.
- CLARKE, RICHARD A.; CLARKE, ROBERT K. **Guerra Cibernética: a próxima ameaça à segurança e o que fazer a respeito**. Bruno Salgado Guimarães. Rio de Janeiro: Brasport, 2015.

- CODING RIGHTS. **Megaeventos: Um Legado de Vigilância**. Disponível em: <<https://legadovigilante.codingrights.org/>>. Acesso em: 7 jun. 2023.
- COMISSÃO EUROPEIA. **Diretiva Ciber-Resiliência: novas regras em matéria de cibersegurança para produtos digitais e serviços auxiliares**. Disponível em: <https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/13410-Diretiva-Ciber-Resiliencia-novas-regras-em-materia-de-ciberseguranca-para-produtos-digitais-e-servicos-auxiliares_pt>. Acesso em: 3 mar. 2023.
- COULDRIY, N.; MEJIAS, U. A. Data Colonialism: Rethinking Big Data's Relation to the Contemporary Subject. **Television & New Media**, v. 20, n. 4, p. 336-349, 1 maio 2019.
- COUTURE, S. **The Diverse Meanings of Digital Sovereignty**. **Global Media Technologies and Cultures Lab**, 5 ago. 2020. Disponível em: <<https://globalmedia.mit.edu/2020/08/05/the-diverse-meanings-of-digital-sovereignty/>>. Acesso em: 3 mar. 2023.
- DARKTRACE. **Darktrace**. Disponível em: <<https://pt-br.darktrace.com/>>. Acesso em: 7 jun. 2023.
- DAUCÉ, F.; MUSIANI, F. Infrastructure-embedded control, circumvention and sovereignty in the Russian Internet: An introduction. **First Monday**, 7 abr. 2021.
- DIXON, W.; EAGAN, N. **3 ways AI will change the nature of cyber attacks**. Disponível em: <<https://www.weforum.org/agenda/2019/06/ai-is-powering-a-new-generation-of-cyberattack-its-also-our-best-defence/>>. Acesso em: 12 jun. 2023.
- DRAKE, W. J.; CERF, V. G.; KLEINWÄCHTER, W. **Internet Fragmentation: An Overview**. Geneva, jan. 2016.
- EDQUIST, C. Systems of Innovation: Perspectives and Challenges. Em: **The Oxford Handbook of Innovation**. Oxford: Oxford University Press, 2006. p. 181-208.
- EICHENSEHR, K. E. The law and politics of cyberattack attribution. **UCLA L. Rev.**, v. 67, p. 520, 2020.
- ENISA. **Foreign Information Manipulation and Interference (FIMI) and cybersecurity: threat landscape**. LU: Publications Office, 2022.
- ENISA. **ENISA threat landscape: transport sector (January 2021 to October 2022)**. LU: Publications Office, mar. 2023. Disponível em: <<https://data.europa.eu/doi/10.2824/553997>>. Acesso em: 7 jun. 2023.
- EQUIPE TECMUNDO. **Governo do Ceará sofre ataque hacker com motivações políticas**. Disponível em: <<https://www.tecmundo.com.br/seguranca/256773-governo-ceara-sofre-ataque-hacker-motivacoes-politicas.htm>>. Acesso em: 7 fev. 2023.
- EU DISINFOLAB. **Why Disinformation is a Cybersecurity Threat**. **EU DisinfoLab**, [s.d.]. Disponível em: <<https://www.disinfo.eu/advocacy/why-disinformation-is-a-cybersecurity-threat/>>. Acesso em: 7 fev. 2023.

- EVANGELISTA, R.; BRUNO, F. WhatsApp and political instability in Brazil: targeted messages and political radicalisation. **Internet Policy Review**, v. 8, n. 4, 31 dez. 2019.
- FICHTNER, L. What kind of cyber security? Theorising cyber security and mapping approaches. **Internet Policy Review**, v. 7, n. 2, 15 maio 2018.
- FLORIDI, L. 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.
- FMPRC. **International Code of Conduct for Information Security**. Disponível em: <https://www.fmprc.gov.cn/mfa_eng/wjdt_665385/2649_665393/201109/t20110913_679318.html>. Acesso em: 7 mar. 2023.
- FUSTER, G. G.; JASMONTAITE, L. Cybersecurity Regulation in the European Union: The Digital, the Critical and Fundamental Rights. Em: CHRISTEN, M.; GORDIJN, B.; LOI, M. (Eds.). **The Ethics of Cybersecurity**. The International Library of Ethics, Law and Technology. Cham: Springer International Publishing, 2020. p. 97–115.
- G1. **Aplicativo do ConecteSUS deixa de apresentar vacinas; site está fora do ar**. Disponível em: <<https://g1.globo.com/saude/noticia/2021/12/10/site-do-ministerio-da-saude-sofre-ataque-de-hackers-e-sai-do-ar.ghtml>>. Acesso em: 7 fev. 2023.
- GAILLARD, J. C.; MERCER, J. From knowledge to action: Bridging gaps in disaster risk reduction. **Progress in Human Geography**, v. 37, n. 1, p. 93–114, 1 fev. 2013.
- GALF, R. Plano do governo Lula contra fake news gera divergência. **Folha de S. Paulo**, 21 jan. 2023.
- GELUVARAJ, B.; SATWIK, P. M.; ASHOK KUMAR, T. A. **The future of cybersecurity: Major role of artificial intelligence, machine learning, and deep learning in cyberspace**. International Conference on Computer Networks and Communication Technologies: ICCNCT 2018. **Anais...** Springer, 2019.
- GILES, M. **Explainer: What is post-quantum cryptography?** Disponível em: <<https://www.technologyreview.com/2019/07/12/134211/explainer-what-is-post-quantum-cryptography/>>. Acesso em: 18 fev. 2023.
- GROHMANN, R. Cooperativismo de plataforma como alternativa à plataformização do trabalho. **Revista Rosa**, v. 4, n. 1, 27 ago. 2021.
- HOSSAIN FARUK, M. J. et al. **A Review of Quantum Cybersecurity: Threats, Risks and Opportunities**. 2022 1st International Conference on AI in Cybersecurity (ICAIC). **Anais...** Em: 2022 1ST INTERNATIONAL CONFERENCE ON AI IN CYBERSECURITY (ICAIC). Victoria, TX, USA: IEEE, 24 maio 2022. Disponível em: <<https://ieeexplore.ieee.org/document/9896970/>>. Acesso em: 18 fev. 2023.
- HUREL, L. M. **Cibersegurança no Brasil: Uma análise da estratégia nacional**: Artigos Estratégicos. Rio de Janeiro: Instituto Igarapé, abr. 2021.
- IBGE. **PNAD Continua TIC 2016: 94,2% das pessoas que utilizaram a Internet o fizeram para trocar mensagens**. Disponível em: <<https://agenciadenoticias.ibge.gov.br/agencia-sala-de-imprensa/2013-agencia-de-noticias/releases/20073-pnad-continua-tic-2016-94-2-das-pessoas-que-utilizaram-a-internet-o-fizeram-para-trocar-mensagens>>. Acesso em: 3 mar. 2023.

- IBM. **Watson for Cyber Security**. Disponível em: <<https://www.ibm.com/blogs/nordic-msp/watson-cyber-security/>>. Acesso em: 7 jun. 2023.
- IDEC; INSTITUTO LOCOMOTIVA. **Acesso à internet móvel pelas classes CDE**. São Paulo: IDEC e Instituto Locomotiva, nov. 2021. Disponível em: <https://idec.org.br/sites/default/files/pesquisa_locomotiva_relatorio.pdf>. Acesso em: 3 mar. 2023.
- ISO. **ISO/IEC 27001:2005**. Disponível em: <<https://www.iso.org/standard/42103.html>>. Acesso em: 7 mar. 2023.
- ISO. **ISO/IEC 27001:2013**. Disponível em: <<https://www.iso.org/standard/54534.html>>. Acesso em: 7 mar. 2023.
- ITU. **Global Cybersecurity Index**. Disponível em: <<https://www.itu.int:443/en/ITU-D/Cybersecurity/Pages/global-cybersecurity-index.aspx>>. Acesso em: 3 mar. 2023.
- ITU-T. **Recommendation ITU-T X.1205: Overview of Cybersecurity**. Disponível em: <<https://www.itu.int/rec/T-REC-X.1205-200804-I>>. Acesso em: 3 mar. 2023.
- IZAGUIRRE OLMEDO, J.; LEÓN GAVILÁNEZ, F. Análisis de los Ciberataques Realizados en América Latina. **INNOVA Research Journal**, v. 3, n. 9, p. 180–189, 2 out. 2018.
- JIANG, M. **U.S. Ban on Huawei: Superpowers’ Insecurities and Nightmares**. **CyberBRICS**, 3 jun. 2019. Disponível em: <<https://cyberbrics.info/u-s-ban-on-huawei-superpowers-insecurities-and-nightmares/>>. Acesso em: 3 mar. 2023.
- KALISZ, A. **Public-Private Partnerships on Cybersecurity and International Law: Finding Multilateral Solutions**. Rochester, NY, 15 dez. 2022. Disponível em: <<https://papers.ssrn.com/abstract=4304460>>. Acesso em: 1 mar. 2023.
- KREMER, J.-F.; MÜLLER, B. (EDS.). **Cyberspace and International Relations: Theory, Prospects and Challenges**. Berlin, Heidelberg: Springer Berlin Heidelberg, 2014.
- KUEHL, DANIEL T. From Cyberspace to Cyberpower: Defining the Problem. Em: KRAMER, FRANKLIN D.; STARR, STUART H.; WENTZ, LARRY K. (Eds.). **Cyberpower and National Security**. Washington: University Of Nebraska Press, Potomac Books, 2009.
- LIAROPOULOS, A. A Human-Centric Approach to Cybersecurity. **Journal of Information Warfare**, v. 14, n. 4, p. 15–24, 2015.
- LUNDVALL, B.-Å. **Innovation System Research and Policy: Where it came from and where it might go**. Em: CAS SEMINAR. Oslo: 4 dez. 2007.
- MAZZUCATO, M. **The Entrepreneurial State**. London: Penguin, 2018.
- MAZZUCATO, M.; RYAN-COLLINS, J. 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.
- MICHEL, C. **Digital sovereignty is central to European strategic autonomy**. Em: MASTERS OF DIGITAL 2021. online: 2021. Disponível em: <<https://www.consilium.europa.eu/en/press/press-releases/2021/02/03/speech-by-president-charles-michel-at-the-digitaleurope-masters-of-digital-online-event/>>. Acesso em: 3 mar. 2023.

- MIT TECHNOLOGY REVIEW INSIGHTS. **Preparing for AI-enabled cyberattacks.** Disponível em: <<https://www.technologyreview.com/2021/04/08/1021696/preparing-for-ai-enabled-cyberattacks/>>. Acesso em: 12 jun. 2023.
- MTST. **Núcleo de Tecnologia do MTST.** Disponível em: <<https://nucleodetecnologia.com.br/>>. Acesso em: 7 jun. 2023.
- NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY. **Post-Quantum Cryptography Standardization.** Disponível em: <<https://csrc.nist.gov/projects/post-quantum-cryptography/post-quantum-cryptography-standardization>>. Acesso em: 15 fev. 2023.
- OAS; GLOBAL PARTNERS DIGITAL. **National Cybersecurity Strategies. Lessons learned and reflections from the Americas and other regions.** [s.l.: s.n.]. Disponível em: <<https://gp-digital.org/wp-content/uploads/2021/06/National-Cybersecurity-Strategies-Lessons-learned-and-reflections-ENG.pdf>>. Acesso em: 7 fev. 2023.
- PAARLBERG, R. L. Knowledge as Power: Science, Military Dominance, and U.S. Security. **International Security**, v. 29, n. 1, p. 122-151, 1 jul. 2004.
- PALMER, M. **Data is the New Oil.** Disponível em: <https://ana.blogs.com/maestros/2006/11/data_is_the_new.html>. Acesso em: 3 mar. 2023.
- PARLAMENTO EUROPEU; CONSELHO DA UE. **Regulamento (UE) 2019/881.** , 17 abr. 2019. Disponível em: <<http://data.europa.eu/eli/reg/2019/881/oj>>. Acesso em: 2 mar. 2023.
- PARSHEERA, S. Net neutrality in India: From rules to enforcement. Em: BELLI, L.; PAHWA, N.; MANZAR, O. (Eds.). **The value of internet openness in times of crisis: Official outcome of the UN IGF coalitions on net neutrality and on community connectivity.** Rio de Janeiro: FGV Direito Rio, 2020. p. 61-68.
- REDE TRANSFEMINISTA DE CUIDADOS DIGITAIS. **Sobre o site - prato do dia. Prato do dia,** [s.d.]. Disponível em: <<https://pratododia.org/pt/sobre-o-site-2/>>. Acesso em: 7 jun. 2023.
- RID, T.; BUCHANAN, B. Hacking Democracy. **SAIS Review of International Affairs**, v. 38, n. 1, p. 3-16, 2018.
- RIZZINI, I.; ARAUJO, C. DE S.; COUTO, R. M. B. DO. Crianças, adolescentes e os desafios da pandemia de Covid-19. Em: RIZZINI, I.; SILVEIRA, P. (Eds.). **Incluir para não excluir!** Porto Alegre: Editora Rede Unida, 2022. p. 763.
- ROUSSEFF, D. **Discurso da Presidenta da República, Dilma Rousseff, por ocasião do Debate Geral da 68ª Assembleia-Geral das Nações Unidas.** Disponível em: <<https://www.gov.br/mre/pt-br/centrais-de-conteudo/publicacoes/discursos-artigos-e-entrevistas/presidente-da-republica/presidente-da-republica-federativa-do-brasil-discursos/discurso-da-presidenta-da-republica-dilma-rousseff-na-abertura-do-debate-geral-da-68-assembleia-geral-das-nacoes-unidas>>. Acesso em: 3 mar. 2023.
- SCHENDES, W. **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: 7 fev. 2023.

- SECURITY REPORT. **Brasil sofreu 103,16 bilhões de tentativas de ataques cibernéticos no ano passado. Security Report**, 1 mar. 2023. Disponível em: <<https://www.securityreport.com.br/overview/brasil-sofreu-10316-bilhoes-de-tentativas-de-ataques-ciberneticos-em-2022/>>. Acesso em: 2 mar. 2023.
- SENTINELONE. **Autonomous AI Endpoint Security Platform**. Disponível em: <<https://www.sentinelone.com/>>. Acesso em: 7 jun. 2023.
- SHIRA, F.; JANCZ, C. **Barricadas, estratégias e coletividade: Uma cartilha de segurança digital para organizações**. São Paulo: MariaLab, dez. 2020. Disponível em: <<https://www.marialab.org/wp-content/uploads/2020/12/Barricas-estrategias-coletividade.pdf>>. Acesso em: 2 mar. 2023.
- SORENSEN, D. **Unicorn Hunting 2022: Top Countries & Industries for Unicorn Companies**. Disponível em: <<https://tipalti.com/unicorn-hunting-2022/>>. Acesso em: 3 mar. 2023.
- SOUZA, V. **A Era da Informação e as Relações Internacionais**. ESRI, 6 out. 2021. Disponível em: <<https://relacoesinternacionais.com.br/a-era-da-informacao-e-as-relacoes-internacionais/>>. Acesso em: 28 fev. 2023.
- STEWART, FRANCES; HUANG, CINDY; WANG, MICHAEL. Internal Wars In Developing Countries: An Empirical Overview of Economic and Social Consequences. Em: STEWART, FRANCES; FITZGERALD, VALPY (Eds.). **War and Underdevelopment: The Economic and Social Consequences of Conflict**. Oxford: Revista Oxford University, 2000. v. 1.
- TALESH, S. A.; CUNNINGHAM, B. **The Technologization of Insurance: An Empirical Analysis of Big Data and Artificial Intelligence's Impact on Cybersecurity and Privacy**. Rochester, NY, 6 maio 2021. Disponível em: <<https://papers.ssrn.com/abstract=3841045>>. Acesso em: 7 jun. 2023.
- TALESH, S.; FILHO, P. G. 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.
- TÖDTLING, F.; LEHNER, P.; TRIPPL, M. Innovation in knowledge intensive industries: The nature and geography of knowledge links. **European Planning Studies**, v. 14, n. 8, p. 1035-1058, 1 set. 2006.
- TORRIJOS RIVERA, V.; JIMÉNEZ SALCEDO, D. ¿Seguridad sin fronteras, seguridad en abstracto? Tendencias en el estudio de la ciberseguridad y la ciberdefensa. **Revista Política y Estrategia**, n. 138, p. 141-164, 2021.
- TRELLIX. **Analytical Firms and Peer Review Programs Position Trellix to Lead the XDR Market**. Disponível em: <<https://www.trellix.com/en-us/about/newsroom/stories/xdr/analytical-firms-and-peer-review-programs-position-trellix-to-lead-the-xdr-market.html>>. Acesso em: 7 jun. 2023.
- UNGA. **Progress made in the implementation of and follow-up to the outcomes of the World Summit on the Information Society at the regional and international levels**. Geneva: United Nations, 1 mar. 2018. Disponível em: <https://unctad.org/system/files/official-document/a73d66_en.pdf>. Acesso em: 1 mar. 2023.

- U.S. DEPARTMENT OF HOMELAND SECURITY. **Memorandum: Preparing for post-quantum cryptography.** , 17 set. 2021. Disponível em: <<https://www.dhs.gov/quantum>>. Acesso em: 15 fev. 2023.
- VALENTE, F.; VITAL, D. **STJ sofre ataque hacker e suspende prazos processuais até segunda (9/11).** Disponível em: <<https://www.conjur.com.br/2020-nov-04/stj-sofre-ataque-hacker-suspende-prazos-segunda-911>>. Acesso em: 7 fev. 2023.
- VAN DEN BERG, J. 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, M.; RODRIGUES, E. **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: 7 fev. 2023.
- VASCONCELLOS, H. **Justiça do RS sofre ataque hacker sem precedentes, segundo desembargador.** Disponível em: <<https://www.uol.com.br/tilt/noticias/redacao/2021/04/30/tj-rs-sofre-ataque-hacker-sem-precedentes-diz-desembargador.htm>>. Acesso em: 7 fev. 2023.
- VON DER LEYEN, U. **A Union that strives for more: My agenda for Europe.** [s.l.: s.n.]. Disponível em: <https://commission.europa.eu/system/files/2020-03/political-guidelines-next-commission_en.pdf>. Acesso em: 3 mar. 2023.
- WOLFF, J. What we talk about when we talk about cybersecurity: security in internet governance debates. **Internet Policy Review**, v. 5, n. 3, 30 set. 2016.
- YAMPOLSKIY, R. V.; SPELLCHECKER, M. S. Artificial intelligence safety and cybersecurity: A timeline of AI failures. **arXiv preprint arXiv:1610.07997**, 2016.
- ZUBOFF, S. **The Age of Surveillance Capitalism.** London: Profile Books, 2019.

Por sua própria natureza, a cibersegurança é um fenômeno multidimensional e transnacional. Ameaças cibernéticas afetam o funcionamento de processos econômicos, políticos e sociais, de modo que a regulação da cibersegurança se relacione à proteção das informações e das pessoas, bem como da soberania digital. O Brasil, em que pese a importância do tema, não evoluiu, ainda, em uma estratégia unificada adequada para solucionar o problema da cibersegurança.

Este livro representa um esforço de análise do quadro da cibersegurança no país. Uma introdução da visão sistêmica sobre a cibersegurança destaca o complexo cenário de vulnerabilidades cibernéticas e caminhos de proteção – com a significativa contribuição recente de ferramentas de inteligência artificial. O conceito de soberania digital é abordado, destacando-se a importância de estratégias educacionais multigeracionais para o efetivo exercício da autodeterminação digital, além da necessidade de uma postura que vise reduzir a dependência tecnológica nacional.

Finalmente, a partir do mapeamento e da análise crítica do arcabouço normativo vigente, com base em referências normativas, doutrinárias e de boas práticas internacionais, propõe-se um Marco de Cibersegurança e Soberania Digital para o Brasil, baseado na ampla participação social, proteção dos indivíduos, políticas públicas de incentivo e uma estrutura de governança adequada. Pretende-se, assim, prover subsídios para uma discussão frutífera a respeito dos caminhos que a política brasileira em cibersegurança tomará.

ISBN: 978-65-00-72715-9

TCR



9 786500 727159