Luca Belli, Walter B. Gaspar,
Natália Couto, Breno Pauli Medeiros,
Nicolo Zingales, Germano Johansson,
Erica Bakonyi e Filipe Medon

Soberania Digital e Inteligência Artificial no Brasil

Rumo à autonomia tecnológica

Apresentação: Ministra Luciana Santos

Prefácio: Ministra Esther Dweck

Lumen Juris Direito

Soberania Digital e Inteligência Artificial no Brasil

Lumen Juris Editora
www.lumenjuris.com.br

Filiais

Sede: Rio de Janeiro
Rua Newton Prado, n° 43
CEP: 20930-445
São Cristóvão
Rio de Janeiro – RJ
Tel. (21) 2580-7178

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

Luca Belli, Walter B. Gaspar,
Natália Couto, Breno Pauli Medeiros,
Nicolo Zingales, Germano Johansson,
Erica Bakonyi e Filipe Medon

Soberania Digital e Inteligência Artificial no Brasil

Rumo à autonomia tecnológica

Apresentação: Ministra Luciana Santos

Prefácio: Ministra Esther Dweck

Editora Lumen Juris
Rio de Janeiro
2026

Categoria: Direito Digital

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

Impresso no Brasil | *Printed in Brazil*

Dados Internacionais de Catalogação na Publicação (CIP)

S677

Soberania digital e inteligência artificial no Brasil : rumo à autonomia tecnológica / Luca Belli... [et al.] ; apresentação ministra Luciana Santos ; prefácio ministra Esther Dweck. – 1. ed. – Rio de Janeiro : Lumen Juris, 2026.
300 p. ; 23 cm.

Inclui bibliografia ao final.

ISBN 978-85-519-3956-7

1. Inteligência artificial. 2. Inovações tecnológicas. 3. Autonomia. 4. Governança corporativa. 5. Regulação. I. Belli, Luca (autor). II. Santos, Luciana (apresentador). III. Dweck, Esther (prefaciador). IV. Título.

CDD 346.0485

Ficha catalográfica elaborada por Ellen Tuzi CRB-7: 6927

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

Resumo executivo

Ao longo dos últimos anos, o assunto da soberania digital emergiu como um dos temas mais debatidos nos círculos das políticas digitais. A Soberania Digital é um conceito central no debate contemporâneo sobre a autonomia tecnológica dos Estados e o direito à autodeterminação individual e coletiva. Nas nossas pesquisas sobre soberania digital, elaboradas entre 2020 e 2025 e citadas ao longo deste estudo, definimos este conceito como "a capacidade de entender o funcionamento das tecnologias digitais, conseguir desenvolvê-las e regulá-las efetivamente, exercendo, portanto, autodeterminação, poder e controle sobre ativos digitais tais como dados, softwares, hardwares e redes eletrônicas".

Desde 2020, o projeto CyberBRICS, do Centro de Tecnologia e Sociedade da FGV Direito Rio, vem analisando as estratégias, regulações e iniciativas sobre soberania digital dos países do bloco BRICS ao longo de três fases dedicadas à cibersegurança, à transformação digital e à governança de inteligência artificial (IA) nos BRICS. Este estudo apresenta alguns dos principais achados das nossas pesquisas, que nos últimos anos alcançaram amplo destaque nacional e internacional. Neste volume, os resultados de nossas pesquisas precedentes são atualizados com base nos dados empíricos mais recentes, para estimular um debate nacional informado sobre o assunto, considerando que, como acontece com frequência quando um tema se torna popular, muitos "novos especialistas" emergem, e o debate pode acabar confuso.

Este trabalho é estruturado em cinco capítulos, que seguem a introdução e precedem a conclusão. A introdução destaca a necessidade de uma abordagem sistêmica para entender os riscos das dependências tecnológicas e enxergar as oportunidades de desenvolvimento de tecnologias digitais e, particularmente, os elementos que compõem os sistemas de inteligência artificial (IA), para conseguir manter a capacidade de escolha e de regulação sobre tais tecnologias.

O primeiro capítulo analisa e articula as dimensões conceituais e as bases constitucionais da soberania digital, frisando que esse conceito não

deve ser considerado como sinônimo de autarquia digital, mas como expressão da autonomia tecnológica consagrada no artigo 219 da Constituição Federal, bem como do direito fundamental à autodeterminação.

O segundo capítulo oferece um *framework* para analisar os elementos facilitadores essenciais da soberania em IA – dados, software e modelos de IA, capacidade computacional, conectividade significativa, recursos energéticos e minerais, capacitação humana, cibersegurança, gestão de riscos, e resiliência cognitiva –, propondo a metáfora da Pilha para ilustrar as interconexões entre as camadas que compõem tanto a estrutura técnica quanto a arquitetura de governança dos sistemas de IA.

O terceiro capítulo examina alguns dos principais riscos que podem se concretizar em uma situação de dependência tecnológica, frisando que tais riscos abrangem desde a perda de ganhos financeiros e da capacidade competitiva, até o eventual comprometimento da capacidade estatal de entender o funcionamento social, econômico e democrático e de organizar a prestação de serviços essenciais.

O quarto capítulo explora os atores, os arranjos e os instrumentos que precisam ser considerados para definir um mecanismo de governança efetivo da soberania digital, destacando a existência de elementos, não somente econômicos e tecnológicos, mas, sobretudo, institucionais e normativos subaproveitados, que deveriam ser utilizados de maneira mais efetiva para aprimorar a autonomia tecnológica do Brasil. Nesse sentido, o capítulo destaca o papel das compras públicas como instrumento central de fomento à política industrial digital do país. Destaca-se que, de maneira paradoxal, ao longo da última década, as compras públicas subsidiaram um número limitado de empresas estrangeiras, particularmente no âmbito da computação em nuvem, ao invés de ser alavancadas para apoiar o crescimento de empresas nacionais.

O quinto capítulo ilustra os caminhos e as soluções que poderiam ser adotados para reorganizar a governança da soberania digital no país, oferecendo propostas de arranjos institucionais e políticas públicas que podem ser adotadas no curto, médio e longo prazo. O capítulo ressalta a importância de se articular a cooperação multissetorial por meio de um Conselho, delegando a coordenação operacional a uma Secretaria, estabelecendo um Fundo dedicado ao suporte financeiro e alavancando a diplomacia brasileira para alcançar *situational awareness*, identificando,

interpretando e reagindo a riscos e oportunidades inerentes às evoluções tecnológicas. Sublinha, outrossim, a urgência de se definirem padrões rigorosos de segurança da informação, auditabilidade e interoperabilidade, bem como de se otimizar o aproveitamento dos marcos normativos e das instituições já existentes.

Por fim, a conclusão elabora algumas considerações finais, enfatizando que a soberania digital deve ser considerada como projeto de Estado, essencial para o desenvolvimento nacional e para a promoção da cooperação internacional com base em regras compartilhadas, arquiteturas tecnológicas abertas e interoperáveis, e relações multissetoriais e multilaterais cooperativas.

Agradecimentos

Os autores deste livro expressam sua profunda gratidão pelos valiosos feedbacks recebidos ao longo do segundo semestre de 2025. Diversas versões deste trabalho foram apresentadas e debatidas em encontros enriquecedores que contribuíram significativamente para o aprimoramento do conteúdo.

Gostaríamos de agradecer especialmente à Ministra da Gestão e Inovação nos Serviços Públicos, Esther Dweck, pelo diálogo colaborativo, pelo prefácio, pela abertura ao debate e pelas discussões altamente construtivas, junto com sua equipe, à qual foi apresentada uma versão embrionária deste trabalho no início de setembro 2025.

Manifestamos nossa imensa gratidão à Ministra da Ciência, Tecnologia e Inovação, Luciana Santos, pela excelente apresentação, e Henrique Miguel, Secretário de Ciência e Tecnologia para Transformação Digital, do Ministério da Ciência, Tecnologia e Inovação (MCTI), à Renata Mielli, assessora especial da Ministra Luciana Santos, e a André Rafael, coordenador de Políticas de Ciência, Tecnologia e Inovação Digital no MCTI, por compartilharem seus conhecimentos em várias ocasiões, especialmente durante o Seminário "Pilha de IA: Desafios para Autonomia Tecnológica e Soberania Digital".

Também agradecemos à Secretária Cristiane Rauen, diretora do Departamento de Transformação Digital e Inovação do Ministério de Desenvolvimento, Indústria e Comércio, por ter proporcionado valiosas conversas, particularmente no âmbito da Câmara Técnica de Economia Digital do Comitê Interministerial sobre Transformação Digital (CITDigital).

Agradecemos ainda à Beatriz Vasconcelos, secretária adjunta de transformação digital da Casa Civil e a Eugenio Garcia, Embaixador Extraordinário para a Tecnologia e Inovação, pelas reuniões proveitosas e, especialmente, pelas ricas oportunidades de trocas de experiências, debates e análises que enriqueceram nosso diálogo.

Nosso reconhecimento vai também ao Professor Caetano Penna, à Carolina Pereira e à Isabela Quadros, do Centro de Gestão e Estudos Estratégicos, por seu engajamento e por compartilhar seus insights e suas

perspectivas valiosas, que nos permitiram ampliar e aprofundar nossa reflexão. Tais reflexões foram destiladas pelo autor principal deste volume, para elaborar o trabalho "Soberania digital no Brasil: diagnóstico, desafios e caminhos sob a perspectiva da ciência, tecnologia e inovação", com base nas nossas pesquisas analisadas neste volume.

Manifestamos gratidão à Ministra Carolina Hippolito Von Der Weid, do Ministério das Relações Exteriores do Brasil, e a James Görgen, Especialista em Políticas Públicas e Gestão Governamental no Ministério do Desenvolvimento, Indústria, Comércio e Serviços, por ter proporcionado uma ocasião única para compartilhar e debater nossas pesquisas sobre soberania de dados no âmbito do primeiro evento do BRICS sobre governança de dados na economia digital, para subsidiar a elaboração do Entendimento sobre governança da economia de dados do BRICS, adotado durante a cúpula do BRICS de 2026.

Gostaríamos de agradecer também ao Secretário de Políticas Digitais da Secretaria de Comunicação Social da Presidência da República, João Brant, e à Professora Marília Bassetti Marcato, Assessora da Presidência do Banco Nacional de Desenvolvimento Econômico e Social (BNDES), por terem proporcionado a oportunidade de apresentar e debater nossas pesquisas no seminário "*Governance and Public Strategy in AI*" organizado pelo BNDES como pré-evento da Cúpula do BRICS 2025. Agradecemos também os membros do Conselho Consultivo do Comitê Interministerial sobre Transformação Digital (CITDigital) e do Comitê Nacional sobre Cibersegurança (CNCiber), com os quais travamos conversas estimulantes e essenciais, fundamentais para o desenvolvimento deste trabalho.

Finalmente, agradecemos à Fundação Getulio Vargas pelo apoio institucional, assim como às Fundações Ford e Open Society pelo financiamento de várias das pesquisas que possibilitaram o desenvolvimento desta obra, em especial o projeto CyberBRICS.

A todos e todas, nosso sincero muito obrigado.

Apresentação

O livro *Soberania digital e inteligência artificial no Brasil: rumo à autonomia tecnológica* coroa um trabalho de pesquisa e sistematização sobre um tema estratégico para o desenvolvimento científico, tecnológico e econômico do Brasil pautado numa perspectiva de promoção e proteção dos interesses nacionais com foco na inclusão, redução de desigualdades e fortalecimento do país no contexto geopolítico. Este trabalho é lançado em um momento no qual o Brasil procura traduzir em ações concretas o objetivo de deixar de ser um país consumidor de soluções importadas para se tornar produtor de tecnologias alinhadas às necessidades nacionais. Entre as muitas políticas públicas que materializam esse objetivo, cito o Plano Brasileiro de Inteligência Artificial (PBIA) que de forma arrojada estabelece em torno de 5 eixos um conjunto de ações ambiciosas que somam 23 bilhões de reais em investimentos até 2028.

A pesquisa coordenada pelo Professor Luca Belli, do Centro de Tecnologia e Sociedade da Escola de Direito da Fundação Getulio Vargas, no Rio de Janeiro, nos oferece uma visão conceitual aprofundada para o debate sobre soberania digital e traz um mapa de experiências que têm sido desenvolvidas em outros países. Além de grande valor acadêmico, é também uma referência para os que estão, como nós, a cargo da elaboração das políticas públicas, ao nos oferecer análises e cenários que precisam ser considerados para que essas sejam bem-sucedidas.

Temos acompanhado, nos muitos fóruns nacionais e internacionais dos quais participamos, como a discussão sobre soberania digital têm ocupado espaço central nos debates. E, vale registrar, não necessariamente convergente. Aqui, quero destacar uma contribuição científica fundamental deste livro: oferecer não apenas uma definição de soberania digital, mas explorar ao longo dos capítulos suas dimensões, contribuindo para que o termo não seja capturado de forma equivocada. Os autores deixam claro que soberania digital nada tem a ver com isolamento tecnológico, com rechaço à cooperação internacional, com o fechamento de fronteiras e ausência de diálogo. Para os autores, e esta é também a nossa visão, a

soberania digital está relacionada à "capacidade de entender, desenvolver e regular tecnologias digitais, exercendo autodeterminação sobre dados, softwares, hardwares e redes".

Resgatam, oportunamente, que desenvolver políticas voltadas à autonomia tecnológica do país é, inclusive, diretriz constitucional de desenvolvimento nacional – consagrada no artigo 219 da Constituição Federal. Os autores mostram que buscar a soberania digital e em Inteligência Artificial passa por ter uma política voltada à soberania de dados, pelo desenvolvimento da nossa capacidade computacional, por políticas industriais, de ciência e tecnologia e cibersegurança, pela conectividade significativa, formação e retenção de talentos, e marcos regulatórios robustos. Articulando essas dimensões em torno da estruturação do que o livro chama de "pilha" de soberania em IA, os pesquisadores adotam uma abordagem sistêmica para a compreensão dos desafios, riscos e oportunidades para a construção da soberania digital e de IA no Brasil.

Essa abordagem sistêmica, que é um dos pontos altos do livro, dialoga diretamente com o nosso Plano Brasileiro de Inteligência Artificial. O PBIA foi um trabalho coordenado pelo Ministério da Ciência, Tecnologia e Inovação que envolveu dezenas de órgãos públicos entre ministérios, agências, unidades de pesquisa, sociedade civil, setor privado, comunidade acadêmica e foi lançado durante a 10ª Conferência Nacional de Ciência, Tecnologia e Inovação, em julho de 2024.

Organizado em torno de cinco eixos – infraestrutura, formação, uso em serviços públicos, inovação empresarial e apoio regulatório –, o PBIA apresenta uma agenda brasileira para dar um passo consistente na estruturação dessa pilha de soberania em IA, prevendo investimentos estruturantes em centros de pesquisa, redes de computação de alto desempenho, laboratórios de teste, programas de difusão tecnológica, formação, adoção de IA pelo Estado e mecanismos de apoio a empresas.

Num contexto geopolítico marcado pela concentração econômica em torno de um pequeno punhado de corporações de tecnologia que dominam a cadeia global do digital, o Plano Brasileiro de IA assume o objetivo de fomentar a produção nacional de tecnologias e de orientar o uso de IA para o bem-estar social, propor ações que visam reduzir gargalos nas cadeias produtivas, estimular a pesquisa aplicada em setores estratégicos e apoiar empresas inovadoras, especialmente aquelas comprometidas com

soluções aderentes às necessidades do país. Ao mesmo tempo, ao inserir a IA como instrumento para melhoria dos serviços públicos, o Plano reconhece que a demanda estatal pode ser alavanca decisiva para consolidar um mercado interno dinâmico e menos dependente de soluções proprietárias externas.

Dedicado à infraestrutura e ao desenvolvimento de IA, o eixo 1 do PBIA prevê a criação de um supercomputador nacional e de uma "nuvem soberana" de dados públicos, passos concretos para reduzir a dependência de provedores estrangeiros. Ao discutir a dependência de plataformas e infraestruturas globais, os autores oferecem o contraponto teórico e empírico para o eixo 1 do PBIA: investimentos massivos em computação de alto desempenho só produzirão autonomia se articulados a políticas de dados, software de base, energia e conectividade que fortaleçam o que os autores denominam de Facilitadores Essenciais da Soberania em Inteligência Artificial (FESIA).

O PBIA também prevê o desenvolvimento de uma pilha nacional de software para IA, interoperável com ecossistemas abertos, e o fomento a modelos fundacionais treinados com dados brasileiros, em especial grandes modelos de linguagem em português. O livro ajuda a entender por que isso importa: ele recupera o debate sobre código aberto como estratégia de soberania, mostrando como experiências bem-sucedidas trataram *open source* não apenas como algo a ser usado, mas como objeto de política industrial, construindo ecossistemas produtivos em torno de infraestruturas abertas. Ao situar a discussão brasileira nesse contexto, a obra oferece critérios para que as ações do PBIA consolidem capacidades próprias em dados, modelos e ferramentas críticas de IA.

Nessa perspectiva, é importante destacar a relevância de os autores trazerem uma análise da estratégia e experiência chinesa. Ao examinar o uso estratégico de *open source* em sistemas operacionais (como o Kylin), arquiteturas abertas de hardware (como RISC-V) e sua articulação com planos quinquenais, os autores mostram como a China combinou política industrial, financiamento público e regulação para transformar tecnologias abertas em alavanca de autonomia tecnológica. O capítulo sobre soberania de dados reforça essa leitura, destacando políticas de controle sobre fluxos de informação, construção de nuvens domésticas e uso de dados como insumo central para a soberania em IA.

Outro ponto de forte convergência entre o livro e o PBIA está nas políticas para formação, retenção e repatriação de talentos previstas no eixo 2. Com ações voltadas à difusão, formação e capacitação em IA, com programas de educação digital, pesquisa e P&D multidisciplinar. O livro acrescenta uma camada crítica: não basta formar; é preciso que o sistema produtivo e o Estado consigam absorver essa mão de obra, oferecendo trajetórias de carreira, previsibilidade e oportunidades reais de empreender em tecnologias intensivas em conhecimento. Nesse contexto, o Programa Conhecimento Brasil aparece como peça-chave da agenda recente de soberania em IA.

Por fim, o livro *Soberania digital e inteligência artificial no Brasil* alerta para um ponto que também é objeto das nossas preocupações: a necessidade de tratar a autonomia tecnológica como projeto de Estado, e não como iniciativa episódica de governo. Lido em conjunto com o Plano Brasileiro de Inteligência Artificial, o volume *Soberania Digital e Inteligência Artificial no Brasil* oferece um roteiro consistente para que o país deixe de ser apenas mercado consumidor de soluções alheias e se afirme como desenvolvedor de tecnologias críticas, capaz de projetar seus próprios valores na arquitetura digital que organiza sua economia, sua esfera pública e sua democracia.

Luciana Santos
Ministra de Ciência, Tecnologia e Inovação

Prefácio

Este livro oferece uma visão abrangente, realista e inspiradora sobre os caminhos que a democracia brasileira pode e deve percorrer para assegurar o controle sobre o próprio destino a partir dos ativos e das tecnologias digitais. Almejar soberania em um Estado e em uma sociedade como a brasileira, em uma economia global marcada pela plataformização que extrai valor produzido em rede para um conjunto de empresas de tecnologia oriundas sobretudo dos EUA e, de forma ainda secundária, da China, implica perseguir, necessariamente, soberania no âmbito *digital*. Qualquer proposta de desenvolvimento e autonomia para o Brasil que não reconheça – e atue – sobre a centralidade e os desafios das tecnologias digitais tende a fracassar sob o peso de seu anacronismo.

O livro é fundamentado em análises empíricas de várias experiências internacionais, além da brasileira, e dá destaque à singularidade da experiência chinesa que, não obstante compartilhar com o Brasil a condição de país em desenvolvimento impactado por séculos de práticas colonialistas e imperialistas, constitui hoje o país que mais longe chegou no alcance da soberania digital para sua sociedade e economia. Não por coincidência, é o mesmo país que hoje rivaliza com os EUA em prosperidade econômica e desenvolvimento.

Nessa competente contribuição teórica e prática, os autores investigam a atuação de outros países, analisando, com isenção, o que funcionou e o que não funcionou, como base para suas prescrições de política pública para o Brasil. A partir de uma bem-vinda perspectiva desenvolvimentista e democrática, não se deixam seduzir pelo tecno-otimismo propagandeado pelas grandes empresas fornecedoras de tecnologia globais e são pragmáticos no reconhecimento da inexorabilidade do impacto da economia digital.

Diante de um contexto geopolítico crescentemente instável e conflituoso, o livro reconhece tanto a premência da transformação digital quanto os riscos a ela associados. Os autores reforçam a prioridade à cibersegurança e às ações destinadas a reduzir a dependência do país em relação a empresas e atores externos.

A abordagem equilibrada dos autores aparece na formulação do conceito de soberania digital e suas dimensões (capítulo 1), bem como na descrição das camadas necessárias à soberania em IA e suas interconexões (capítulo 2) e dos riscos da falta de soberania digital (capítulo 3). A governança ainda fragmentada da soberania digital no país também é objeto de análise (capítulo 4). As propostas de aperfeiçoamento dessa governança, de políticas de incentivo econômico e de regulação para o Brasil (capítulo 5) iluminam caminhos futuros, para além dos avanços que já empreendemos sob a gestão iniciada em 2023 do Presidente Lula.

Ao longo do livro, o estudo das experiências dos países do BRICS vai ao encontro da estratégia brasileira de cooperação Sul-Sul como eixo para o fortalecimento da soberania, a partir de aprendizado não só com o caso peculiar chinês, mas também da necessidade de intensificar esse intercâmbio com a Índia. O Brasil tem aprofundado colaborações com este país a partir de projetos envolvendo infraestruturas públicas digitais.

Trata-se de visão coerente com o que procuramos implementar à frente do Ministério da Gestão e Inovação em Serviços Públicos (MGI), criado em 2023, no âmbito do governo federal sob a liderança do Presidente Lula.

Em minha função à frente do MGI, tive o privilégio de receber em mais de uma ocasião o Prof. Luca Belli, um dos autores deste livro, para debatermos acerca das questões refletidas neste livro, o que contribuiu para qualificar nossa ação no governo. Entre as medidas que adotamos no MGI está a Nuvem de Governo, modelo padronizado e obrigatório para a contratação de serviços de computação em nuvem por órgãos do Executivo Federal, em parceria entre o MGI, Serpro e Dataprev – empresas estatais federais de tecnologia. A Nuvem de Governo, em linha com o gradualismo pragmático de *frameworks* como o da União Europeia (*Cloud Sovereignty Framework* – CSF), descrito neste livro, ainda não garante a almejada autonomia tecnológica plena, mas representa um avanço ao exigir que os dados sejam armazenados em território nacional sob algum nível de controle público e regras para mitigação de riscos.

Destaco também a ideia, trazida pelo livro, de que as experiências mais exitosas em soberania de dados, como a chinesa, são marcadas pela sinergia entre a possibilidade de sanções inerente à regulação e os incentivos típicos das ferramentas de indução econômica. No caso brasileiro, adotamos o Plano Brasileiro de Inteligência Artificial, também referida no

livro, da qual participa o MGI com projetos estratégicos em Inteligência Artificial para alavancar políticas públicas e bases de dados. Entre os projetos em implementação, estão o núcleo de tecnologias em cibersegurança no contexto de IA, voltado a garantir a privacidade e a segurança dos dados e aplicações envolvendo IA, bem como uso de IA para personalizar a comunicação de governo com o cidadão e melhorar a orientação sobre direitos e acesso a políticas.

Temos consciência do quanto é preciso não só ampliar ações voltadas à soberania digital, mas, sobretudo, conferir maior centralidade estratégica ao tema. Iniciativas como a deste livro aguçam nossa criatividade e nos animam a ampliar as inovações que nos ajudarão a construir uma democracia mais sólida e mais autônoma.

Conforme destacam os autores, o sucesso da agenda de soberania digital depende, além da formulação de uma estratégia comum para todos os governos, de uma governança adequada que garanta coerência a longo prazo. Atuar sobre os ativos e interesses críticos e transformá-los ao longo do tempo exige continuidade de esforços e capacidade de coordenação nacional. Acrescento que, em uma democracia como a brasileira, essa continuidade só será alcançada com a construção de um pacto nacional amplo e suprapartidário em torno da soberania digital, a partir de um diálogo que demonstre inclusive para o setor produtivo nacional os riscos e custos dessa dependência. É essa a missão de alto nível, a ser travada nos próximos ciclos políticos do país, a que os autores nos inspiram.

Devemos avançar ainda mais em reformas no âmbito da governança estatal no Brasil para ampliar as condições institucionais para atuação em prol da soberania digital. É preciso coordenar de forma mais intensa os diversos órgãos do Estado brasileiro responsáveis por regulações setoriais, tributação, incentivo à pesquisa e desenvolvimento, políticas industriais e compras públicas.

Carregamos o desafio, no Brasil, de avançar na digitalização e qualificação dos serviços públicos e privados, ao mesmo tempo em que criamos as condições para um ecossistema digital autônomo e resiliente em face de ameaças externas, que infelizmente tendem a ficar cada vez mais comuns em nosso contexto geopolítico. Este livro é, portanto, de leitura essencial na atual conjuntura.

Gestores públicos, pesquisadores, usuários de serviços públicos, funcionários de empresas de tecnologia nos setores público e privado, jornalistas, políticos, além de cidadãos em geral interessados e vocacionados à defesa da soberania digital do país encontrarão aqui, além da pesquisa acadêmica séria e consistente feita pelos autores, um convite à construção coletiva. A missão da soberania digital é de longo prazo. Não cabe em um só mandato eletivo nem compete apenas aos poderes constituídos. É tarefa de toda a sociedade brasileira: movimentos sociais, empresas, universidades, instituições de pesquisa, organizações não governamentais e quem mais se interessar. Boa leitura!

Esther Dweck
Ministra da Gestão e Inovação em Serviços Públicos

Sobre os Autores

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

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

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

Erica Bakonyi é doutoranda em Direito da Regulação, na FGV Direito Rio; mestre em Direito pela Universidade de Coimbra; possui MBA em Gestão da Segurança da Informação (Infnet) e especialização em Licitações e Contratos Administrativos (Uniseb); membro do Conselho Municipal de Proteção de Dados Pessoais e da Privacidade (CMPDPP) da cidade do Rio de Janeiro; pesquisadora no CTS-FGV, no projeto CyberBRICS. Advogada e consultora na área de Proteção de Dados, foi *Visiting Fellow* na ANU Australian College of Law 2025.

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

Nicolo Zingales é advogado e professor em Direito da Regulação da FGV Direito Rio, onde coordena o Núcleo de Estudos em e-commerce e os projetos de governança de plataformas. Consultor PNUD e assessor não governamental do Conselho Administrativo de Defesa Econômica (CADE) junto à International Competition Network. Diretor da conferência *Computers Privacy and Data Protection in Latin America* (CPDP LatAm) e do *BRICS + Digital Competition Forum*. Pesquisador adjunto na Universidade de Tilburg e no Centre for Internet & Society de Stanford Law School. Mestre em Direito pela Università degli Studi di Bologna e doutor em Direito e Economia pela Universitá Bocconi.

Germano Johansson é doutorando em Ciência Política pela Universidade de Brasília, mestre em Engenharia (MSc) e em Planejamento (MPL) pela University of Southern California, especialista em Políticas de Infraestrutura pela Escola Nacional de Administração Pública e engenheiro pela Universidade Federal do Paraná; é servidor público federal com experiência na área de infraestrutura e no Congresso Nacional; pesquisador

do projeto CyberBRICS do CTS-FGV. Sua pesquisa inclui o mapeamento de riscos e oportunidades para a soberania digital brasileira, estudando infraestruturas digitais públicas e privadas e examinando dependências tecnológicas no contexto digital.

Filipe Medon é doutor e mestre em Direito Civil pela Universidade do Estado do Rio de Janeiro (UERJ). Professor de Direito Civil na FGV Direito Rio, onde também é pesquisador no CTS-FGV e Coordenador Adjunto do AI Hub da FGV Direito Rio. Professor convidado de cursos de pós-graduação e extensão de diversas instituições no Brasil e fora. Membro do European Law Institute, da Comissão de Proteção de Dados e Privacidade da OAB/RJ, tendo integrado, ainda, a Comissão de Juristas do Senado Federal responsável pela criação do Marco Legal da IA e do Grupo de Trabalho sobre *deepfakes* da Presidência da República do Brasil. Seus trabalhos foram citados mais de trezentas vezes por inúmeros meios de comunicação internacionais, incluindo a TIME Magazine e The Washington Post. Advogado, consultor e parecerista.

Sumário

Introdução

Ao longo dos últimos anos, o assunto da soberania digital emergiu como um dos temas mais debatidos nos círculos das políticas digitais. Desde 2020, o projeto CyberBRICS[1], do Centro de Tecnologia e Sociedade da FGV Direito Rio[2], vem analisando as estratégias, regulações e iniciativas sobre soberania digital dos países do bloco BRICS ao longo de três fases dedicadas à cibersegurança,[3] transformação digital[4] e governança de IA no BRICS.[5]

A pesquisa elaborada no âmbito do projeto CyberBRICS oferece percepções valiosas para os debates brasileiros sobre soberania digital, por três razões diferentes. Primeiramente, é uma das únicas pesquisas que existem no mundo que analisa quais estratégias, políticas industriais e regulações foram adotadas por um grupo de países em desenvolvimento e que se transformaram em lideranças tecnológicas globais ao longo das últimas décadas.

Nesse sentido, apesar de estarmos cientes das peculiaridades dos sistemas políticos de alguns países do bloco BRICS e das legítimas críticas que podem surgir sobre tais sistemas, parece-nos particularmente valioso analisar e tentar entender como países em desenvolvimento conseguiram aprimorar sua soberania digital, em vez de tentarem copiar "soluções" propostas, com resultados muito questionáveis, de países europeus, cujo nível de auto-

1 Este trabalho baseia-se nas pesquisas elaboradas no âmbito do Projeto CyberBRICS desde seu estabelecimento, em 2018. Todas as pesquisas estão disponíveis em acesso livre no site do projeto www.cyberbrics.info.

2 CTS-FGV, **Centro de Tecnologia e Sociedade**, Centro de Tecnologia e Sociedade. Disponível em: <https://direitorio.fgv.br/pesquisa/centro-de-tecnologia-e-sociedade>. Acesso em: 20 out. 2025.

3 BELLI, Luca (Org.). **CyberBRICS: Cybersecurity Regulations in the BRICS Countries**, Cham: Springer International Publishing, 2021.
BELLI, Luca et al. **Governança e regulação da cibersegurança no Brasil**: Proteção da infraestrutura crítica, segurança da informação e construção da soberania digital. Rio de Janeiro, RJ: Editora Lumen Juris, 2025.

4 BELLI, Luca; MAGALHÃES, Larissa, Computer Law & Security Review, **Digital Transformation in the BRICS Countries**, v. 54.

5 BELLI, Luca, BRICS countries and AI sovereignty: Introduction to Thematic Section. **The African Journal of Information and Communication (AJIC)**, n. 34, p. 1-6, 2024.

nomia tecnológica continua sendo extremamente limitado, apesar de amplo desenvolvimento econômico e maturidade institucional de tais países.[6]

Em segundo lugar, como será evidente para o leitor deste trabalho, nossa pesquisa baseia-se numa abordagem sistêmica, evitando se concentrar somente em um setor regulado ou dimensão única (por exemplo, regulação de dados pessoais, acesso à Internet, cibersegurança etc.), mas adotando a visão multidisciplinar e multicamada, que será proposta no primeiro capítulo deste trabalho. Assim, nossa pesquisa demonstra que tal abordagem se torna necessária para analisar e conectar as diferentes dimensões e elementos indissociáveis de um sistema digital (incluindo sistemas de IA) e identificar as interconexões entre tais elementos. Entendemos perfeitamente a dificuldade de se adotar tal abordagem sistêmica, especialmente devido à enorme setorialização e consequente compartimentação da regulação, das políticas públicas e do próprio ensino sobre o funcionamento das tecnologias digitais que compõem sistemas de IA.

No entanto, parece-nos essencial ter uma abordagem sistêmica não somente para compreender o funcionamento, mas também para conseguir regular efetivamente sistemas de IA e/ou sistemas digitais. Nessa perspectiva, nossa pesquisa almeja analisar as diferentes estratégias regulatórias que podem ser usadas para regular o desenvolvimento e o uso de tecnologias digitais e sistemas de IA para além da lei. As últimas três décadas de estudos sobre direito e tecnologia demonstraram que, para se regular tecnologias de maneira efetiva, não podem ser desconsideradas as outras "modalidades de regulação" que alavancam ferramentas econômicas para

6 O nível extremamente elevado de dependência tecnológica da UE e as consequentes vulnerabilidades são analisadas de maneira eloquente no relatório do ex-Presidente do Banco Central Europeu, Mario Draghi. EUROPEAN COMMISSION (Org.). **The future of European competitiveness: Part A: a competitiveness strategy for Europe**, Luxembourg: Publications Office, 2025 O fracasso da UE na construção de soberania digital na última década e, especialmente, desde a primeira administração Trump, foi amplamente debatido ao longo da conferência "Towards European Digital Independence: Building the Eurostack", organizada no próprio Parlamento Europeu, ao longo da qual um dos coautores desse trabalho apresentou alguns casos de estudo com base nas experiências dos países do bloco BRICS. https://digitalindependenceeu.wordpress.com/agenda/. Cabe ressaltar que a dependência tecnológica europeia foi instaurada apesar dos países membros da EU disporem de capacidades intelectuais, financeiras, tecnológicas e institucionais extremamente elevadas. Assim, parece evidente que a experiência europeia precisa ser estudada principalmente como exemplo de fracasso em termos de soberania digital, como evidenciado por vários relatórios elaborados pelos participantes da conferência https://eurostack.eu/.

regular comportamentos de pessoas físicas e jurídicas por meio de investimentos, subsídios e tributação; a própria estrutura dos hardwares e softwares que compõem sistemas digitais, que regulam por meio da "arquitetura" e do "poder estrutural" da tecnologia digital; ou ainda por meio de hábitos que podem ser criados artificialmente para definir os comportamentos dos usuários de tecnologias.[7]

Ao moldar como os usuários (sejam pessoas físicas ou jurídicas) podem interagir entre si, como podem fazer negócios, se comunicar e relacionar, a tecnologia pode exercer um enorme poder estrutural que regula de maneira particularmente dominante as atividades de seus usuários e, consequentemente, o funcionamento das sociedades e economias onde tal tecnologia é utilizada. O poder estrutural dos provedores de aplicativos consta na definição das plataformas, ou seja, "as estruturas técnicas e de governança que facilitam o relacionamento e a troca de valor entre diferentes categorias de usuários".[8]

Cabe destacar que o entendimento da existência de diferentes modalidades de regulação não implica a obsolescência do direito, mas, ao contrário, a necessidade de se alavancar o direito para direcionar os outros vetores regulatórios a alcançar os objetivos prepostos. Assim, o direito pode – e, na perspectiva de quem escreve, deve – atuar como agente de promoção e facilitação da autonomia tecnológica por meio do desenvolvimento.

---

7 Tais dimensões são estudadas no âmbito do direito e tecnologia há mais de vinte cinco anos e pelos cientistas políticos há quase quarenta anos. A cientista política britânica Susan Strange argumenta que as entidades soberanas exercem o poder não apenas pela capacidade de compelir alguém a fazer algo e por meio de manifestações "clássicas" de poder – ou seja, pela criação de regimes que regulam as sociedades –, mas também pelo poder de moldar as estruturas que definem como as demais atividades podem acontecer – ou seja, definindo as estruturas dentro das quais pessoas, corporações e até Estados se relacionam. Apesar do trabalho de Strange considerar as estruturas administrativas do Estado e comerciais do mercado, é importante ressaltar que as considerações da politóloga são extremamente úteis para entender o papel regulatório da tecnologia em geral e dos aplicativos em particular. Ver STRANGE, Susan, **States and markets**. 1. ed. London: Continuum, 1988; BELLI, Luca *et al*, Structural Power as a Critical Element of Digital Platforms Private Sovereignty. In: **Constitutionalising Social Media**. London: Hart, 2022. Sobre as diferentes modalidades de regulação das tecnologias digitais, ver LESSIG, Lawrence, The law of the horse: What cyber law might teach, **Harv. L. Rev.**, v. 113, p. 501, 1999; LESSIG, Lawrence, **Code: And Other Laws of Cyberspace**. Sydney: ReadHowYouWant.com, 2009. BELLI, Luca. **De la gouvernance à la régulation de l'internet**. Paris: Berger Levrault, 2015.

8 BELLI, Luca. **Glossary of Platform Law and Policy Terms**. Rio de Janeiro, RJ: Publicações Direito Rio, 2021.

Ao definir subsídios, isenções fiscais, linhas de crédito ou políticas de fomento à pesquisa e inovação, o Estado utiliza a função promocional para induzir comportamentos inovadores e colaborativos entre empresas, universidades e centros de pesquisa. Adotando uma abordagem funcionalista do direito[9], a regulação deixa de ter caráter meramente coercitivo para assumir papel direcional, guiando a sociedade rumo à soberania tecnológica e à redução da dependência externa: o direito torna-se um instrumento estratégico de transformação social, econômica e tecnológica, atuando de forma ativa na construção da soberania digital.

Nesse contexto, a soberania digital se torna um conceito central no debate contemporâneo sobre a autonomia tecnológica e a capacidade regulatória dos Estados, bem como sobre o pleno gozo do direito à autodeterminação de forma individual ou coletiva. A soberania digital deve ser compreendida como "a capacidade de entender o funcionamento das tecnologias digitais, conseguir desenvolvê-las e regulá-las efetivamente, exercendo, portanto, autodeterminação, poder e controle sobre ativos digitais tais como dados, softwares, hardwares e redes eletrônicas".[10]

---

9 A teoria funcionalista do direito destaca a importância da regulação como instrumento de facilitação além de sanção. Formulada por Norberto Bobbio, esta abordagem entende o ordenamento jurídico como um sistema dinâmico voltado não apenas à repressão de condutas indesejadas, mas também à promoção de comportamentos socialmente úteis. Para Bobbio, o direito cumpre múltiplas funções – repressiva, protetiva e promocional –, sendo esta última responsável por estimular ações que contribuam para o alcance de fins coletivos desejáveis, por meio de instrumentos como incentivos, benefícios ou estímulos econômicos. BOBBIO, Norberto. **Dalla struttura alla funzione: nuovi studi di teoria del diritto**, Milano: Edizioni di Comunità, 1976. Da Estrutura A Funcao: Novos Estudos de Teoria do Direito - Bobbio Norberto - Touché Livros.

10 BELLI, Luca. **Da soberania digital à soberania em IA**. JOTA Jornalismo. Disponível em: <https://www.jota.info/opiniao-e-analise/colunas/ia-regulacao-democracia/da-soberania-digital-a-soberania-em-ia>. Acesso em: 11 mar. 2025; BELLI, Luca. Cibersegurança: uma visão sistêmica rumo a uma Proposta de Marco Regulatório para um Brasil Digitalmente soberano. BELLI, Luca. Exploring the Key AI Sovereignty Enablers (KASE) of Brazil, towards an AI Sovereignty Stack. **SSRN Electronic Journal**, 2023. BELLI, Luca. Soberania em Inteligência Artificial: O que é e quais facilitadores essenciais podem tornar o Brasil um país soberano em IA? (Sovereignty in Artificial Intelligence: What Is It and What Key Enablers Can Make Brazil a Sovereign Country in AI?), 2024. JIANG, Min; BELLI, Luca. Digital Sovereignty in the BRICS Countries, 2024. JIANG, Min; BELLI, Luca (Orgs.). **Digital Sovereignty in the BRICS Countries: How the Global South and Emerging Power Alliances Are Reshaping Digital Governance**, 1. ed. [s.l.]: Cambridge University Press, 2025.

A partir dessa definição, podemos estruturar três pilares fundamentais: i) a capacidade de entender riscos; ii) a capacidade de entender oportunidades; e iii) a capacidade de escolha para mitigar riscos e aproveitar oportunidades e, se for necessário, reverter sua escolha. Esses pilares asseguram que países, entidades e até pessoas possam entender, desenvolver, gerir e proteger suas infraestruturas digitais de forma independente, evitando vulnerabilidades decorrentes da dependência excessiva de atores estrangeiros.[11]

Com base nesses pilares, Belli destaca três dimensões para a efetivação da soberania digital: pesquisa, desenvolvimento[12] e regulação[13]. Tais dimensões são intimamente conectadas e, como destacaremos nos Capítulos 4 e 5 deste trabalho, precisam ser articuladas por meio de mecanismos de governança multissetorial voltados ao estabelecimento de uma sinergia entre objetivos públicos, fomento de tais objetivos, pesquisa sobre como alcançar tais objetivos por meio de inovação, desenvolvimento de soluções e a consequente transformação de tais soluções em produtos e serviços escaláveis, e fiscalização da regulação setorial.

Nomeadamente, a incorporação da preocupação com a soberania digital, como critério estruturante da nossa análise, exerce uma função tripla e complementar. Primeiramente, ao estimular a análise pormenorizada do funcionamento das tecnologias digitais, atua como mecanismo de reforço do controle jurisdicional, operacional e individual sobre os ativos digitais. Em segundo lugar, ao estimular o desenvolvimento de tais tecnologias funciona como instrumento de estímulo à capacidade produtiva doméstica, inclusive direcionando demanda pública para soluções tecnológicas ciberseguras desenvolvidas e escaladas no país. Em terceiro lugar, a exigência de comprovada observância da legislação vigente, torna o compliance regulatório um critério de qualidade para o consumidor e, ao mes-

11 JIANG; BELLI. Digital Sovereignty in the BRICS Countries.

12 Cabe ressaltar que pesquisa e desenvolvimento, apesar de conceitos distintos, são frequentemente tratados em conjunto – P&D –, sendo a pesquisa voltada para a expansão das fronteiras do conhecimento ou seu aprofundamento e o desenvolvimento, para a realização de etapas iniciais ou avançadas no processo de criação de novos produtos, serviços etc. Assim, devem ser enxertadas como parte de um mesmo processo contínuo, iterativo, complexo, desenvolvido de forma sistêmica, de inovação, que possa, por meio de várias etapas, levar à introdução de novos produtos e serviços no mercado ou para o proveito da sociedade.

13 BELLI, Luca. Exploring the Key AI Sovereignty Enablers (KASE) of Brazil, towards an AI Sovereignty Stack.

mo tempo, impõe ao Estado o dever de contratar exclusivamente soluções seguras, abertas e conformes com a legislação em vigor, contribuindo para o estímulo de um ecossistema digital tecnologicamente autônomo.

Este trabalho apresenta alguns dos principais achados das nossas pesquisas, para estimular um debate informado sobre o assunto. Os autores deste estudo acreditam que não somente um debate informado sobre este assunto tão relevante seja essencial para o Brasil, mas que uma estratégia clara precise ser definida e implementada com urgência para garantir o próprio funcionamento constitucional do país.

1 As dimensões conceituais da soberania digital

Esta seção aborda a complexidade conceitual da soberania digital, buscando explicar a evolução histórica da noção de soberania até sua forma digital atual e, a partir disso, analisá-la como um conceito em constante transformação. Ao examinar os elementos que perpassam a evolução deste conceito polissêmico, como cibersegurança, *open source* e governança de dados, esta seção cria uma conexão entre conceitos técnicos e jurídicos, explicando como tais conceitos podem ser associados para implementar valores constitucionais e direitos fundamentais, por meio de desenvolvimento tecnológico autônomo.

1.1 Da soberania à soberania digital e, finalmente, à soberania em IA

A soberania em IA é uma espécie do *genus* soberania digital, que, por sua vez, representa uma evolução da noção de soberania. Porém, como destacamos em nosso estudo sobre "*Digital Sovereignty in the BRICS Countries: How the Global South and Emerging Power Alliances Are Reshaping Digital Governance*"[14], embora a soberania digital tenha atraído uma atenção crescente tanto dos decisores políticos como dos acadêmicos, esse conceito continua a ser fluido, polissêmico e multifacetado, não tendo ainda encontrado uma definição universalmente aceita. Nesse contexto, o objetivo deste trabalho é oferecer as ferramentas necessárias para esclarecer o debate, desde as bases conceituais da soberania digital até as implementações práticas e operacionais do conceito.

14 JIANG, Min; BELLI, Luca (Orgs.), **Digital Sovereignty in the BRICS Countries: How the Global South and Emerging Power Alliances Are Reshaping Digital Governance**, 1. ed. Cambridge: Cambridge University Press, 2025.

A noção westfaliana de soberania é entendida como a prerrogativa dos Estados-Nação de pleno gozo da integridade territorial, igualdade legal e não interferência em assuntos internacionais junto com o monopólio do uso legítimo da força e autoridade suprema sobre seu território. Tal noção implica uma centralidade do Estado desafiada pelo papel essencial que as tecnologias digitais com alcance transnacional – especialmente, no âmbito da automatização por meio de sistemas de IA – acabaram desempenhando no que diz respeito ao funcionamento de nossas sociedades, economias e democracias. Contudo, a evolução da própria noção de soberania, determinada pela transformação digital do Estado, da economia e da sociedade como um todo, não implica a capitulação do poder público: ao contrário, leva-nos a considerar a necessidade de saber analisar o funcionamento das tecnologias que usamos e, idealmente, saber construir alternativas, quando aquelas que usamos possam determinar efeitos colaterais que prejudicam nossos valores constitucionais.

Desde Bodin e Hobbes, a teoria da soberania busca explicar a organização jurídico-política da sociedade a partir da centralidade do poder estatal. Todavia, é importante reiterar que a digitalização da economia e das relações sociais e até democráticas tornaram o direito apenas uma das modalidades de ordenação social. Outras modalidades de regulação estão inscritas no poder estrutural das arquiteturas técnicas da própria tecnologia, na regulação pelos incentivos econômicos (subsídios e tributações) ou pelas normas sociais (hábitos), cuja eficácia supera, muitas vezes, a normatividade estatal.[15]

Assim, a soberania digital deve ser concebida entendendo essas complexidades, como elemento estruturante da soberania nacional contemporânea e, por conseguinte, como condição essencial para a manutenção da própria democracia constitucional em cada país que defina e implemente um processo de transformação digital. De fato, o processo de transformação digital não é neutro, considerando que pode determinar a crescente dependência de setores inteiros da economia e sociedade em um número exíguo de provedores (muitas vezes estrangeiros) de in-

15 Ver *supra* nota 7. Cabe ressaltar que a criação de hábitos para engajar o usuário e criar, idealmente, uma verdadeira dependência de uma tecnologia é um dos principais objetivos da maioria das empresas de sucesso. Ver EYAL, Nir; HOOVER, Ryan. **Hooked: Como construir produtos e serviços formadores de hábitos**, São Paulo: AlfaCon, 2020.

fraestruturas e serviços cujo funcionamento não é entendido, cuja substituição não é possível ou cuja regulação se torna inviável, levantando sérios desafios de soberania e governança.

Como destacaremos no capítulo 3, ao se tornar dependente de infraestruturas de computação em nuvem controladas por reduzido número de corporações estrangeiras para a transformação digital de seus serviços públicos, os Estados correm o risco de comprometer a sua própria função ordenadora sobre a vida social. Empresas globais de tecnologia, como Amazon Web Services (AWS), Microsoft Azure e Google Cloud, concentram em suas infraestruturas – como *data centers*, sistemas de identidade, hospedagem, análises e modelos de IA – funções de organização social que antes eram de responsabilidade direta do poder público.[16]

Os objetivos da transformação digital do Estado devem ser alcançados mediante o entendimento e o gerenciamento dos riscos de dependência estrutural e das limitações à autonomia estatal. A literatura acadêmica aponta que esse processo de "plataformização" do Estado constitui não apenas uma transformação tecnológica, mas também uma transformação política e econômica, em que serviços públicos essenciais passam a ser mediados por plataformas privadas orientadas por incentivos corporativos, e não por critérios de responsabilidade democrática e pelo interesse público.[17]

Em nome da eficiência e da conveniência, muitas organizações públicas e privadas estão se digitalizando cada vez mais por meio de uma rede complexa de soluções de terceiros que geram dependências estruturais e que estão fora de seu controle direto. Essas soluções, tipicamente administradas por empresas estrangeiras e baseadas em softwares proprietários ou em plataformas de Software como Serviço (SaaS, no acrônimo inglês) fornecidas por meio da computação em nuvem, uma vez adotadas, tornam-se extremamente difíceis de substituir, em razão da dependência estrutural criada pela própria arquite-

16 BELLI, Luca. Structural Power as a Critical Element of Social Media Platforms' Private Sovereignty, 2022; BRUNER, Christopher, States, Markets, and Gatekeepers: Public-Private Regulatory Regimes in an Era of Economic Globalization. **Michigan Journal of International Law**, v. 30, n. 1, p. 125–176, 2008. CULPEPPER, Pepper D.; THELEN, Kathleen. Are We All Amazon Primed? Consumers and the Politics of Platform Power. **Comparative Political Studies**, v. 53, n. 2, p. 288–318, 2020. BREMMER, Ian, The Technopolar Moment: How Digital Powers Will Reshape the Global Order. **Foreign Affairs**, v. 100, n. 6, p. 112–128, 2021.

17 POPIEL, Pawel; VASUDEVAN, Krishnan. Platform frictions, platform power, and the politics of platformization. **Information, Communication & Society**, v. 27, n. 10, p. 1867-1883, 2024.

tura dessas tecnologias. O preço que se paga por essa "conveniência" é a perda de controle sobre informações – dados pessoais ou críticos – e operações essenciais para o funcionamento de empresas ou administrações.

Essas lógicas de apropriação de informações e intermediação de qualquer atividade por meio de sistemas digitais frequentemente se entrelaçam com modelos de negócios baseados no chamado "capitalismo de vigilância",[18] nos quais as tecnologias digitais, aparentemente utilizadas apenas para digitalizar administrações e serviços, tornam-se ferramentas para o controle generalizado e a captura de valor e da possibilidade de tomar decisões autônomas, servindo, na realidade, à concentração de poder e capital nas mãos de pouquíssimas empresas de computação em nuvem.[19]

Combinando a teoria estrutural e a análise empírica de um conjunto abrangente de dados, várias pesquisas apontam como a dependência de infraestruturas digitais limita a autonomia dos Estados e possibilita o uso assimétrico do poder infraestrutural embutido em tais infraestruturas, no âmbito de uma ordem mundial na qual apenas os Estados Unidos e, em certa medida, a China, podem ser considerados tecnologicamente autônomos.[20]

Pesquisa, inovação e investimentos são, portanto, pré-requisitos essenciais para gerar processos sustentáveis de transformação digital que possam concretizar o conceito de "Estado digital".[21] Sendo assim, a inovação desempenha um papel particularmente importante como "um processo pelo qual a novidade é assumida e disseminada na esfera pública",[22]

---

18 ZUBOFF, Shoshana. **The age of surveillance capitalism: the fight for a human future at the new frontier of power**, First trade paperback edition. New York, NY: PublicAffairs, 2020.NY: PublicAffairs, 2020.

19 BELLI, Luca et al. **L' État digital: numérisation de l'administration publique et administration publique du numérique / sous la direction de Luca Belli et Gilles J. Guglielmi**, [s.l.]: Berger-Levrault, 2022.

20 MAYER, Maximilian; LU, Yen-Chi. Global structures of digital dependence and the rise of technopoles, **New Political Economy**, v. 30, n. 5, p. 755–774, 2025. **Big AI: Cloud infrastructure dependence and the industrialisation of artificial intelligence**. Disponível em: <https://journals.sagepub.com/doi/epdf/10.1177/20539517241232630?src=getftr&utm_source=tfo&getft_integrator=tfo>. Acesso em: 25 set. 2025; BELLI, Luca; GASPAR, Walter Britto (Orgs.). **The Quest for AI Sovereignty, Transparency and Accountability**. Rio de Janeiro: FGV Direito Rio, 2023.

21 BELLI, Luca et al, **L' État digital**.

22 DE SAILLE, Stevienna; MEDVECKY, Fabien. Innovation for a steady state: a case for responsible stagnation. **Economy and Society**, v. 45, n. 1, p. 1-23, 2016.

apresentada como essencial para o desenvolvimento social e econômico. É importante enfatizar aqui que a inovação não se manifesta exclusivamente por meio da tecnologia, mas também como inovação normativa, institucional e administrativa.[23]

De um lado, a lógica de plataformização extrativista é antitética à essência do serviço público, que é o instrumento por meio do qual as Nações conseguem concretizar suas aspirações constitucionais, avançando no caminho de um desenvolvimento socioeconômico comum. Assim, a digitalização de serviços públicos deve permanecer ao serviço da própria Nação, e não de interesses privados ou políticos que se mostram contrários ao interesse nacional. De outro lado, a dependência de infraestruturas digitais opacas representa um enorme risco ao setor produtivo nacional. Assim, existe um real desafio regulatório devido à opacidade técnica e até contratual das infraestruturas e serviços digitais dos quais o Estado e inteiros setores da economia nacional se tornam dependentes. Cabe enfatizar a absoluta impossibilidade em se regular sistemas cujo funcionamento não se compreende, e que não há eficácia em regular – nem possibilidade de concorrência – quando inexistem alternativas tecnológicas viáveis.

Nesse contexto, quando a transformação digital se torna dependência tecnológica, a perda de soberania digital equivale a um enfraquecimento estrutural da autoridade estatal. A perda de soberania (digital) configura transferência de poderes soberanos para entes privados que operam fora do alcance das jurisdições nacionais, com base em interesses econômicos e políticos que podem ser literalmente antitéticos ao interesse público nacional.

Para evitar ou reverter essa situação, torna-se essencial entender as dinâmicas da soberania digital. Nossa definição de trabalho de soberania digital[24] tem sido "a capacidade de entender o funcionamento das tecnologias digitais, conseguir desenvolvê-las e regulá-las efetivamente, exercendo, portanto, autodeterminação, poder e controle sobre ativos digitais tais como dados, softwares, hardwares e redes eletrônicas". Com base nessa definição, a soberania em IA pode ser definida como "a capacidade de en-

23 BELLI, Luca et al. **L' État digital**.

24 JIANG, Min; BELLI, Luca (Orgs.). **Digital Sovereignty in the BRICS Countries: How the Global South and Emerging Power Alliances Are Reshaping Digital Governance**, 1. ed. Cambridge: Cambridge University Press, 2025.

tender, desenvolver e regular sistemas de IA, mantendo, assim, a autodeterminação, agência e controle sobre tais sistemas".[25]

Ela implica, então, a aptidão não somente dos Estados, mas também de outras entidades de natureza diferente, tais como grupos de indivíduos, corporações, organizações supranacionais, dentre outros, para entender os efeitos positivos e negativos que determinadas tecnologias podem ocasionar. Concerne, ainda, à capacidade desses atores de desenvolver tais tecnologias de maneira autônoma e consciente e as regular conforme os próprios valores.

1.2 A evolução da soberania digital

Antes mesmo de o termo "soberania digital" surgir no debate internacional, os Estados Unidos já exerciam um elevado grau de soberania digital de fato, consolidado por sua autonomia tecnológica, domínio sobre os principais elementos infraestruturais da Internet – como aplicativos, infraestruturas, produção de conteúdo e processamento de dados, devido a décadas de investimentos em pesquisa e desenvolvimento por meio de política industrial extremamente focada – e regulação privada[26] de tais elementos, inclusive por meio da capacidade de definir padrões e normas globais sem depender de instâncias externas.[27]

Entretanto, o discurso sobre soberania digital parece começar oficialmente em 2011, com a proposição da Organização de Cooperação de Xangai, uma organização intergovernamental liderada por China e Rússia que, em 2011, elaborou um Código Internacional de Conduta para Segurança da Informação, atualizado em 2015, mencionando explicitamente o tema da "soberania na Internet." A proposta de tal tema para uma organização cujos membros incluem alguns dos países com baixos índices de respeito

25 *Ibid*.

26 BELLI, Luca et al. Structural Power as a Critical Element of Digital Platforms Private Sovereignty.

27 A articulação e institucionalização desta evolução tecnológica, infraestrutural e normativa pode ser considerada como a primeira forma de soberania digital, sabidamente organizada por meio de parcerias multissetoriais pelo governo estadunidense, desde o final dos anos 1950. Tais evoluções são analisadas nas páginas 133-303 de BELLI, Luca. **De la gouvernance à la régulation de l'internet**, Berger-Levrault, Boulogne-Billancourt, 2016.

à direitos humanos[28] sugeriu a associação do tema a uma conotação autoritária. Por certo, existem manifestações autoritárias da soberania (não somente digital), mas associar soberania digital inevitavelmente ao autoritarismo significaria ignorar não somente a evolução do conceito, mas uma amplíssima gama de exemplos de "boa soberania digital".[29]

Um desses exemplos já é parte do cotidiano brasileiro: o Pix. Antes do Pix, a única opção disponível para processar pagamentos eletrônicos instantâneos em tempo integral no Brasil era utilizar as redes das gigantes estadunidenses Visa e Mastercard, que cobram uma taxa de 3% a 5% em cada transação, além de centralizar a coleta de dados de todos os seus usuários.[30] O papel-chave das duas empresas antes do Pix significava que a soberania brasileira sobre pagamentos digitais era, de fato, delegada a dois atores estrangeiros que monopolizavam não somente renda extraída de cada transação, mas também o controle sobre os dados coletados de cada transação e, com base neles, a capacidade de desenvolver sistemas de IA.

Como ressaltaremos no próximo capítulo, a capacidade de inovar e competir no mercado de IA depende em larga medida de acesso a dados de alta qualidade. Portanto, ter uma posição de controle na coleta de dados sobre um setor inteiro – nesse caso, os pagamentos online – permite à entidade controlador de definir quem poderá competir no mercado ou até de "desertificar"[31] o setor, impedindo o acesso a um dos insumos essenciais para competir e inovar, nesse caso, os dados. Esses pontos são a principal razão pela qual o desenvolvimento de infraestruturas públicas digitais[32] como o Pix é enormemente relevante do ponto de vista daquilo que designamos boa soberania digital.

---

28 HUMAN RIGHTS WATCH. **World Report 2025 | Human Rights Watch**, [s.l.: s.n.], 2025.

29 BELLI, Luca. **Building Good Digital Sovereignty through Digital Public Infrastructures and Digital Commons in India and Brazil**. ThinkTwenty (T20) India 2023 - Official Engagement Group of G20. Disponível em: <https://t20ind.org/research/building-good-digital-sovereignty-through-digital-public-infrastructures/>. Acesso em: 24 set. 2025.

30 CHRISTL, Wolfie. How Companies Use Personal Data Against People. Automated Disadvantage, Personalized Persuasion, and the Societal Ramifications of the Commercial Use of Personal Information. **Working paper by Cracked Labs**, 2017.

31 Esse assunto será explorado na seção 3.2.

32 DRAPER, Hannah et al. **A Consumer-centric Approach to DPIs for sustainable financial inclusion**, Brasil: T20 Brasil 2024, 2024.

Cabe frisar que pouquíssimos estudos abordam a origem do Pix, que é diretamente inspirado no UPI, análogo sistema introduzido pela *Reseve Bank of India* em 2016 como uma rede de pagamento instantâneo baseada em uma API aberta operada pela *National Payments Corporation of India*.[33] Ainda menos estudos frisam que o UPI é inspirado pelo sistema Russo Mir, desenvolvido logo depois da invasão da Crimeia, em 2014, que resultou na primeira rodada de sanções – entre as quais a proibição do uso das redes Visa e Mastercard.[34]

É importante enfatizar que a criação do Pix ou do UPI demonstra a capacidade de proporcionar mais alternativas e estimular a inovação autóctone reduzindo custos e aumentando o bem-estar do consumidor. Portanto, a visão de boa soberania digital – que acreditamos que o Brasil deveria adotar internamente e promover internacionalmente – não deve se confundir com a promoção de uma autarquia digital. Ao contrário, a soberania digital deve necessariamente incluir a promoção e construção de ecossistemas digitais abertos, interoperáveis e cooperativos, capazes de preservar a autonomia e autodeterminação de indivíduos, empresas e Estados, evitando dependências tecnológicas que geram aprisionamento (*lock-in*[35]) e restringem a capacidade de escolha e tomada de decisão.

É interessante também frisar que o conceito de soberania digital ganhou uma conotação menos negativa somente quando, em 2020, se tornou uma pauta europeia, apresentada pelo Presidente Macron e pela Presidenta Von Der Leyen como a legítima aspiração à autonomia estratégica e controle sobre ativos digitais. Na época, o debate se tornou necessário diante da postura imprevisível e potencialmente danosa da primeira administração Trump no que diz respeito a sanções sobre tecnologia digital – postura

33 Tal origem é abordada em JIANG; BELLI, Digital Sovereignty in the BRICS Countries.

34 BELLI, Luca; JIANG, Min, Conclusion: Digital Sovereignty in the BRICS: Structuring Self-Determination, Cybersecurity, and Control, *in*: JIANG, Min; BELLI, Luca (Orgs.). **Digital Sovereignty in the BRICS Countries**, 1. ed. Cambridge: Cambridge University Press, 2025, p. 214–238.

35 A situação de lock-in determina uma dependência de fornecedor de computação em nuvem e ocorre quando os clientes ficam literalmente presos (ou seja, *locked-in* em inglês) a uma única implementação tecnológica de um provedor de nuvem e não conseguem migrar facilmente para um fornecedor diferente no futuro sem custos substanciais, restrições legais ou incompatibilidades técnicas. Essa situação será analisada na seção 3.1.

que, em retrospectiva, parece tímida comparada aos primeiros meses do segundo mandato Trump.

Quando o presidente estadunidense começou a adotar ordens executivas como armas econômicas, proibindo o uso de software estadunidense pela chinesa Huawei[36] e tentando bloquear o TikTok, a maioria dos países europeus começou a perceber os riscos da dependência tecnológica. Pela primeira vez nos últimos trinta anos, as lideranças europeias se deram conta de sua extrema vulnerabilidade por falta de autonomia tecnológica e, ao contrário, a total dependência de infraestruturas digitais controladas por empresas e estados com interesses geopolíticos potencialmente hostis.

Porém, é assustador constatar que nos últimos cinco anos eles não foram capazes sequer de elaborar um esboço de plano para criar autonomia tecnológica, sendo hoje totalmente desamparados face à sua situação de colônia digital.[37] Nesse sentido, não nos parece que a experiência europeia ofereça boas práticas de soberania digital que possam ser replicadas. Ao contrário, parece-nos que poderia ser estudada como um exemplo de falta de soberania digital.

A ciência política complementa essa perspectiva ao identificar soberania como autonomia e projeção de poder. No âmbito da disciplina de Relações Internacionais, especialmente na corrente realista, a soberania é compreendida não apenas como independência formal, mas, na ausência de uma autoridade superior, a soberania surge como um equalizador político entre as unidades estatais, que buscam simultaneamente garantir sua autonomia e projetar poder sobre os demais atores (estatais ou não) no sistema internacional. Para tanto, a soberania é fundamentada pelo controle e exploração de elementos de poder estatal. Esses elementos de poder emanam de recursos, incluindo a influência sobre organizações e atores não estatais, que compõem capacidades estratégicas fundamentais para a autonomia, sobrevivência e eventual projeção de poder pelo Estado.[38]

---

36 JIANG, Min. **U.S. Ban on Huawei: Superpowers' Insecurities and Nightmares**, CyberBRICS, Disponível em: <https://cyberbrics.info/u-s-ban-on-huawei-superpowers-insecurities-and-nightmares/>. Acesso em: 11 nov. 2025.

37 Esta situação é descrita de maneira detalhada e contundente em BRIA, Francesca; TIMMERS, Paul; GERNONE, Fausto. **EuroStack** – A European Alternative for Digital Sovereignty, p. 127, 2025.

38 CARR, E. H. **The Twenty Years' Crisis, 1919-1939: Reissued with a new preface from Michael Cox**, [s.l.]: Springer, 2016; MORGENTHAU, Hans J. **A política entre nações**, [s.l.]: Universidade

Assim, sob as lentes das Relações Internacionais, o conceito de soberania digital implica diretamente a construção de capacidades nacionais para controlar aqueles que podem ser considerados os ativos críticos para o desenvolvimento de sistemas de IA, desde a matriz energética para abastecimento e resfriamento de *data centers* até recursos minerais críticos, indispensáveis à fabricação de semicondutores e infraestrutura tecnológica, bem como dados de alta qualidade, que alimentam algoritmos de inteligência artificial e sistemas digitais.

Nota-se, portanto, que, assim como os recursos naturais eram alicerces de poder no século XX, hoje o domínio sobre minerais estratégicos e fluxos de dados se converte em um pilar central da autodeterminação e da projeção de poder soberano no século XXI. Contudo, ao passo que a digitalização permitiu a transferência de serviços (públicos e privados), como educação, saúde e economia, para empresas e serviços estrangeiros, ocorre um esvaziamento da soberania e cidadãos de um Estado ficam à mercê de interesses comerciais de empresas e, inevitavelmente, dos interesses políticos de outros governos.

Nessa perspectiva, cabe frisar que as dinâmicas da globalização, amplamente refletidas na governança digital das últimas três décadas, evidenciaram uma crescente "difusão do poder" estatal,[39] deslocando o Estado de organizador e implementador de políticas públicas para a condição de ator (ou *stakeholder*) que pode ser regulado por meio de estruturas privadas transnacionais.[40] A globalização transformou a ordem liberal ao deslocar a ação política de negociações multilaterais entre Estados para redes de atores privados.[41]

Essa transformação teve consequências cruciais sobre a localização e o exercício do poder estatal em nível doméstico e internacional. Sistemas privados globais e infraestruturas privadas, originalmente projetadas para

---

de Brasília, 2003. WALTZ, Kenneth N., Structural Realism after the Cold War. **International Security**, v. 25, n. 1, p. 5–41, 2000; WALTZ, Kenneth. **Man, the State, and War: A Theoretical Analysis**, [s.l.]: Columbia University Press, 2018.

39 NYE, J.S. **O Futuro Do Poder**, [s.l.]: BENVIRA, 2012.

40 BRUNER, States. Markets, and Gatekeepers; TUSIKOV, Natasha, **Chokepoints: Global Private Regulation on the Internet**. [s.l.]: Univ of California Press, 2016; BELLI, Structural Power as a Critical Element of Social Media Platforms' Private Sovereignty.

41 OATLEY, Thomas. **Toward a political economy of complex interdependence**. Disponível em: <https://journals.sagepub.com/doi/full/10.1177/1354066119846553>. Acesso em: 23 set. 2025.

gerar eficiências de mercado e reduzir custos de transação, tornaram-se pontos estratégicos de controle dos fluxos de informação, moldando oportunidades estratégicas.[42] Atores que controlam sistemas dos quais todos dependem – inclusive os Estados – podem explorar sua posição de poder estrutural para exercer influência e controle.

Portanto, como destacaremos neste trabalho, para construir sua soberania digital, o Brasil – e qualquer outro país ou entidade – necessita adotar uma abordagem sistêmica capaz de articular política industrial, capacidade regulatória, parcerias estratégicas, e *situational awareness*[43], isto é, a capacidade institucional não somente de mapear e conhecer seus próprios ativos, mas também de identificar, interpretar e reagir a riscos e oportunidades inerentes às evoluções (externas) das tecnologias digitais. Assim, os riscos, bem como as oportunidades, emergem e se transformam permanentemente nos ecossistemas digitais, tendo a possibilidade de impactar a soberania nacional e, portanto, determinando a necessidade de capacidade de percepção situacional.

Isso inclui entender que a dependência de infraestruturas e tecnologias estrangeiras permite aos atores que controlam tais sistemas gerir fluxos de informação e definir os comportamentos de quem for dependente deles. Tal percepção situacional exige investimento não apenas na pesquisa, mas também na formação de indivíduos – especialmente funcionários públicos – capazes de entender e mapear tais riscos, e a definição de uma governança multissetorial e multinível para que tal sistema seja capaz de operar efetivamente.

Por fim, é importante destacar que a soberania digital não deve ser enxergada somente como uma aspiração estatal, ou como uma capacidade exclusiva de enormes empresas de tecnologia que dominam ecossistemas digitais inteiros.[44] Ao contrário, existem exemplos particularmente

---

42 TUSIKOV, **Chokepoints**; MAYER; LU. Global structures of digital dependence and the rise of technopoles.

43 JAJODIA, Sushil; ALBANESE, Massimiliano. An Integrated Framework for Cyber Situation Awareness. In*:* LIU, Peng; JAJODIA, Sushil; WANG, Cliff (Orgs.). **Theory and Models for Cyber Situation Awareness**. Cham: Springer International Publishing, 2017, v. 10030, p. 29-46; LUNDBERG, Jonas, Situation awareness systems, states and processes: a holistic framework. **Theoretical Issues in Ergonomics Science**, v. 16, n. 5, p. 447-473, 2015.

44 A existência de concepções e manifestações altamente heterogêneas de soberania digital, que podem interessar não somente Estados ou corporações, mas também comunidades de indivíduos – que organizam sua soberania digital de maneira distribuída e bottom-up – ou

eloquentes que demonstram a possibilidade de iniciativas comunitárias e *bottom-up* de soberania digital.

Nesse sentido, cabe destacar a existência de iniciativas de redes comunitárias,[45] 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[46], que permitem a grupos de trabalhadores e desenvolvedores se associarem para fornecer serviços digitais. Essas iniciativas nos levam a relativizar a importância das dependências tecnológicas existentes e a considerar que o primeiro e talvez o mais relevante ingrediente da soberania digital seja a vontade e a determinação de se tornar tecnologicamente independente.

1.3 Código aberto (*open source*) como estratégia de soberania tecnológica

A adoção e o desenvolvimento estratégico de software, modelos de IA e infraestruturas *open source*[47] constituem, do ponto de vista jurídico e

até organizações supranacionais, é analisada em JIANG; BELLI (Orgs.). **Digital Sovereignty in the BRICS Countries**.

45 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 e autonomia, provando que a conectividade à internet pode ser construída pelas próprias comunidades locais, para benefício delas mesmas. Community networks - the Internet by the people, for the people. 1.1; BELLI, Luca. **Community Networks: Building Digital Sovereignty and Environmental Sustainability**, Rio de Janeiro, RJ: Publicações Direito Rio, 2023; **Network self-determination: When building the internet becomes a right**. 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.

46 GROHMANN, Rafael. Not just platform, nor cooperatives: worker-owned technologies from below. **Communication, Culture and Critique**, v. 16, n. 4, p. 274-282, 2023.

47 Uma IA de código aberto é um sistema de IA disponibilizado sob termos e de uma forma que concede as seguintes liberdades: i) usar o sistema para qualquer finalidade e sem precisar pedir

de política pública, um instrumento central para a construção de soberania tecnológica.[48] Nesse contexto, o *open source* oferece vetores tangíveis de autodeterminação ao reduzir dependências proprietárias e ao possibilitar verificabilidade, auditabilidade e colaborações público-privadas baseadas em transparência.

O debate sobre *open source* como alavanca da soberania digital, especialmente no que diz respeito à IA, merece ser priorizado neste volume, especialmente considerando o papel desempenhado pelo Brasil neste contexto. Essa retrospectiva é essencial para entender quais condições levaram à exploração bem-sucedida das tecnologias de código aberto e quais condições levaram ao fracasso, ao longo das últimas décadas.

Assim, experiência brasileira pode ser considerada ao mesmo tempo um dos casos pioneiros, mas também um fracasso na adoção de software livre e de código aberto como instrumento de política pública voltado à promoção de soberania digital.[49] Isso se deve ao fato de o Brasil ter enxergado, já em 2003, o valor do código aberto como ferramenta de autonomia tecnológica. Contudo, a estratégia nacional, ainda que inovadora, ancorou-se predominantemente na adoção governamental de soluções abertas – sobretudo no âmbito da administração pública federal, ao longo dos anos 2000 – em vez de priorizar investimentos estruturais na produção doméstica de componentes críticos, bibliotecas e comunidades de desenvolvimento, para alavancar a produção e até a exportação de tecnologias em *open software* como vetor do que hoje seria denominado soberania digital.[50]

Essa assimetria implicou uma dependência persistente de projetos estrangeiros, não permitindo ao Brasil consolidar um ecossistema de produção local que conferisse real autonomia tecnológica e permitisse a projeção

---

permissão; ii) estudar como o sistema funciona e inspecionar seus componentes; iii) modificar o sistema para qualquer finalidade, inclusive para alterar sua saída; iv) compartilhar o sistema para que outros o utilizem, com ou sem modificações, para qualquer finalidade. Essas liberdades se aplicam tanto a um sistema totalmente funcional quanto a elementos discretos de um sistema. Uma condição prévia para o exercício dessas liberdades é ter acesso à forma preferencial para realizar modificações no sistema. The Open Source AI Definition – 1.0.

48 JIANG; BELLI (Orgs.). **Digital Sovereignty in the BRICS Countries**; BELLI, **Building Good Digital Sovereignty through Digital Public Infrastructures and Digital Commons in India and Brazil**.

49 Towards a Sovereign Digital Infrastructure of Commons.

50 JIANG; BELLI (Orgs.). **Digital Sovereignty in the BRICS Countries**.

de poder tecnológico. O resultado foi uma experiência frustrada de soberania digital: ampliou-se o acesso e a transparência, mas não se consolidou a capacidade nacional de gerar e sustentar tecnologias de código aberto como infraestruturas estratégicas.

Em contraste, outras experiências nos mostram que, quando o *open software* não é considerado somente como algo a ser adotado, mas cujo desenvolvimento deve ser também estimulado como prioridade de política industrial, os resultados podem ser particularmente interessantes, como mostram as experiências chinesas ou europeias, que serão analisadas especificamente nas próximas subseções.

Experiências recentes de abertura tecnológica em larga escala, como as iniciativas de desenvolvimento de modelos de IA em código aberto, como o GPTNeo e BLOOM e parcialmente abertos (ex.: Mistral, Falcon e DeepSeek[51]) e os investimentos em infraestruturas públicas digitais, como no caso do India Stack, indicam uma abordagem distinta de soberania digital, ancorada não apenas na adoção, mas também na produção e manutenção de ativos tecnológicos. Nesses casos, o código aberto é mobilizado como instrumento de política industrial e de autonomia estratégica, estimulando ecossistemas nacionais e regionais de inovação, reduzindo dependências críticas e consolidando capacidade própria de desenvolvimento tecnológico. Em vez de se limitar à substituição de softwares proprietários por equivalentes abertos, trata-se de usar o *open source* como uma plataforma de coordenação público-privada e de projeção de poder infraestrutural, capaz de moldar padrões tecnológicos e regulatórios a partir da própria arquitetura.

Para Estados que buscam soberania em IA, compreender essas dinâmicas, isto é, a diferença entre adotar tecnologias abertas e produzi-las como bens estratégicos, é crucial para evitar dependências e, ao mesmo tempo, para posicionar-se em cadeias globais de valor, conseguindo ex-

51 Modelos DeepSeek são *open weight*, com parâmetros abertos, mas não são totalmente *open source*, pois código e dados de treinamento não são divulgados. Essa abordagem limita modificações em comparação ao open source verdadeiro. DeepSeek lançou modelos sob licenças permissivas, como DeepSeek-R1 sob MIT, permitindo uso livre, destilação e comercialização. **DeepSeek-R1 Release | DeepSeek API Docs**. Disponível em: <https://api-docs.deepseek.com/news/news250120>. Acesso em: 7 nov. 2025.

plorar os próprios ativos nacionais.[52] Reconhecer tal processo permite que países como o Brasil repensem suas políticas, passando de uma soberania baseada no consumo para uma soberania baseada na produção, a qual se revelaria mais robusta e duradoura.

Cabe ressaltar, porém, que, do ponto de vista técnico-jurídico, a opção pelo *open source* introduz vantagens e limites que exigem tratamento normativo diferenciado. Em termos positivos, o código aberto promove auditabilidade *ex ante* e *ex post* dos sistemas de IA (permitindo avaliações de conformidade técnica com obrigações de segurança, privacidade e não discriminação), facilita a portabilidade e a interoperabilidade (reduzindo *lock-in* e custos de transição) e cria um ecossistema onde fornecedores locais, pesquisadores e administrações públicas podem adaptar, auditar e manter componentes críticos sem depender exclusivamente de fornecedores estrangeiros.[53]

Esses atributos operacionais traduzem-se em menores barreiras à implementação de exigências legais – por exemplo, avaliações de impacto algorítmico, diligências técnicas obrigatórias e requisitos de documentação – que são instrumentos de cumprimento normativo cada vez mais adotados para regulamentar tecnologias digitais e, particularmente, sistemas de IA.

Todavia, a instrumentalização do *open source* como política de soberania exige cautelas jurídicas: a simples disponibilidade de código fonte não elimina riscos estruturais (por exemplo, dependências de hardware estrangeiro, expertise técnica concentrada ou financiamento exógeno). A literatura aponta que uma política de "soberania por código aberto" deve conjugar três pilares: i) enquadramento regulatório que obrigue e habilite práticas de transparência e de auditoria; ii) incentivos industriais (financiamento da manutenção de bens comuns digitais, formação e contratação) e iii) mecanismos de cooperação interadministrativa para partilha de componentes críticos que constituam bens públicos digitais.[54] Sem essas medidas complementares, o *open source* pode funcionar apenas como um

52 BELLI; GASPAR (Orgs.). **The Quest for AI Sovereignty, Transparency and Accountability**.

53 EUROPEAN WORKING TEAM ON DIGITAL COMMONS, **Towards a Sovereign Digital Infrastructure of Commons**, Paris, France: [s.n.], 2022.

54 Towards a Sovereign Digital Infrastructure of Commons; **Governance, uses, sovereignty, RGPD, cyber risks: how do local authorities manage their data? - Labo**. Disponível em: <https://labo.societenumerique.gouv.fr/en/articles/governance-uses-sovereignty-rgpd-risks-cyber-how-communities-manage-their-data/>. Acesso em: 24 set. 2025. *Ibid*.

rótulo retórico, com impacto limitado sobre a industrialização tecnológica e sobre a autonomia normativa efetiva.[55]

É importante frisar também que, juridicamente, o *open source* altera as relações contratuais e de responsabilidade. Contratos públicos que privilegiam soluções proprietárias tendem a abarcar cláusulas de confidencialidade, restrições à auditoria e dependências contratuais que reduzem a capacidade do Estado de supervisionar software crítico. Como destacaremos em seguida, a adoção massiva de componentes *open source* em soluções públicas requer, portanto, o estabelecimento de regimes regulatórios e contratuais renovados que contemplem instrumentos capazes de reduzir a incerteza jurídica e assegurar que o código aberto produza não só transparência técnica, mas também responsabilização jurídica.[56]

Portanto, no domínio da IA, o *open source* desempenha papel triplo para estruturar a soberania: como mitigador de riscos de dependência, como catalisador de capacidades locais de pesquisa e certificação, e como vetor de projeção internacional de autonomia tecnológica. Por outro lado, é fundamental reconhecer riscos decorrentes da governança do próprio ecossistema *open source*: projetos críticos muitas vezes dependem de um número reduzido de colaboradores-chave e de financiamento voluntário, o que cria vulnerabilidades operacionais e de segurança. Assim, políticas públicas destinadas à soberania digital devem destinar recursos à sustentabilidade das infraestruturas necessárias para permitir a sustentabilidade do *open source* (por exemplo, manutenção de repositórios, auditorias de segurança, seguros de responsabilidade para colaboradores institucionais) e criar padrões de certificação que valorizem práticas de gestão de dependências e de testes de segurança.

Ademais, o *open source* também é usado como forma de captura de valor por empresas controladoras de sistemas corporativos de inovação[57]. A título de exemplo, pode-se mencionar o fato de que a Microsoft comprou

---

55 ZINGALES, Nicolo, **Open Source AI: um conceito à procura da sua definição**. JOTA Jornalismo. Disponível em: <https://www.jota.info/opiniao-e-analise/colunas/ia-regulacao-democracia/open-source-ai-um-conceito-a-procura-da-sua-definicao>. Acesso em: 11 nov. 2025.

56 Ver a Seção 1.6.2.

57 RIKAP, Cecilia. **Dynamics of Corporate Governance Beyond Ownership in AI**, Common Wealth. Disponível em: <https://www.common-wealth.org/publications/dynamics-of-corporate-governance-beyond-ownership-in-ai>. Acesso em: 5 out. 2024.

o GitHub e, posteriormente, o utilizou como insumo para o treinamento de sua ferramenta de IA Copilot[58]. Dito diversamente, essas acabam se revelando como formas de obter trabalho gratuito das comunidades e reforçar sua dependência do ecossistema controlado por elas. De certa forma, isso representa uma inversão da lógica de funcionamento do *open source* que, ao definir requisitos de uso abertos (via licenças de propriedade intelectual e termos de uso) – determinando direitos de uso e reuso –, busca promover a abertura do sistema tecnológico, não o seu encerramento em torno de lógicas proprietárias.

Em conclusão, devemos enxergar o *open source* como estratégia para promover soberania digital e soberania em IA, desde que incorporado num quadro jurídico e institucional que assegure financiamento, responsabilização e integração normativa. A mera disponibilização de código não substitui a necessidade de políticas públicas robustas: a soberania real exige coesão entre normas, capacidades institucionais e investimentos sustentados que transformem códigos abertos em infraestruturas resilientes e compatíveis com arcabouços jurídicos nacionais.

1.3.1 Open source *como pilar estruturante da autonomia tecnológica chinesa: Kylin, RISC-V e o XV Plano Quinquenal*

A experiência chinesa é particularmente interessante, porque o gigante asiático começou a se interessar pelo *open source* no mesmo período do Brasil; no entanto, a abordagem chinesa revela a importância de se enxergar não somente a adoção, mas também o investimento em pesquisa, desenvolvimento e institucionalização da governança, como elementos estruturantes necessários. Assim, ao longo das últimas duas décadas, o *open source* consolidou-se como um elemento constante e estruturante da estratégia chinesa de autonomia tecnológica. Desde o início dos anos 2000, quando começou

58 XIANG, Chloe. **GitHub Users File a Class-Action Lawsuit Against Microsoft for Training an AI Tool With Their Code**, Vice. Disponível em: <https://www.vice.com/en/article/bvm3k5/github-users-file-a-class-action-lawsuit-against-microsoft-for-training-an-ai-tool-with-their-code>. Acesso em: 21 nov. 2023.

o desenvolvimento do sistema operativo Kylin[59], o Estado chinês passou a reconhecer o código aberto como um instrumento de soberania nacional, capaz de reduzir dependências tecnológicas externas e fortalecer suas capacidades estratégicas em setores sensíveis. A China investiu de forma continuada em pesquisa e desenvolvimento de tecnologias abertas, criando sistemas operacionais próprios, incentivando a adoção de padrões abertos como RISC-V[60] em semicondutores[61] e fomentando ecossistemas acadêmicos e industriais baseados em compartilhamento tecnológico regulado.

Paralelamente, institucionalizou a governança do *open source*, com a criação de fundações nacionais, diretrizes jurídicas específicas e integração de políticas de abertura no planejamento estatal de médio e longo prazo. Assim, o *open source* não foi um fenômeno isolado, mas uma escolha deliberada da política industrial e desenvolvimentista, alinhada aos objetivos de autossuficiência, segurança digital e liderança tecnológica global. Particularmente, a incorporação do *open source* no XV Plano Quinquenal (2026–2030)[62] demonstra que o código aberto deixa de ser apenas um recurso técnico e passa a ocupar posição central como instrumento de soberania digital, inovação regulada e fortalecimento da segurança nacional.

O XV Plano Quinquenal enfatiza a necessidade de alcançar independência tecnológica, referida como "autossuficiência e autoconfiança científica". Entre as diretrizes do documento, destaca-se o estímulo formal à abertura de software, hardware e serviços, com o objetivo de consolidar um ecossistema nacional de inovação baseado em tecnologias auditáveis,

---

59 **Kylin_OS/index**. Disponível em: <https://web.archive.org/web/20040926085248/http://www.kylin.org.cn/>. Acesso em: 19 nov. 2025.

60 RISC-V significa "Reduced Instruction Set Computing Five" e é um tipo de Arquitetura de Conjunto de Instruções (ISA). As ISAs funcionam como uma interface entre o software e o hardware, determinando como as CPUs são controladas pelo software. Uma analogia útil compara a ISA aos pedais e à interface do usuário entre o carro (o hardware) e o motorista (o software). About RISC-V.

61 XiangShan: open-source high-performance RISC-V processor.

62 Recommendations of the Central Committee of the Communist Party of China on the formulation of the fifteenth five-year plan for national economic and social development. Adopted at the Fourth Plenary Session of the 20th Central Committee of the Communist Party of China on October 23, 2025. CHINA, Proposta do Comitê Central do PCC sobre a formulação do 15º Plano Quinquenal para o Desenvolvimento Econômico e Social Nacional (中共中央关于制定国民经济和社会发展第十五个五年规划的建议), 2025.

modificáveis e juridicamente controláveis. O texto estabelece que empresas e instituições devem promover a abertura regulada de software, arquiteturas de hardware e plataformas de serviço, para criar um ambiente competitivo de inovação. Essa orientação não é meramente econômica ou técnica, mas normativa, pois impõe diretrizes para propriedade intelectual, segurança nacional e controle estatal sobre tecnologias críticas.

Cabe ressaltar que a consagração do *open source* no mais alto nível do planejamento estatal é somente a última etapa de uma evolução de mais que duas décadas. Como mencionado acima, o sistema operacional Kylin, e sua versão NeoKylin[63], ilustram claramente a estratégia de apropriação estatal do *open source* para fins de segurança tecnológica. Baseado no kernel Linux[64] e em componentes de código aberto, o Kylin permite auditoria de segurança, customização para dispositivos nacionais e compatibilidade com arquiteturas domésticas. Seu desenvolvimento foi institucionalizado em políticas públicas, e sua adoção é promovida de maneira mandatória em órgãos governamentais, empresas estatais e infraestruturas críticas.

No campo do hardware, a arquitetura RISC-V é tratada pelo governo chinês como uma oportunidade histórica para superar barreiras impostas por modelos de licenciamento restritivos e sanções comerciais.[65] Ao contrário das arquiteturas proprietárias, como ARM e x86, a RISC-V é baseada em padrões abertos e permite liberdade jurídica para desenvolvimento, produção e exportação de designs de processadores modificados e otimizados para o contexto nacional. O XV Plano Quinquenal destaca a importância das "tecnologias centrais e estratégicas", e a adoção da RISC-V reflete exatamente essa diretriz, pois trata o *open source* não como fragilidade, mas como fundamento da resiliência tecnológica. A abertura de sua especificação permite à China – e a qualquer outro ator interessado – desenvolver chips compatíveis com suas próprias infraestruturas de computação, sistemas de IA e

63 Kylin (operating system), *in*: **Wikipedia**, [s.l.: s.n.], 2025.

64 O kernel Linux é o núcleo central do sistema operacional Linux, atuando como interface essencial entre hardware e software. Ele gerencia memória, processos, dispositivos e chamadas de sistema, garantindo eficiência e segurança em diversos dispositivos, de smartphones a servidores. Iniciado por Linus Torvalds em 1991 como projeto open source, é desenvolvido colaborativamente por centenas de contribuidores globais.

65 **Examining China's Grand Strategy For RISC-V - Jamestown.** Disponível em: <https://jamestown.org/examining-chinas-grand-strategy-for-risc-v/>. Acesso em: 19 nov. 2025.

objetos conectados na Internet das Coisas, sem depender de licenças estrangeiras que possam ser interrompidas por sanções ou disputas comerciais.

A experiência chinesa é particularmente valiosa como ilustração de promoção do *open source* como uma estratégia híbrida de governança, regulação e desenvolvimento para alcançar a autonomia tecnológica. Por um lado, o Estado promove a abertura, a colaboração, a inovação e a transparência como instrumentos voltados a mitigar a hegemonia de empresas estrangeiras em setores tecnológicos estratégicos. Por outro lado, insere tais iniciativas em um arcabouço normativo que garante controle estatal, proteção à propriedade intelectual, a cibersegurança e a segurança nacional. Cabe reiterar que a abertura do código não equivale à ausência de regulação, mas à sua reconfiguração. Trata-se da criação de uma abertura controlada, em que o Estado determina os limites e as formas de colaboração tecnológica, tanto nacional quanto internacional.

A adoção estratégica de tecnologias abertas, como Kylin e RISC-V, evidencia que a China não vê o *open source* como simples alternativa de baixo custo, mas como estratégia voltada a alavancar a própria tecnologia para a alcançar o objetivo regulatório da autonomia. O XV Plano Quinquenal demonstra que o código aberto está sendo institucionalizado como elemento jurídico, tecnológico e político da modernização nacional chinesa. Dessa forma, a importante lição para o Brasil é que a promoção do desenvolvimento, não a mera adoção, do *open source*, passa a constituir uma base estruturante de soberania digital e autonomia tecnológica.

1.3.2 A Suite Numérique*: reconstruir a soberania digital no setor público francês por meio do* open source

Apesar de a Europa carecer de iniciativas capazes de construir concretamente a soberania digital, cabe ressaltar que a França se consolidou como um dos países mais sensíveis à soberania digital e mais proativos para alcançar tal objetivo. Entre as iniciativas mais recentes está a Suite Numérique[66], um ecossistema de ferramentas colaborativas e de produtivi-

66 FRANÇA. **LaSuite : l'espace de travail collaboratif**, LaSuite : l'espace de travail collaboratif. Disponível em: <https://www.numerique.gouv.fr/offre-accompagnement/expertise-suite-num%C3%A9rique/>. Acesso em: 4 dez. 2025.

dade desenvolvido especificamente para a administração pública francesa, baseado em software livre, padrões abertos e infraestrutura controlada nacionalmente.[67] O projeto surgiu da percepção de que órgãos governamentais dependiam de maneira excessiva de soluções proprietárias estrangeiras, como Microsoft Office, Teams, Google Workspace ou Zoom.

Como destacaremos no capítulo 3, essa dependência representa riscos relevantes para a proteção de dados pessoais e cibersegurança, a confidencialidade de informações sigilosas, a interoperabilidade, a inovação e a concorrência, e se torna particularmente prejudicial especialmente diante de leis extraterritoriais e de debates sobre o uso de plataformas globais em ambientes sensíveis do Estado. Diante desse cenário, o governo francês decidiu adotar uma estratégia ativa: em vez de apenas ajustar contratos ou ampliar exigências de conformidade, optou por fomentar o desenvolvimento de alternativas abertas, auditáveis e sob controle nacional.

A Suite Numérique nasceu com o propósito de fortalecer a autonomia tecnológica do Estado, reduzir a exposição a fornecedores estrangeiros, ampliar a proteção de dados sensíveis e promover maior interoperabilidade entre ferramentas públicas. Ao priorizar padrões abertos e software livre, o governo buscou evitar o bloqueio tecnológico e garantir que a evolução das ferramentas fosse guiada pelas necessidades do setor público, e não por ciclos comerciais de grandes corporações. Outra ambição relevante da iniciativa foi o estímulo ao ecossistema digital francês, mobilizando empresas locais, comunidades de software livre e centros de pesquisa na construção de soluções modernas e competitivas.

O núcleo da Suite Numérique é o Docs, um editor colaborativo avançado inspirado na experiência de plataformas como Notion e Google Docs. Ele permite edição em tempo real, exportação em diversos formatos, sincronização offline, controle granular de acessos e ainda incorpora funcionalidades de inteligência artificial para geração, resumo, tradução e revisão de conteúdo, sempre dentro de uma infraestrutura controlada pelo Estado francês. A Suite inclui também outras ferramentas importantes, como o Visio, uma solução soberana para videoconferências hospedada em servidores nacionais; o Nextcloud, utilizado como base de armazena-

67 **Work with La Suite numérique**. Disponível em: <https://lasuite.numerique.gouv.fr/en>. Acesso em: 17 nov. 2025.

mento e sincronização de arquivos; o OnlyOffice ou LibreOffice para edição de documentos; e o Matrix, empregado para comunicação segura entre órgãos públicos. A integração dessas ferramentas cria um ambiente digital completo, capaz de substituir plataformas proprietárias amplamente utilizadas no governo.

O desenvolvimento da Suite Numérique segue um modelo colaborativo que combina participação direta de agências governamentais, contribuições de comunidades de software livre, envolvimento de empresas francesas e apoio de laboratórios de pesquisa. Esse arranjo é particularmente interessante porque visa a garantir transparência, auditabilidade e independência tecnológica, permitindo que o Estado acompanhe e oriente a evolução das soluções. A abertura do código e a possibilidade de auditoria pública reforçam a confiança e evitam dependência de fornecedores específicos.

A experiência francesa demonstra que a soberania digital pode se traduzir em produtos concretos e amplamente utilizados, e não apenas em diretrizes normativas. Nessa direção, vale ressaltar que a Suite Numérique já está em adoção progressiva em ministérios, prefeituras, escolas e administrações regionais, promovendo maior controle sobre fluxos de trabalho, comunicação e armazenamento de dados governamentais. Além de reduzir riscos jurídicos e de segurança, a iniciativa fortalece o setor tecnológico local, cria condições para inovação contínua e demonstra que um Estado pode moldar suas próprias ferramentas digitais de acordo com seus interesses estratégicos.

Para países que buscam avançar na autonomia tecnológica, como o Brasil, a experiência francesa oferece uma lição clara: a soberania digital depende de ação direta e investimento em soluções abertas e auditáveis, e não apenas de regulação[68]. A França mostra que, quando há decisão política e coordenação institucional, é possível construir alternativas modernas, eficientes e alinhadas ao interesse público, diminuindo a dependência de plataformas estrangeiras e aumentando a capacidade do Estado de controlar seus próprios sistemas e dados.

Para o Brasil, essa alternativa revela-se não apenas desejável, mas tecnicamente viável. Assim, cabe frisar que a Rede Nacional de Ensino e Pesquisa (RNP) já disponibiliza as ferramentas fundamentais para a es-

68 Esses pontos serão analisados no capítulo 4.

truturação de uma plataforma nacional de comunicação e colaboração profissional comparável com elementos da Suite Numérique, baseada em tecnologias de código aberto e capaz de integrar e suportar IA brasileira. Porém, cabe ressaltar também que, embora o Sistema RNP já proveja conectividade avançada e softwares de colaboração para a rede acadêmica, o sistema ainda depende de serviços de computação em nuvem estrangeiros.[69] Sua adoção em escala pela administração pública federal, aliada à expansão de capacidade computacional sob jurisdição nacional, permitiria reduzir a subordinação a plataformas externas, fortalecer a soberania digital e oferecer um importante exemplo ao nível regional.

1.4 Cibersegurança, ciber-resiliência e segurança nacional: alicerce da soberania digital

A cibersegurança, que inclui o conceito de ciber-resiliência[70] e é essencial para garantir a segurança nacional, representa uma dimensão instrumental essencial para alcançar a soberania digital.[71] Ser soberano, no ambiente digital, significa ser capaz de proteger e controlar as infraestruturas críticas que garantem a continuidade do Estado, a segurança de seus cidadãos e a estabilidade de sua economia e democracia. Isso abrange não

69 BR, Núcleo de Informação e Coordenação do Ponto; EVANGELISTA, Rafael de Almeida; RABELLO, Maricy, **Educação em um cenário de plataformização e economia de dados: soberania e infraestrutura**, São Paulo, SP: Núcleo de Informação e Coordenação do Ponto BR, 2023.

70 O conceito de ciber-resiliência refere-se à capacidade de um sistema, organização ou infraestrutura de informação de continuar operando de forma aceitável mesmo diante de incidentes cibernéticos, falhas, ataques ou ameaças, e recuperar-se ou adaptar-se rapidamente para restaurar a funcionalidade, preservar a integridade dos dados e assegurar a continuidade dos serviços essenciais. Trata-se de um conceito complementar à cibersegurança preventiva, envolvendo a preparação, adaptação, mitigação, resposta e capacidade de recuperação. Reconhecendo que nem todos os riscos cibernéticos podem ser evitados antecipadamente, a ciberresiliência é o mecanismo pelo qual se assegura a resistência e a continuidade dos sistemas digitais, sendo portanto essencial para garantir a soberania tecnológica. ARAUJO, Misael Sousa de; MACHADO, Bruna Aparecida Souza; PASSOS, Francisco Uchoa. Resilience in the Context of Cyber Security: A Review of the Fundamental Concepts and Relevance. **Applied Sciences**, v. 14, n. 5, p. 2116, 2024; **Handbook for Cyber Stress Tests | ENISA**. Disponível em: <https://www.enisa.europa.eu/publications/handbook-for-cyber-stress-tests>. Acesso em: 3 dez. 2025.

71 BELLI, Cibersegurança; BELLI, Luca et al. **Governança e regulação da cibersegurança no Brasil**, [s.l.: s.n.], 2025.

apenas a defesa das redes eletrônicas e dos bancos de dados que armazenam informações sensíveis, mas também a proteção das infraestruturas políticas e administrativas que sustentam a governança nacional.[72]

Como destacado em publicações dedicadas ao assunto, a cibersegurança é um conjunto de iniciativas voltadas à segurança de ativos digitais, incluindo pessoas, diante de riscos cibernéticos.[73] As medidas de soberania digital e de cibersegurança desempenham um papel altamente complementar: o estudo da tecnologia é essencial para identificar e prevenir usos abusivos, enquanto o desenvolvimento tecnológico contribui para a criação de soluções mais seguras. A pesquisa e desenvolvimento são instrumentais para aprimorar a qualidade da regulação que, por sua vez, desempenha um papel fundamental no equilíbrio do setor, definindo os padrões mínimos a serem implementados para facilitar o desenvolvimento e adoção sustentável das tecnologias digitais, reduzindo e – idealmente – evitando riscos e, caso seja necessário, sancionando comportamentos abusivos.

Portanto, a segurança digital deve ser entendida como dimensão constitutiva da soberania digital, e ambas são essenciais para garantir a segurança nacional, considerando que a economia, a sociedade e a democracia brasileira dependem do bom funcionamento de infraestruturas digitais. Em um cenário no qual ataques cibernéticos, espionagem digital, roubo de propriedade intelectual e desinformação são utilizados como instrumentos de poder geopolítico, a incapacidade de proteger ativos digitais e processos democráticos dependentes de tais ativos equivale à vulnerabilidade estrutural do próprio Estado. Em outras palavras, não há soberania possível sem o domínio e a resiliência das infraestruturas digitais das quais nossa sociedade, economia e democracia dependem.[74]

Assim, nesse âmbito, a segurança da informação constitui o fio condutor da cibersegurança, sendo central para a proteção dos ativos digitais de ameaças externas bem como internas. A informação, seja pessoal ou

72 BELLI, Luca et al**. Cibersegurança: uma visão sistêmica rumo a uma Proposta de Marco Regulatório para um Brasil Digitalmente soberano**, Rio de Janeiro, RJ: FGV Direito Rio, 2023.

73 *Ibid*.; ITU-T - INTERNATIONAL TELECOMMUNICATION UNION, Recommendation ITU-T X.1205: Overview of Cybersecurity.

74 BELLI, Luca et al. **Governança e regulação da cibersegurança no Brasil**.

não, passou a ser um ativo estratégico essencial[75], com papel decisivo na gestão de governos, empresas e serviços, refletindo a emergência de um novo paradigma tecnoeconômico[76] centrado em dados e conhecimento, no âmbito do qual a cibersegurança é indissociável de soberania.

Nesse contexto, as políticas nacionais de cibersegurança devem ser concebidas, ao mesmo tempo, como estratégias de empoderamento cidadão, desenvolvimento nacional e segurança nacional, alinhando instituições acadêmicas, setor produtivo, forças armadas e sociedade civil em uma arquitetura multissetorial voltada à mitigação dos riscos e ao desenvolvimento de capacidades de defesa e resiliência.

Tal arquitetura deve contemplar, entre outros aspectos: (i) a definição de padrões mínimos de segurança da informação; ii) a proteção de infraestruturas críticas e serviços essenciais; iii) a criação de sistemas de monitoramento, prevenção e resposta a incidentes cibernéticos, inclusive estabelecendo as competências regulatórias de normatização, fiscalização e aplicação de sanções; iv) o estímulo à indústria nacional e à preferência de produtos e serviços capazes de garantir o respeito à legislação nacional e ao controle técnico-operacional, insulando as infraestruturas críticas de interferências estrangeiras v) a garantia da coordenação e comunicação entre órgãos reguladores setoriais, atores operacionais e entidades privadas; vi) a articulação de mecanismos de resposta a incidentes e prevenção de riscos, em conjunto com as Equipes de Resposta a Incidentes de Segurança em Sistemas Computacionais (conhecidas como CSIRTs, do inglês *Computer Security Incident Response Teams*) e os Centros de Compartilhamento e Análise de Informações sobre Cibersegurança (conhecidos como ISACs, do inglês ou *Information Sharing and Analysis Centers*); vii) fomentar capacitação, educação e cultura de cibersegurança, fortalecendo a educação digital e a preparação de profissionais; e viii) facilitar a integração entre setores, promovendo harmonização normativa e colaboração interinstitucional.[77]

---

75 ORSI, Fabienne; CORIAT, Benjamin. The New Role and Status of Intellectual Property Rights in Contemporary Capitalism. **Competition & Change**, v. 10, n. 2, p. 162-179, 2006; CORIAT, Benjamin; WEINSTEIN, Olivier, Intellectual Property Right Regimes, Firms and the Commodification of Knowledge, **SSRN Electronic Journal**, 2009.

76 PEREZ, C. Technological revolutions and techno-economic paradigms. **Cambridge Journal of Economics**, v. 34, n. 1, p. 185-202, 2010.

77 BELLI, Luca et al. **Governança e regulação da cibersegurança no Brasil**.

Do ponto de vista jurídico, a cibersegurança se articula, ainda, com o dever positivo do Estado de proteger direitos fundamentais de seus cidadãos, como a privacidade, a autodeterminação informativa, a liberdade de expressão, a educação e a participação na vida pública. Sem cibersegurança, esses direitos podem ser facilmente comprometidos por atores maliciosos. Assim, a cibersegurança é simultaneamente instrumento de soberania e condição de exercício da cidadania.[78]

Por fim, a interconexão global e a (inter)dependência de produtos e serviços digitais estrangeiros exigem que a cibersegurança seja também tratada em termos de soberania compartilhada, uma vez que vulnerabilidades em um país podem gerar efeitos transfronteiriços. Nesse sentido, a definição de padrões internacionais de cibersegurança, cibercrime, governança de dados, cooperação e resposta a incidentes é indispensável. No entanto, essa cooperação não pode prescindir da capacidade nacional mínima de proteger seus ativos digitais necessários para o bom funcionamento de sua infraestrutura crítica e serviços essenciais: caso contrário, o Estado deixa de ser soberano.

Assim, a ciber-resiliência emerge como um componente essencial da cibersegurança e, consequentemente, da soberania digital, sobretudo em um contexto global em que infraestruturas digitais críticas – como *data centers*, redes de comunicação eletrônica, cabos submarinos, redes elétricas e plataformas digitais – representam alvos estratégicos em potenciais conflitos ou tentativas de coerção tecnológica.[79] A resiliência da infraestrutura nacional confere credibilidade à capacidade de dissuasão de um Estado, assegurando que sistemas civis continuem operacionais mesmo sob ataques ou tensões externas.

Sob essa ótica, a ciber-resiliência não se limita à adoção de boas práticas de segurança ou à prevenção de invasões. Ela envolve a construção de uma capacidade estruturada e sistêmica de absorver choques, adaptar-se a incidentes e recuperar operações críticas – seja após ataques cibernéticos, crises geopolíticas, falhas de suprimento ou interrupções de infraestrutura. Infraestruturas digitais robustas, com redundância, isolamento, governança transparente e controle sobre cadeias de suprimento tecnológico,

78 BELLI, Luca et al. **Cibersegurança**.

79 Esses riscos serão explorados nas seções 3.1, 3.6 e 3.7.

funcionam como alicerce da soberania nacional. A interrupção deliberada de comunicações, energia ou tráfego de dados pode paralisar serviços essenciais, comprometer a soberania estatal e desorganizar a economia e a administração pública.

Cabe frisar que a cibersegurança deve ser concebida como instrumento de suporte à soberania nacional e, consequentemente, à soberania digital, garantindo a proteção de infraestruturas críticas e a resiliência dos sistemas nacionais, com o intuito de fortalecer e nunca prejudicar o pleno gozo de direitos fundamentais. Assim, é essencial evitar a securitização desproporcional do espaço digital, que poderia transformar a cibersegurança e a soberania digital em justificativas para a adoção de medidas repressivas e restritivas de direitos.[80] A cibersegurança deve, antes, cumprir sua função primordial de identificar vulnerabilidades, mitigar riscos e ampliar oportunidades de inovação e desenvolvimento, fortalecendo a confiança pública e a autonomia tecnológica. Nessa perspectiva, a regulação deve equilibrar a necessidade de proteção com a preservação de liberdades, de modo que a defesa das infraestruturas digitais não se converta em pretexto para práticas de vigilância abusiva ou restrições desproporcionais à cidadania digital.

Em síntese, a cibersegurança é o pilar que sustenta a soberania digital e a soberania digital, por sua vez, é instrumento essencial para garantir a cibersegurança. Sem cibersegurança, a autodeterminação (informativa), o livre desenvolvimento de uma nação no ambiente digital e, em última instância, a soberania nacional tornam-se ilusões. Alavancando a cibersegurança, torna-se possível construir uma autonomia tecnológica robusta, capaz de proteger direitos, assegurar desenvolvimento e reforçar a posição soberana do Estado, e enxergar a tecnologia como uma oportunidade de desenvolvimento sustentável para pessoas e empresas.[81]

---

80 SHCHERBOVICH, Andrey. Data Protection and Cybersecurity Legislation of the Russian Federation in the Context of the "Sovereignization" of the Internet in Russia. In: BELLI, Luca (Org.). **CyberBRICS: Cybersecurity Regulations in the BRICS Countries**. Cham: Springer International Publishing, 2021, p. 67-131. IGNATOV, Alexander; KERIMI, Danil, Russia's securitised approach to AI sovereignty. **The African Journal of Information and Communication (AJIC)**, n. 35, p. 1-11, 2025.

81 BELLI, Luca; GALDINO DE MAGALHÃES SANTOS, Larissa. Editorial: Toward a BRICS stack? Leveraging digital transformation to construct digital sovereignty in the BRICS countries. **Computer Law & Security Review**, v. 55, p. 106064, 2024.

1.5 As bases constitucionais da soberania tecnológica no Brasil

A evolução do debate sobre soberania digital na direção da garantia da autonomia tecnológica é particularmente relevante, não somente porque tal aspiração é mais que legítima, mas, sobretudo, porque, diferentemente da União Europeia e de muitos dos países que integram o bloco, no Brasil a autonomia tecnológica é um objetivo constitucionalmente protegido.[82]

A soberania digital, embora não expressamente mencionada na Constituição Federal de 1988, encontra fundamento em diversos dispositivos constitucionais que consagram a soberania nacional, o desenvolvimento tecnológico e a proteção da privacidade como pilares estruturantes da República. O artigo 1º, inciso I, estabelece a soberania como um dos fundamentos do Estado brasileiro, conferindo-lhe o poder supremo sobre seu território e sua autodeterminação no cenário internacional. No contexto digital, tal princípio implica a necessidade de o país dispor de autonomia sobre suas infraestruturas tecnológicas, redes de comunicação e sistemas de armazenamento de dados, de modo a evitar a dependência de tecnologias estrangeiras que possam comprometer sua segurança e autodeterminação.

Os objetivos fundamentais da República, dispostos no artigo 3º, incisos II e III, reforçam a importância da soberania digital ao vincular o desenvolvimento nacional e a redução das desigualdades sociais à promoção da inovação e da inclusão tecnológica. O desenvolvimento econômico e social contemporâneo depende diretamente da capacidade de um país em gerar e controlar conhecimento tecnológico, especialmente no campo digital. A ampliação da infraestrutura tecnológica nacional e o incentivo à pesquisa aplicada permitem não apenas o crescimento econômico, mas também a democratização do acesso à informação, promovendo maior equidade social e regional. A proteção da privacidade e do sigilo das comunicações, garantida pelo artigo 5º, incisos X e XII, revela outro aspecto essencial da soberania digital: a segurança informacional dos cidadãos e do próprio Estado.

82 *Ibid*.

Como destacaremos na próxima seção, o controle sobre dados pessoais requer um aparato tecnológico e normativo capaz de garantir a segurança, a proteção e a capacidade de aproveitar o valor das informações. Nesse sentido, a soberania digital se manifesta também como soberania informacional, garantindo que o tratamento de dados de cidadãos brasileiros obedeça a parâmetros nacionais e a princípios constitucionais de dignidade e liberdade, e que os benefícios econômicos e científicos de tal tratamento sejam redistribuídos equitativamente, no interesse nacional.

Por fim, porém não menos importantes, os artigos 218 e 219 conferem base jurídica direta à promoção da ciência, tecnologia e inovação como instrumentos de fortalecimento da autonomia tecnológica do país. O texto constitucional reconhece que o desenvolvimento científico e a capacitação tecnológica são essenciais para o bem-estar social e a independência econômica, devendo o Estado promover políticas públicas que incentivem a inovação e a produção tecnológica nacional. Assim, a soberania digital, sustentada por esses preceitos constitucionais, representa não apenas uma exigência técnica, mas um imperativo jurídico para a consolidação da soberania nacional em um contexto de crescente interdependência digital e global.

Nesse sentido, o Brasil tem uma clara vantagem competitiva comparado com outros países onde a soberania digital e soberania em IA são conceitos artificiais sem embasamento jurídico claro: no Brasil, tais conceitos encontram amparo constitucional diretamente na autonomia tecnológica, nos termos da Constituição:

> Art. 219. O mercado interno integra o patrimônio nacional e será incentivado de modo a viabilizar o desenvolvimento cultural e socioeconômico, o bem-estar da população e a autonomia tecnológica do País, nos termos de lei federal.
> Parágrafo único. O Estado estimulará a formação e o fortalecimento da inovação nas empresas, bem como nos demais entes, públicos ou privados, a constituição e a manutenção de parques e polos tecnológicos e de demais ambientes promotores da inovação, a atuação dos inventores independentes e a criação, absorção, difusão e transferência de tecnologia.

Assim, a soberania digital, sustentada por esses preceitos constitucionais, representa não apenas uma exigência técnica, mas um imperativo

jurídico para a consolidação da soberania nacional em um contexto de crescente interdependência digital e global. Para se alcançar tal autonomia em relação à IA, é necessário se adotar estratégias, políticas e mecanismos de governança e regulação aptos a entender e gerenciar as (inter)dependências e as potenciais vulnerabilidades existentes entre os diferentes elementos que dão suporte ao funcionamento dos sistemas de IA.

Tais elementos, que serão explorados no próximo capítulo, podem ser considerados como "Facilitadores Essenciais da Soberania em IA"[83] e são: dados, capacidade algorítmica, capacidade computacional, conectividade significativa, energia elétrica, recursos humanos capacitados, cibersegurança e um marco legislativo capaz de regular os riscos da IA de maneira efetiva, bem como a chamada resiliência cognitivo-informacional. Como demonstra nossa pesquisa[84], esses facilitadores estão interligados e a compreensão acerca desta conexão se revela essencial para implementar a regulação de maneira eficiente e efetiva.

1.5.1 O papel do direito fundamental à autodeterminação (informativa) como base da soberania digital

A soberania digital, enquanto conceito jurídico e político, deve ser compreendida, em primeiro lugar, como uma extensão do direito fundamental à autodeterminação dos povos e, em segundo lugar, como uma operacionalização do direito fundamental à autodeterminação informativa. O direito à autodeterminação dos povos, consagrado no Artigo 1º da Carta das Nações Unidas e reiterado tanto no Pacto Internacional sobre Direitos Civis e Políticos (PIDCP) quanto no Pacto Internacional sobre Direitos Econômicos, Sociais e Culturais (PIDESC), estabelece que "todos os povos têm direito à autodeterminação" e que, em virtude deste direito, "determinam livremente seu estatuto político e asseguram livremente seu

83 BELLI, Luca. To Get Its AI Foothold, Brazil Needs to Apply the Key AI Sovereignty Enablers (KASE), 2023; BELLI; GASPAR (Orgs.). **The Quest for AI Sovereignty, Transparency and Accountability**; BELLI, Luca, Soberania em Inteligência Artificial: O que é e quais facilitadores essenciais podem tornar o Brasil um país soberano em IA?, *in*: VILLAS BÔAS CUEVA, Ricardo *et al* (Orgs.), **Inteligência Artificial e Regulação**, Rio de Janeiro: Gen Jurídico, 2024.

84 BELLI; GASPAR (Orgs.). **The Quest for AI Sovereignty, Transparency and Accountability**.

desenvolvimento econômico, social e cultural".[85] Assim, a soberania digital deve ser vista como uma dimensão tecnológica da autodeterminação dos povos no século XXI.

A autodeterminação dos povos, tradicionalmente discutida sob sua vertente externa – isto é, a independência territorial e política em relação a potências estrangeiras – deve ser igualmente concebida em sua vertente interna: a capacidade de um povo de definir, organizar e perseguir autonomamente o seu próprio desenvolvimento econômico, social e cultural. Essa dimensão interna torna-se particularmente relevante no domínio digital, uma vez que a escolha, o desenvolvimento e a adoção independente de tecnologias constituem, hoje, condições estruturais para o pleno exercício da autodeterminação.

Essa concepção encontra eco na noção de "Boa Soberania Digital"[86], que compreende a soberania não como monopólio do Estado, mas como possibilidade de qualquer entidade, seja pública, privada ou comunitária – exercer autonomia digital enquanto for capaz de compreender, dominar e utilizar as tecnologias digitais em benefício próprio, inclusive desenvolvendo novas soluções. Nessa visão, a soberania digital é tanto uma função da capacidade de compreender a tecnologia quanto do poder de se apropriar de seus benefícios para o progresso coletivo.

Para complementar esta perspectiva, a soberania digital, na sua concepção de soberania de dados, que será explorada na seção seguinte, visa a operacionalizar o direito fundamental à autodeterminação informativa. Conforme destacado pela jurisprudência da Corte Interamericana de Direitos Humanos (CIDH) no caso CAJAR v. Colômbia, a autodeterminação informativa é um direito fundamental autônomo, e o Estado deve desempenhar um papel ativo no auxílio aos titulares, por meio de mecanismos que permitam o pleno gozo desses direitos.[87]

---

85 Cabe lembrar que o PIDCP foi promulgado no Brasil pelo Decreto nº 592, de 6 de julho de 1992, enquanto o PIDESC foi promulgado pelo Decreto n.º 591, de 6 de julho de 1992.

86 BELLI, Luca. **Building Good Digital Sovereignty through Digital Public Infrastructures and Digital Commons in India and Brazil**; JIANG; BELLI (Orgs.). **Digital Sovereignty in the BRICS Countries**.

87 BELLI, Luca et al. **Transferência internacional de dados pessoais na América Latina: rumo à harmonização de normas**, 1a edição. Rio de Janeiro, RJ: Lumen Juris, 2024.

Tal direito, consagrado no artigo 2 da Lei Geral de Proteção de Dados (LGPD), foi concebido como extensão do livre desenvolvimento da personalidade, afirmando que os indivíduos têm poder de controle sobre suas informações como condição para sua autodeterminação pessoal. No entanto, a autodeterminação informativa transcende a proteção individual e precisa ser enxergada também no sentido coletivo, ou seja, do direito de um Estado-nação de se beneficiar dos dados que produz.[88] A ligação entre autodeterminação informativa e soberania digital é direta: ambos afirmam que autonomia – individual ou coletiva – exige controle sobre os dados e tecnologias que moldam a vida contemporânea.

Portanto, para garantir o pleno gozo do direito fundamental à autodeterminação (informativa), o país precisa reconhecer os riscos e o potencial estratégico das tecnologias digitais, definindo uma postura coordenada e estratégica que articule políticas públicas de educação, pesquisa, desenvolvimento industrial, expansão de infraestrutura digital e governança de dados de modo integrado e com objetivo explícito de fortalecimento da soberania digital. O déficit de uma política consciente tem resultado em uma posição de vulnerabilidade, caracterizada por uma dependência excessiva de tecnologias estrangeiras, que limita e prejudica – ou até incapacita e nulifica – o direito à autodeterminação informativa.

Torna-se, assim, urgente assumir uma política assertiva de soberania digital que não se confunda com protecionismo, mas que seja encarada como pilar da pesquisa, desenvolvimento e regulação nacional, com o objetivo de consagrar a autonomia tecnológica do Brasil.

1.6 Soberania em IA é soberania sobre dados

Continuamos a proclamar em termos abstratos e retóricos que os dados são "o petróleo do século XXI", mas, na realidade da vida concreta, continuamos fornecendo uma espécie de concessão gratuita para explorar essa riqueza *ad infinitum*. Com a difusão da IA generativa, ingressamos

88 BELLI, Luca; GASPAR, Walter B.; JASWANT, Shilpa Singh. Data sovereignty and data transfers as fundamental elements of digital transformation: Lessons from the BRICS countries. **Computer Law & Security Review**, v. 54, p. 106017, 2024.

em uma dinâmica ainda mais perversa[89]: o usuário transforma-se em trabalhador não remunerado, fornecendo informações de alto valor – sejam dados pessoais, oriundos da administração pública, do Judiciário, ou desenvolvidos por pesquisadores e educadores nacionais – que alimentam sistemas de IA estrangeiros. Esses dados se tornam essenciais para subsidiar o desenvolvimento de produtos e serviços de IA, os quais nos são posteriormente vendidos pelas mesmas pouquíssimas empresas de tecnologia, tipicamente norte-americanas.

Desde as revelações de Edward Snowden, em 2013, as maiores empresas processadoras de dados pessoais são conhecidas por sua cooperação em atividade de espionagem global, lideradas pela National Security Agency estadunidense.[90] Além disso, recentemente, as mesmas empresas manifestaram total submissão à nova administração Trump, revelando sua clara dependência da pendularidade política dos EUA.[91] Adicionalmente, apesar de determinar uma ampla gama de externalidades negativas – do ponto de vista social, econômico e político – e concentrar lucro e capacidade quase-soberanas[92], essas mesmas empresas se beneficiam de tributação extremamente vantajosa e limitada[93].

Esse cenário está bem distante de uma situação de soberania e ainda mais da cibersegurança que o País precisa.[94] Ao contrário, políticas de soberania digital são essenciais para (re)construir autodeterminação, cibersegurança e controle sobre ativos digitais ao invés de ser controlados por

89 BELLI, Luca. **Opinião: IA generativa "grátis" é a nova fronteira da colonização digital**, Folha de S.Paulo. Disponível em: <https://www1.folha.uol.com.br/tec/2025/09/ia-generativa-gratis-e-a-nova-fronteira-da-colonizacao-digital.shtml>. Acesso em: 5 mar. 2026.

90 MACASKILL, Ewen et al. **NSA files decoded: Edward Snowden's surveillance revelations explained**. The Guardian. Disponível em: <https://www.theguardian.com/world/interactive/2013/nov/01/snowden-nsa-files-surveillance-revelations-decoded>. Acesso em: 2 dez. 2025.

91 MAGEE, Tamlin. **Big tech's support for Trump isn't a moral about-face – it's business**, Raconteur. Disponível em: <https://www.raconteur.net/technology/tech-tribute-trump-oped>. Acesso em: 11 nov. 2025.

92 BELLI, Luca. Structural Power as a Critical Element of Social Media Platforms' Private Sovereignty.

93 Uma análise detalhada da atual ineficiência do regime tributário pátrio no que diz respeito à tributação de modelos extrativistas de dados pessoais se encontra em BELLI, Luca *et al*, Proteção de dados, tributação de dados e equidade de dados: equilíbrio entre valores, riscos e obrigações. **CPDP LatAm Discussion Papers**, 2025.

94 BELLI, Luca et al, **Cibersegurança**.

meio de sistemas de IA e tecnologias estrangeiras das quais nos tornamos perigosamente dependentes.[95] Neste sentido, é necessário frisar que soberania em IA não pode prescindir de soberania sobre dados.[96]

Com base na nossa pesquisa em soberania digital[97], podemos definir a soberania de dados como a aptidão para compreender o funcionamento de tecnologias que processam dados, saber desenvolver tais tecnologias e regulá-las efetivamente.[98] Tal capacidade é essencial para conseguir romper com modelos extrativistas que reproduzem lógicas coloniais na extração de dados pessoais e outras informações valiosas por meio de tecnologia digital. Nada obstante, é importante enfatizar que a mera "localização de dados", ou seja, o mero armazenamento de dados no território nacional não é, por si só, garantia de desenvolvimento ou inovação, que precisam de estratégias sólidas, política industrial focada, e definição de papéis e responsabilidades precisos para serem promovidos.[99] Daí a ideia de que simplesmente atrair *data centers* para o país não seja, necessariamente, a mais soberana das soluções, caso não venha acompanhada de outros elementos.

Como destacado por Lastres, Cassiolato e Dantas, a crescente centralidade dos dados como insumo estratégico no capitalismo contemporâneo torna indispensável que países desenvolvam capacidades próprias para explorar economicamente esses recursos, sob pena de aprofundar formas de dependência típicas do chamado "colonialismo digital".[100] À medida que dados e informações passam a constituir matéria-prima fundamental para inovação, inteligência artificial, serviços digitais e tomada de decisão, o controle sobre sua produção, tratamento e circulação deixa de ser apenas um tema tecnológico e se converte em questão de soberania.

---

95 BELLI, Luca; JIANG, **Conclusion**.

96 BELLI, Luca; GASPAR; JASWANT. **Data sovereignty and data transfers as fundamental elements of digital transformation.**

97 JIANG; BELLI (Orgs.). **Digital Sovereignty in the BRICS Countries**.

98 BELLI; GASPAR; JASWANT, Data sovereignty and data transfers as fundamental elements of digital transformation.

99 Idem.

100 LASTRES, Helena Maria Martins; CASSIOLATO, José Eduardo; DANTAS, Marcos (Orgs.). **ECONOMIA POLÍTICA DE DADOS E SOBERANIA DIGITAL: conceitos, desafios e experiências no mundo**, Avaré, SP: Editora Contracorrente, 2025.

Quando a infraestrutura digital, as plataformas e os fluxos de dados ficam concentrados nas mãos de grandes corporações transnacionais, países do Sul Global tornam-se meros fornecedores de matéria-prima informacional, sem participação significativa nos ganhos econômicos, tecnológicos e geopolíticos que ela gera. Assim, construir políticas industriais robustas para estimular o acesso, o processamento, a análise e uso econômico de dados é condição essencial para evitar uma nova configuração de dependência, garantir autonomia estratégica e participar de forma ativa, ao invés que subordinada, da economia digital global.[101]

Ser soberano sobre dados também não significa simplesmente adotar leis de proteção de dados: a soberania depende da habilidade para desenvolver tecnologias baseadas em dados e para implementar efetivamente as normas que as regulam, e ambas as habilidades podem ser realizadas concretamente somente quando existir a compreensão do funcionamento das tecnologias que coletam e processam dados. Contudo, tal ideal ainda está distante da realidade da maioria global. Fortalecer esse domínio é crucial tanto para a proteção individual de dados quanto para a promoção de autonomia tecnológica nacional; porém, como destacaremos em seguida, é somente uma dimensão da soberania sobre dados.

Conforme destacado na seção anterior, o recente precedente interamericano consagra a autodeterminação informativa como direito fundamental autônomo e prescreve a obrigação estatal de permitir o pleno gozo de tal direito. O controle sobre como dados pessoais são tratados é essencial para a dignidade do indivíduo; entretanto, é importante frisar que a autodeterminação informativa transcende a proteção individual e deve ser considerada também na sua dimensão coletiva.

É justamente a consideração de tal dimensão coletiva da autodeterminação informativa[102] que nos permite reconhecer a centralidade dos dados para o desenvolvimento nacional, e exige que a governança de dados reconheça o valor econômico dos dados, de forma a promover o interesse público, o desenvolvimento nacional e assegurar democracia e a cibersegurança das infraestruturas digitais. Nessa perspectiva, dados são um fa-

101 *Ibid*.

102 BELLI; GASPAR; JASWANT. Data sovereignty and data transfers as fundamental elements of digital transformation.

tor de produção[103] equiparável a trabalho, capital e terra, e a regulação de dados deve servir ao interesse público, consolidando a democracia, protegendo infraestruturas digitais e promovendo desenvolvimento nacional.

Portanto, ao considerar a soberania dos dados sob a perspectiva da autodeterminação, podemos identificar uma dimensão individual baseada na capacidade dos sujeitos dos dados de exercer controle sobre seus dados, assim como uma dimensão coletiva. Como destacamos na seção 1.5.1, essa última dimensão consiste na capacidade de exercer o direito fundamental de determinar livremente e buscar seu desenvolvimento econômico, social e cultural. Mais amplamente, devemos lembrar que a dimensão informacional do direito à autodeterminação é uma evolução relativamente recente do conceito e que tal direito tem sido tradicionalmente considerado em sua concepção coletiva – e consagrada em sua conotação coletiva como o primeiro artigo tanto da Carta das Nações Unidas quanto dos Pactos Internacionais dos Direitos Humanos.

Assim, as prerrogativas embasadas no direito fundamental à autodeterminação incluem a capacidade de escolher, desenvolver e adotar tecnologias digitais de forma independente e decidir como os dados (pessoais) podem ser coletados, processados e armazenados, além de ter voz sobre como e onde os dados devem gerar valor.[104]

Para alcançar esta finalidade, não basta criar normas ou agências especializadas na proteção de dados pessoais. É necessário facilitar a pesquisa e o desenvolvimento das infraestruturas de hardware e software que possam permitir ao ecossistema nacional de dados florescer e ser aproveitado pelos atores públicos e privados nacionais, garantindo o respeito da legislação na-

---

103 Esse entendimento representa a base estruturante da concepção chinesa de dados, como destacaremos na seção 1.6. Nesse sentido, após a promulgação da Estratégia Nacional de Big Data em 2015, durante o 18º Congresso do Partido Comunista Chinês, o governo da China instituiu, a partir do 19º Comitê Central, em 2019, um arcabouço regulatório e de política industrial fundamentado na concepção dos dados como fator de produção. Ver XINHUA NEWS AGENCY. **Decision of the Central Committee of the Communist Party of China on Several Major Issues Concerning Upholding and Improving the Socialist System with Chinese Characteristics and Promoting the Modernization of the National Governance System and Governance Capacity**. Gov.CN. Disponível em: <https://www.gov.cn/zhengce/2019-11/05/content_5449023.htm>. Acesso em: 11 nov. 2025.

104 BELLI; GASPAR; JASWANT. **Data sovereignty and data transfers as fundamental elements of digital transformation.**

cional. Nesse sentido, o uso de infraestruturas de coleta e troca de dados, como os *data exchanges* estabelecidos na China ou os *data spaces* vislumbrados pela União Europeia, parece ser uma estratégia promissora para estimular a valorização e uso de dados nacionais, especialmente em setores como agropecuária, transportes, entre outros, nos quais amplas bases de dados já são produzidas e não necessariamente exploradas.[105]

Além disso, a tributação precisa ser enxergada como estratégia regulatória[106] voltada a facilitar o exercício da autodeterminação informativa no sentido individual e coletivo. Como observamos em recente pesquisa, não existem no Brasil políticas tributárias que atuem como instrumentos regulatórios, capazes de incentivar boas práticas de governança, proteção de dados e segurança da informação, bem como de desestimular modelos de negócio baseados na extração ilimitada e na concentração de dados.[107]

Nesse sentido, cabe destacar a extração e exploração de vastos volumes de dados oriundos de países que compõem a parte da maioria global por corporações multinacionais de tecnologia que permanecem sem tributação, embora esses dados – especialmente conjuntos de dados locais de alta qualidade usados para treinamento de IA – gerem valor substancial.[108] Isso cria uma grande classe de ativos intangíveis não tributados, minando a tributação justa e a soberania fiscal. Além disso, as inovações derivadas do processamento de dados, muitas vezes protegidas por direitos de propriedade intelectual domiciliados em jurisdições de baixa tributação, escapam à tributação apropriada.

Como destacamos em outra pesquisa específica sobre tributação, proteção e equidade de dados, as autoridades fiscais atualmente não tribu-

---

105 Os *data exchanges* já operam comercialmente na China há quase uma década, sendo empresas públicas lucrativas que negociam dados sob forte supervisão estatal e foco em segurança nacional. Na Europa, os *data spaces* ainda estão em fase de implementação, buscando criar um ecossistema interoperável e soberano, centrado em privacidade e confiança. Os *data exchanges* serão explorados brevemente na seção 1.6. Os *data spaces* europeus não serão analisados porque, apesar de terem sido anunciados, de fato ainda não existem na prática, tendo somente experiências experimentais que dificilmente podem ser replicadas ou usadas como exemplos.

106 BELLI, Luca et al. Proteção de dados, tributação de dados e equidade de dados: equilíbrio entre valores, riscos e obrigações A pesquisa foi apresentada na conferência CPDP LatAm 2025. Uma versão preliminar se encontra disponível em https://cpdp.lat/pt-br/publicacoes/.

107 *Ibid*.

108 *Ibid*.

tam os dados brutos, nem os direitos de exploração de tais dados, concentrando-se em serviços digitais limitados ao usuário final, o que contradiz os princípios fundamentais de nexo e criação de valor no direito tributário internacional e facilita a erosão da base tributária e a transferência de lucros.[109] Além disso, as estruturas tributárias atuais não incentivam a conformidade com as leis nacionais de proteção de dados e segurança da informação, permitindo que grandes empresas com uso intensivo de dados externalizem os custos sociais e regulatórios enquanto se beneficiam de uma isenção fiscal tripla. Nesse sentido, sustenta-se a necessidade de vincular a tributação desses modelos extrativistas à promoção da justiça social e à efetividade do direito fundamental à proteção de dados.[110]

Por fim, além da necessidade de ser enxergada como a base infraestrutural do desenvolvimento nacional, a tecnologia pode se tornar uma poderosa aliada do direito no que diz respeito à governança de dados, por exemplo, por meio de infraestruturas públicas digitais (DPIs no acrônimo em língua inglesa) e protocolos técnicos para registro do consentimento e comunicação de requisições, como já feito de forma embrionária pelo *Data Empowerment and Protection Architecture* (DEPA)[111] da Índia. Apesar de o exemplo Indiano não ser isento de críticas[112], é interessante frisar que, por meio das DPIs, o Estado recupera um protagonismo atrelado ao desenvolvimento de infraestrutura digital confiável[113] e interoperável, o qual se revela como decisivo para construir bases concretas da soberania digital[114], mitigando as assimetrias e promovendo a responsabilização efetiva contra abusos e usos indevidos dos dados.

Assim, a adoção de protocolos padronizados merece atenção para facilitar a aplicação de direitos como portabilidade e exclusão, respeitando a

109 *Ibid*.

110 *Ibid*.

111 BELLI; GASPAR; JASWANT. Data sovereignty and data transfers as fundamental elements of digital transformation.

112 PARSHEERA, Smriti, Stack is the New Black?: Evolution and Outcomes of the 'India-Stackification' Process. **Computer Law & Security Review**, v. 52, p. 105947, 2024.

113 MISRA, Manu; PANDAY, Jyoti; ZINGALES, Nicolo. Applying the CII Framework to DPIs considerations, challenges and opportunities. **T20 Policy Brief**, 2024.

114 BELLI, Luca. **Building Good Digital Sovereignty through Digital Public Infrastructures and Digital Commons in India and Brazil**.

diversidade tecnológica e regulatória dos países da maioria global. Soberania de dados: a experiência da China e lições para o Brasil

1.6.1 Soberania de dados: a experiência da China e lições para o Brasil

A experiência chinesa revela-se especialmente relevante como paradigma para demonstrar como, mesmo países em desenvolvimento, podem alcançar posições de liderança em governança de dados (ou, genericamente, de tecnologia). No caso chinês, tal liderança foi alcançada, dentre outras razões, em virtude de uma abordagem sistêmica que conjuga regulação normativa via legislação, padrões técnicos e política industrial, articulados por meio de uma coordenação multissetorial sob a égide do Estado.[115]

Assim, a experiência chinesa em matéria de governança de dados é notadamente interessante, porque constitui um dos exemplos mais consistentes de articulação entre regulação por meio da sanção, isto é, que implementa a norma jurídica, e regulação por meio da facilitação, ou seja: consequência da política industrial. Assim, o modelo chinês ilustra como a regulação pode ser voltada não somente para definir limites, mas também para proporcionar as ferramentas necessárias ao aproveitamento de dados na economia digital.

Nessa direção, desde outubro de 2019, o Comitê Central do Partido Comunista da China reconheceu, com decisão adotada no 4º Plenário do 19º, os dados como um novo fator de produção, ao lado de terra, trabalho e capital, desencadeando uma abordagem sistêmica a eles. Esse novo fator de produção passou a ser compreendido não apenas como insumo econômico, mas como recurso estratégico, indissociável da segurança nacional, da soberania tecnológica e do desenvolvimento socioeconômico.[116]

---

115 BELLI, Luca. 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, p. 145, 2022.

116 WANG, Wayne Wei, Contextualizing Personal Information: Privacy's Post-Neoliberal Constitutionalism and Its Heterogeneous Imperfections in China; WANG, Wayne Wei, China's digital transformation: Data-empowered state capitalism and social governmentality. **The African Journal of Information and Communication (AJIC)**, n. 31, 2023.

Do ponto de vista normativo, a República Popular da China adota instrumentos clássicos de regulação pela lei fundados no poder sancionatório do Estado. Nesse sentido, destacam-se três diplomas fundamentais: a Lei de Cibersegurança, promulgada em 2017; a Lei de Segurança de Dados, de 2021; e a Lei de Proteção de Informações Pessoais, igualmente de 2021.[117] A aplicação desses diplomas é concentrada na *Cyberspace Administration of China* (CAC), autoridade administrativa com ampla capacidade regulatória, responsável pela fiscalização e pela imposição de sanções.

Ao lado desse aparato sancionatório, observa-se a presença de uma política industrial de caráter facilitador, cujo objetivo é estruturar o ecossistema nacional de dados como espaço de inovação e de desenvolvimento econômico.[118] Dentre os principais instrumentos empregados, destacam-se os investimentos públicos maciços em pesquisa e desenvolvimento; o estabelecimento de plataformas de intercâmbio de dados (*data exchanges*) desde 2015, que chegaram a gerar faturamentos bilionários para as empresas públicas que os gerenciam em cidades como Guiyang, Xangai, Pequim e Shenzhen[119]; e a utilização de contratos administrativos e encomendas tecnológicas para estimular empresas nacionais do setor de tecnologia da informação. Tais medidas visam não apenas a fomentar a circulação de dados como ativo econômico, mas também assegurar que essa circulação ocorra em ambiente controlado, certificado – especialmente em termos de qualidade, cibersegurança e direitos de exploração de dados, elementos explicitamente controlados pelos *data exchanges* – e auditável, compatível com os imperativos da segurança nacional e da proteção de direitos individuais.

A experiência chinesa com plataformas públicas de intercâmbio de dados pode, então, oferecer lições importantes para o Brasil na construção de uma infraestrutura nacional de dados voltada à soberania digital

117 WANG, Contextualizing Personal Information; WANG, China's digital transformation.

118 BELLI, Luca; CHANG, Sofia, Governança de dados na China: Soberania, cibersegurança e proteção de dados rumo ao "Efeito Pequim", **Revista Brasileira de Direitos Fundamentais & Justiça**, v. 24, n. 53, 2025; MA, Aifang, Regulation in pursuit of artificial intelligence (AI) sovereignty: China's mix of restrictive and facilitative modalities, **The African Journal of Information and Communication (AJIC)**, n. 34, p. 1–16, 2024; BELLI, New Data Architectures in Brazil, China, and India.

119 HE, Alex; ARCESATI, Rebecca. **Data Marketplaces and Governance: Lessons from China**, Centre for International Governance Innovation. Disponível em: <https://www.cigionline.org/articles/data-marketplaces-and-governance-lessons-from-china/>. Acesso em: 11 nov. 2025.

e à inteligência artificial. Os *data exchanges* foram alavancados para criar mercados regulados de dados, no âmbito dos quais o Estado atua como avaliador e garante da qualidade, segurança e rastreabilidade dos (bancos de) dados disponibilizados. Assim, o estado desempenha um papel central para facilitar a transformação de dados (públicos) em ativos econômicos e estratégicos, assegurando sua circulação em ambientes auditáveis e compatíveis com as exigências de proteção de direitos e segurança nacional.

Numa tentativa de transposição para a realidade brasileira, as empresas públicas estaduais de tecnologia da informação, conhecidas como PRODEs[120], poderiam ser alavancadas para desempenhar papel semelhante. Com ampla experiência em infraestrutura de TIC e serviços de governo digital, os PRODEs têm potencial para se tornar operadores regionais de plataformas públicas de intercâmbio de dados. Nesse modelo, cada PRODE gerenciaria a curadoria e certificação de bases públicas, criaria ambientes seguros para análise de dados e registraria o uso dessas informações de maneira auditável, estimulando tanto a inovação científica quanto o desenvolvimento econômico regional.

A transformação dos PRODEs em operadores regionais de *data exchanges* públicos estaduais representa uma oportunidade estratégica para descentralizar a governança de dados e criar uma infraestrutura federada, interoperável e economicamente sustentável. Idealmente, a atividade dos PRODEs deveria ser articulada no âmbito de uma Rede Nacional de Intercâmbio de Dados Públicos. A iniciativa também estimularia a capacitação técnica regional e consolidaria as bases de um ecossistema nacional de dados públicos, seguro, transparente e sustentável, fundamental para o avanço da inteligência artificial no país.

Cada PRODE poderia atuar como um nó de confiança dentro de uma rede nacional, e o fortalecimento dos PRODEs nessa função ampliaria sua relevância econômica e institucional, integrando-os aos ecossistemas de inovação estaduais e às políticas de desenvolvimento regional. Em parceria com universidades, parques tecnológicos e empresas locais, esses operado-

120 Os PRODEs são órgãos ou entidades estaduais responsáveis por prover serviços de tecnologia da informação e comunicação ao governo. Criados para centralizar o processamento de dados públicos, podem ser autarquias ou empresas públicas, conforme a legislação de cada estado. Sua função é desenvolver, manter e integrar sistemas, garantir infraestrutura tecnológica e apoiar a transformação digital da administração estadual.

res poderiam oferecer serviços especializados de curadoria de dados, hospedagem segura e apoio técnico para projetos de IA, reduzindo barreiras de entrada para startups e grupos de pesquisa. Assim, o estudo do modelo chinês é útil como inspiração para a eventual aprimoramento dos PRODEs. Particularmente, nos parece que tais atores poderiam ser enxergados não apenas como provedores de infraestrutura tecnológica, mas também como catalisadores de uma nova economia de dados, podendo ser aproveitados para desempenhar um papel parecido com os *data exchanges* chineses, ou seja, como plataformas de avaliação e disponibilização de dados.

Por fim, o estudo da experiência chinesa nos parece relevante para ilustrar os benefícios da sinergia entre regulação pela sanção e política industrial pela facilitação, que confere ao modelo chinês elevada efetividade regulatória e reforça a soberania de dados do país. O Estado chinês, ao mesmo tempo em que estabelece normas jurídicas e instrumentos de fiscalização efetivos, cria condições materiais e institucionais para o desenvolvimento das tecnologias digitais no plano doméstico e, de maneira particularmente importante, a tributação dos ativos de dados. Daí a nossa sugestão de que a experiência chinesa nesse aspecto seja considerada como exemplo de um mecanismo de coordenação estratégica para facilitar o desenvolvimento tecnológico, em consonância com os objetivos nacionais de segurança, inovação e competitividade.

1.6.2 O Marco Europeu de Soberania em Nuvem: racional, funcionamento e lições para o Brasil

Em 20 de outubro de 2025, a Comissão Europeia apresentou o *Cloud Sovereignty Framework* (CSF)[121], ou Marco Europeu de Soberania em Nuvem, um passo relevante – porém ainda amplamente insuficiente – na busca da Europa por maior controle sobre sua infraestrutura digital e pela garantia de autonomia estratégica no domínio da computação em nuvem. O *framework* representa o resultado de anos de discussões sobre como definir, medir e aplicar dimensões que compõem o conceito de soberania digital, de modo a quantificar o nível de cumprimento de requisitos quan-

121 European Union Cloud Sovereignty Framework Version 1.2.1 – Oct. 2025.

titativos e qualitativos e comparar tais níveis entre provedores de serviços – especialmente de computação em nuvem.

Nesse sentido, o *framework* é valioso, porém ainda concentrado, principalmente em pontuações sobre *compliance* com obrigações regulatórias, e extremamente carente em medidas concretas para estimular produção e o controle europeu efetivo sobre infraestruturas digitais, que são condição essencial para limitar exposição a legislações extraterritoriais e o efeito de *vendor lock-in* em sistemas estrangeiros, que serão explorados no capítulo 3.

O surgimento do CSF decorre da crescente preocupação de que a economia digital europeia dependa em excesso de provedores estrangeiros, especialmente de origem norte-americana e chinesa. Essa dependência cria vulnerabilidades estratégicas, jurídicas e de segurança, que vão desde o risco de acesso extraterritorial a dados (como o permitido pelo *Clarifying Lawful Overseas Use of Data Act* estadunidense, conhecido como CLOUD Act, que será abordado na Seção 3.1) até a exposição a interrupções na cadeia de suprimentos e à perda de controle sobre infraestruturas críticas.

O CSF surge como resposta à necessidade de se garantir que os serviços digitais utilizados por governos, empresas e cidadãos estejam efetivamente regulados em conformidade com a legislação em vigor. O *framework* é inspirado por iniciativas nacionais como o SecNumCloud[122], elaborado pela Agência Francesa da Cibersegurança (ANSSI), e o *Cloud Computing Compliance Controls Catalogue*[123] (C5) – certificação de segurança em nuvem prescrita pela Agência Federal Alemã de Cibersegurança (BSI), além de práticas internacionais em controle de exportações, resiliência de cadeias produtivas e certificações de segurança cibernética.

Esse movimento se insere em um contexto mais amplo de busca por autonomia estratégica em âmbito digital, estabelecendo dimensões e parâmetros mensuráveis. Assim, o objetivo do CSF é o estabelecimento de critérios voltados a avaliar o nível de controle, conformidade e sustentabili-

122 **SecNumCloud pour les fournisseurs de services Cloud | ANSSI**. Disponível em: <https://cyber.gouv.fr/secnumcloud-pour-les-fournisseurs-de-services-cloud>. Acesso em: 10 nov. 2025.

123 **Criteria catalogue C5**. Federal Office for Information Security. Disponível em: <https://www.bsi.bund.de/EN/Themen/Unternehmen-und-Organisationen/Informationen-und-Empfehlungen/Empfehlungen-nach-Angriffszielen/Cloud-Computing/Kriterienkatalog-C5/kriterienkatalog-c5.html?nn=909536>. Acesso em: 10 nov. 2025.

dade, que podem ser aplicados tanto a contratações públicas quanto à certificação voluntária de provedores, no âmbito da computação em nuvem.

Em especial, o *framework* define oito objetivos de soberania, que compõem um sistema de avaliação padronizado de provedores de nuvem. Cada objetivo é avaliado em uma escala de 0 a 4, chamada SEAL (*Sovereignty Effectiveness Assurance Level*), permitindo medir de forma objetiva o grau de alinhamento de cada serviço com os princípios estratégicos e jurídicos europeus.

Os oito objetivos cobrem as seguintes dimensões:

1. Autonomia estratégica: avaliação da propriedade e do controle europeu sobre o provedor.
2. Jurisdição legal: medição da exposição a leis de países terceiros e garantia de que os dados estejam sob proteção jurídica europeia.
3. Controle operacional: capacidade de operar e proteger serviços sem dependências externas críticas.
4. Transparência da cadeia de suprimentos: rastreabilidade de componentes, fornecedores e parceiros tecnológicos.
5. Abertura tecnológica: estímulo à interoperabilidade, ao uso de padrões abertos e à portabilidade de dados.
6. Segurança e conformidade: aderência a normas europeias de cibersegurança e auditoria de processos.
7. Sustentabilidade ambiental: eficiência energética, pegada de carbono e alinhamento com o Pacto Verde Europeu.
8. Alinhamento com políticas digitais da EU: contribuição para ecossistemas estratégicos, P&D e espaços de dados europeus.

Provedores que desejem oferecer serviços à administração pública europeia são avaliados de acordo com esses critérios. Para participar de licitações para contratação de serviços de nuvem, é obrigatório atingir níveis mínimos de SEAL em todos os oito objetivos. Caso algum critério não seja atendido, a proposta é automaticamente rejeitada. Supostamente, isso garante a aplicação uniforme de obrigações regulatórias, cujo respeito é

essencial para a soberania e deveria estimular a concorrência com base no cumprimento da legislação, e não apenas em preço ou reputação.

A inclusão de todas as dimensões acima, porém, pode se revelar problemática ao misturar elementos essenciais com fatores acessórios. Assim, somente parte dos critérios avaliados está diretamente relacionada à essência da soberania digital: quem detém o controle sobre os ativos, qual legislação se aplica em situações de conflito, e quem se beneficia do serviço prestado. No entanto, o *framework* dá peso equivalente a aspectos periféricos como práticas de documentação. A consequência disso é um desbalanceamento de fatores que, ao agregar fatores diferentes cria incentivos perversos. Isso é particularmente visível ao permitir que bons resultados em critérios secundários compensem deficiências em elementos centrais, como exposição a jurisdições estrangeiras ou falta de controle europeu sobre a infraestrutura.

Grandes hyperscalers podem compensar fragilidades essenciais com desempenhos elevados em dimensões operacionais, ambientais ou de conformidade formal. O resultado é que os provedores verdadeiramente alinhados aos critérios de soberania podem terminar com pontuações inferiores a grandes empresas que apenas criam uma fachada de *compliance*.

Apesar de a União Europeia não ser geralmente um exemplo de sucesso em termos de soberania digital, parece-nos relevante mencionar o CSF como uma iniciativa relevante – porém, insuficiente na estrutura atual – para responder ao desequilíbrio global no mercado de computação em nuvem, que analisaremos na seção 3.1.

Atualmente, provedores norte-americanos como AWS, Microsoft Azure e Google Cloud, juntamente com empresas chinesas como Alibaba Cloud e Huawei Cloud, controlam mais de 75% do mercado mundial.[124] A dependência europeia reflete, em proporções muito parecidas, a dependência do Brasil e implica riscos não apenas econômicos, mas também jurídicos e políticos. A aplicação extraterritorial de legislações estrangeiras, como o CLOUD Act, ameaça diretamente a segurança de dados e, como destacaremos em seguida, o predomínio de tecnologias proprietárias es-

124 RICHTER, Felix, **Infographic: Big Three Hold Dominant Lead in Accelerating Cloud Market**, Statista Daily Data. Disponível em: <https://www.statista.com/chart/18819/worldwide-market-share-of-leading-cloud-infrastructure-service-providers>. Acesso em: 5 mar. 2026.

trangeiras reduz a capacidade de inovação independente, além da aplicação efetiva das legislações.

Assim, embora o CSF pareça oferecer às equipes de compras públicas um instrumento estruturado, de fato ele não conduz a mudanças estruturais, ou seja: não inclui nenhuma medida que obrigue, ou simplesmente facilite, a migração dos sistemas digitais do setor público para provedores europeus soberanos. Não há mecanismos de preferência de provedores nacionais ou de incentivo para a transição gradual, e o *framework* desconsidera totalmente a necessidade de diversificação de provedores ou possibilidade de saída dos sistemas atuais, sendo, portanto, irrelevante no que diz respeito à redução da atual concentração em um número extremamente limitado de provedores estrangeiros. Com efeito, parece-nos essencial que requisitos de diversificação ou planejamento de saída sejam incluídos para eliminar o efeito *vendor lock-in* que será analisado na seção 3.1. A concentração excessiva em um pequeno número de provedores é identificada pela própria União Europeia como um risco de soberania; porém, o *framework* não endereça essa vulnerabilidade. Assim, uma versão brasileira do *framework* deveria incluir exigências de redução de dependência, como destacaremos no capítulo.

Cabe frisar, ainda, que o Brasil se encontra em posição favorável para adaptar e aprimorar a iniciativa europeia e desenvolver um Marco Brasileiro de Soberania em Nuvem, coerente com sua realidade regulatória e estratégica. Não somente, a Lei Geral de Proteção de Dados (LGPD) já fornece uma base jurídica sólida para a proteção de dados pessoais e para desenvolver critérios de soberania relacionados à jurisdição e ao controle de dados, mas o arcabouço regulatório em termos de compras públicas pode ser alavancado para estimar uma transição real rumo a uma infraestrutura digital tecnologicamente autônoma, como destacaremos na seção 4.3.1. Além disso, a Estratégia Brasileira de Transformação Digital (E-digital) deve ser atualizada em 2026, e uma nova Lei Geral de Cibersegurança está sendo elaborada.[125] Essas mudanças oferecem uma oportunidade de ouro

125 MATOS, Mara. **CNCiber cria grupo de trabalho para avaliar Lei Geral da Cibersegurança - TELETIME News**. Disponível em: <https://teletime.com.br/09/10/2025/cnciber-cria-grupo-de-trabalho-para-avaliar-lei-geral-da-ciberseguranca/>. Acesso em: 10 nov. 2025; BELLI, Luca et al. **Governança e regulação da cibersegurança no Brasil: proteção da infraestrutura crítica,**

para formular políticas que contribuam diretamente para o fortalecimento da autonomia tecnológica por meio da segurança da informação.

A experiência europeia oferece um roteiro de ação que poderia ser replicado no Brasil, estabelecendo um mecanismo de certificação com base em níveis de elementos que compõem a soberania, semelhantes ao SEAL europeu. Tal certificação permitiria que provedores nacionais e estrangeiros demonstrem conformidade de maneira graduada, incorporando a pontuação de soberania em nuvem nos processos de contratação pública, especialmente em setores estratégicos como saúde, defesa, finanças e educação.

O objetivo não seria restringir a atuação de empresas estrangeiras, mas criar condições transparentes de confiança e promover um ecossistema nacional capaz de competir em bases equilibradas. Isso fortaleceria a inovação doméstica, aumentaria a segurança dos dados governamentais e ampliaria a autonomia tecnológica brasileira em relação a potências digitais estrangeiras.

Assim, o valor do CSF europeu estaria em redefinir a soberania digital como um conceito mensurável e aplicável, transformando uma agenda política em um instrumento técnico e econômico concreto. Ao converter princípios de autonomia, segurança e sustentabilidade em métricas objetivas, o *framework* permite decisões mais informadas e transparentes por parte de governos e empresas. Para o Brasil, a iniciativa europeia oferece um modelo pragmático de como equilibrar abertura de mercado e controle estratégico, garantindo que a infraestrutura digital que sustenta o desenvolvimento nacional seja não apenas eficiente, mas também soberana.

1.7 O Brasil não é condenado a ser uma colônia digital, mas precisa de pensamento sistêmico, foco e continuidade

Como explica nossa pesquisa, o Brasil foi um precursor da soberania digital[126], com as políticas do primeiro governo do presidente Luiz Inácio Lula da Silva sobre software livre. Por anos, o país foi referência mundial

segurança da informação e construção da soberania digital [s.l.]: Lumen Juris, 2025. BELLI et al. **Cibersegurança**.

126 JIANG; BELLI (Orgs.). **Digital Sovereignty in the BRICS Countries**.

da autonomia tecnológica, oferecendo uma visão de software como ferramenta libertadora, em vez de um instrumento de extração de dados e de colonização digital.

Nada obstante, pode-se apontar que o equívoco brasileiro foi pensar que *open source* deveria ser somente adotado, em vez de estimular sua produção para que um ecossistema de tecnologias *open source* pudesse crescer e até ser exportado. Essa lição, no entanto, foi aprendida por outros países do BRICS e até por corporações multinacionais. Os indianos entenderam o valor de se produzir infraestruturas públicas digitais[127] por meio de software livre os chineses entenderam muito bem o quanto é estratégico promover IA em código aberto para fortalecer sua soberania, como nos lembra o recente exemplo do DeepSeek. Empresas como Meta e Alphabet alavancam o *open source* de maneira extremamente sábia, usando-o como ferramenta de regulação do mercado ao embuti-lo em LLMs e sistemas operativos. Dessa forma, elas conseguem projetar seu poder infraestrutural nos ecossistemas digitais que desenvolvem e regulam privadamente.

O Brasil ainda pode – e deve – definir uma visão estratégica, um arcabouço regulatório, políticas industriais e uma governança capaz de fortalecer e reconstruir sua soberania em IA, focando nos ativos à disposição, alavancando tecnologias *open source* e evitando se isolar e instaurar uma autarquia digital.[128] Como destacaremos nas próximas seções, o país tem importantes ativos e já conseguiu, no passado, articular de maneira extremamente bem-sucedida política industrial, regulação e governança em áreas altamente estratégicas, como demonstram exemplos de sucesso brasileiro tais como a Embraer, a Petrobras e o SUS. Portanto, o Brasil pode alavancar seus talentos somente se conseguir definir sua visão de soberania em IA. Nesse sentido, o país deveria construir uma abordagem desenvolvimentista capaz de promover pesquisa, desenvolvimento e inovação, bem como organizar tais iniciativas de maneira ecossistêmica, por meio de

127 HARIHARAN, Venkatesh; NATARAJAN, Sarayu, Digital Sovereignty and Payments: A Case Study of the National Payments Corporation of India, *in*: JIANG, Min; BELLI, Luca (Orgs.). **Digital Sovereignty in the BRICS Countries**, 1. ed. Cambridge: Cambridge University Press, 2025, p. 105–123.

128 BELLI, Luca. **Views: On AI sovereignty and how Brazil can redefine it**, Medianama. Disponível em: <https://www.medianama.com/2024/06/223-views-ai-sovereignty-brazil-global-debate/>. Acesso em: 13 nov. 2025.

parcerias multissetoriais e cooperações internacionais, voltadas a resolver problemas concretos com base no contexto brasileiro.

Assim, é importante frisar a relevância de se desenvolver uma capacidade situacional de avaliação das oportunidades e dos riscos relativos ao desenvolvimento tecnológico, assim como uma resiliência cognitiva, para evitar ser conduzido a erro por meio de narrativas manipuladas, como destacaremos na seção 2.2.9. Por exemplo, cabe frisar que o recente relatório *State of AI in Business 2025*, elaborado pelo MIT, demonstra que, embora a inteligência artificial generativa apresente elevado potencial econômico, sua aplicação prática nas empresas tem produzido resultados limitados, sendo de utilidade muito limitada para resolver problemas concretos.[129] Apenas cerca de 5% dos projetos-piloto alcança aceleração significativa de receitas, enquanto a ampla maioria (95% segundo o relatório) permanece estagnada, sem impacto mensurável sobre o desempenho financeiro.[130]

A constatação exposta acima evidencia, de um lado, que o desenvolvimento e a implementação de sistemas de IA devem considerar o contexto econômico, social e institucional em que são inseridas, evitando orientar suas políticas com base em propagandas exageradas. De outro lado, como destacaremos em seguida, a resiliência a tais narrativas se torna cada dia mais árdua, considerando que as maiores empresas de tecnologias se tornaram também as principais fontes de (des)informação da população inteira.[131] No caso brasileiro, torna-se juridicamente e estrategicamente imprescindível que a IA seja orientada à solução de problemas locais, com base em dados locais e com intuito de maximizar o interesse público nacional, sob pena de permanecer alheia às necessidades reais do país e de não concretizar sua utilidade social e econômica.

Para que uma visão de soberania digital seja implementada de forma consistente, é indispensável não apenas a identificação dos ativos que podem ser alavancados e dos interesses que precisam ser priorizados, mas

129 CHALLAPALLY, Aditya et al. STATE OF AI IN BUSINESS 2025.

130 *Ibid*.

131 NEWMAN, Nic et al. **Reuters Institute digital news report 2024**, [s.l.]: Reuters Institute for the Study of Journalism, 2024. **Aláfia Lab | Desigualdades informativas e polarização política**. Disponível em: <https://alafialab.org/projeto/desigualdades-informativas-e-polarizacao-politica/>. Acesso em: 10 nov. 2025.

também a existência de mecanismos de governança em rede essenciais para implementar a visão estratégica desejada. Tais mecanismos serão destacados na terceira parte deste trabalho.

Outrossim, tal visão e tais instituições devem ter uma estabilidade necessária para que a implementação possa acontecer no médio e longo prazo. A experiência comparada demonstra que a ausência de instituições estáveis e capazes de garantir continuidade e coerência compromete a capacidade de se implementar políticas de médio e longo prazo, capacidade que nos parece essencial para uma transformação digital cujo objetivo seja a soberania em IA e a sustentabilidade.

Ao contrário, a falta de tal estabilidade institucional expõe inevitavelmente a riscos geopolíticos, mudanças tecnológicas abruptas e vulnerabilidades externas. A soberania digital exige políticas de educação, pesquisa, inovação e cibersegurança, que só podem florescer em um ambiente institucional estável e resiliente. Com efeito, a estabilidade institucional funciona como contrapeso necessário à fluidez e à adaptabilidade da governança em rede, assegurando que iniciativas fragmentadas possam ser integradas em uma estratégia nacional coerente e duradoura. Nesse sentido, parece-nos desejável que seja estabelecido um órgão de governança para a autonomia tecnológica, a exemplo de uma agência, que possa facilitar uma governança em rede. Idealmente, tal órgão não deveria ser criado *ex novo*, mas deveria resultar do reaproveitamento de entidade existentes, como, por exemplo, a Agência Brasileira de Desenvolvimento Industrial.

As próximas seções analisam quais elementos deveriam ser considerados para se estruturar uma visão sistêmica da soberania digital. Parte-se, então, de uma visão da soberania em IA, que, apesar de não representar a totalidade do "digital", contém características sistêmicas que se relacionam a várias das camadas relacionadas à soberania digital e, consequentemente, deveriam ser embutidas numa nova abordagem estratégica e regulatória de tais assuntos.

2 Uma abordagem em "camadas" para construir a pilha da soberania em IA

A metáfora da pilha ou *stack*[132], em língua inglesa, é útil para compreender como as dinâmicas da soberania digital se aplicam a sistemas de inteligência artificial (IA) e, portanto, auxiliam no debate sobre a soberania em IA, que é o objetivo deste segundo capítulo. Assim, a ideia de pilha nos obriga a considerar a existência de vários elementos (empilhados) que compõem os sistemas de IA e as relações entre as camadas em que esses elementos se situam. Assim como uma pilha tecnológica é formada por diferentes níveis – desde a infraestrutura computacional, passando por *frameworks* e bibliotecas de software, até as aplicações finais – o debate sobre a soberania em IA exige que se compreenda a função de cada elemento em cada camada para garantir autonomia e controle efetivo sobre o sistema inteiro.

Como argumenta Benjamin Bratton, a "pilha" organizada em camadas constitui tanto a estrutura técnica quanto a arquitetura de governança que sustentam a transformação digital.[133] Portanto, essa visão estratificada, apesar de não ser perfeita, revela-se útil para analisar como dependências externas ou lacunas em qualquer uma das camadas podem comprometer a capacidade de autodeterminação e autonomia tecnológica de um país (ou de outro ator que organize sua soberania em IA por meio de tal estrutura).

---

132 No contexto tecnológico, o termo "pilha" ou "*Stack*" é usado com frequência para designar uma estrutura utilizada para organizar e gerenciar informações de forma ordenada, sobretudo em sistemas computacionais. No campo do software, uma pilha é frequentemente empregada para controlar o contexto de execução de programas, como nas chamadas de função que armazenam temporariamente dados essenciais para retomada do processo após operações internas. Em termos de hardware, a pilha pode ser integrada na arquitetura do processador para gerenciar o fluxo de instruções. Já na IA, as pilhas são estruturas úteis para organizar o controle rigoroso da ordem de operações e garantir a eficiência e precisão na tomada de decisão computacional. BRATTON, Benjamin H., **The stack: on software and sovereignty**, Cambridge, Mass. London: MIT press, 2015. **(PDF) Rethinking Technology Stack Selection with AI Coding Proficiency**, ResearchGate. Disponível em: <https://www.researchgate.net/publication/395526006_Rethinking_Technology_Stack_Selection_with_AI_Coding_Proficiency>. Acesso em: 8 out. 2025.

133 BRATTON. **The stack**.

No debate jurídico e tecnológico, essa abordagem em camadas destaca a necessidade de ações integradas e políticas públicas que atuem em todos os níveis da pilha, desde o hardware nacional até o desenvolvimento de modelos de IA adaptados à realidade local, respeitando a regulação das demais dimensões da soberania digital. A metáfora reforça que a soberania em IA não se reduz a um dado elemento isolado, mas depende da articulação entre múltiplos componentes interdependentes, cujo gerenciamento estratégico é fundamental para garantir eficiência, segurança jurídica e alinhamento com os valores constitucionais do país. Portanto, refletir sobre a pilha tecnológica na IA é fundamental para a formulação de regulamentações e estratégias que assegurem a autonomia tecnológica e a defesa dos interesses nacionais.

Diante disso, torna-se essencial compreender os elementos que compõem tal pilha e que podem ser definidos como Facilitadores Essenciais da Soberania em Inteligência Artificial[134] (FESIA). Tais elementos serão analisados neste capítulo, bem como o papel que eles desempenham no desenvolvimento da capacidade de percepção situacional (*situational awareness*[135]) sobre IA. Neste contexto, os embates políticos evidenciam como elementos de poder – como recursos estratégicos e capacidade industrial – assumem papel central na definição da autonomia (tecnológica) nacional. Essa realidade tem se tornado particularmente evidente no caso brasileiro, não apenas pelo histórico de tensões entre empresas de tecnologia estadunidenses e o Judiciário[136], mas também pela mais recente disputa entre o presidente estadunidense Donald Trump e o governo brasileiro, que resultou na taxação de produtos brasileiros fundamentada em uma amálgama de fatores políticos, econômicos e narrativos relacionados à

134 BELLI, Luca. To Get Its AI Foothold, Brazil Needs to Apply the Key AI Sovereignty Enablers (KASE); BELLI; GASPAR (Orgs.). **The Quest for AI Sovereignty, Transparency and Accountability**; BELLI, Soberania em Inteligência Artificial.

135 JACKSON, Rosanna. The purpose of policy space for developing and developed countries in a changing global economic system. **Research in Globalization**, v. 3, p. 100039, 2021.

136 SPADONI, Pedro. STF, Anatel, Banco Central: o que incomoda as big techs no Brasil; VITTORAZZI, Davi. **STF forma tese para responsabilizar big techs por conteúdos de terceiros**. CNN Brasil. Disponível em: <https://www.cnnbrasil.com.br/politica/stf-forma-tese-para-responsabilizar-big-techs-por-conteudos-de-terceiros/>. Acesso em: 15 set. 2025.

liberdade de expressão e à regulação das empresas de tecnologia norte-americanas – as chamadas "*big techs*" – no Brasil.[137]

2.1 Um *framework* para organizar os elementos facilitadores da soberania em IA

A partir da perspectiva de um país como o Brasil, o conceito de soberania digital pode ser detalhado em componentes que sejam essenciais para fazer frente a dinâmicas globais que impactam seu espaço de política digital e de desenvolvimento. É possível compreender a soberania digital como uma "pilha" composta por múltiplas camadas interdependentes no âmbito das quais se situam os FESIA[138], que precisam ser enxergados de forma coordenada. Tais elementos, que precisam ser considerados para compor qualquer *framework* de soberania de IA, são:

1. **Dados**: controle sobre coleta, armazenamento, compartilhamento e processamento, considerando que os dados são um recurso estratégico fundamental para inovação em IA e políticas públicas baseadas em evidência.
2. **Software e capacidade algorítmica**: domínio de sistemas operacionais, bibliotecas de IA, modelos e algoritmos estratégicos, reduzindo a dependência de soluções estrangeiras.
3. **Capacidade computacional**: infraestrutura robusta de nuvem, supercomputadores e data centers nacionais, indispensáveis para o processamento de grandes volumes de dados.
4. **Conectividade significativa:** uma infraestrutura de Internet confiável, com bom desempenho e universalmente acessível a

137 LIMA, Bernardo; NALIN, Carolina. Governo já traça estratégia para taxar big techs. Veja as alternativas na mesa. **O Globo**. Disponível em: <https://oglobo.globo.com/economia/noticia/2025/07/19/governo-ja-traca-estrategia-para-taxar-big-techs-veja-as-alternativas-na-mesa.ghtml>. Acesso em: 15 set. 2025.

138 BELLI, Luca. To Get Its AI Foothold, Brazil Needs to Apply the Key AI Sovereignty Enablers (KASE); BELLI; GASPAR (Orgs.). **The Quest for AI Sovereignty, Transparency and Accountability**; BELLI, Luca. Soberania em Inteligência Artificial.

um preço competitivo, desempenha um papel fundamental para que os sistemas de IA sejam acessíveis, utilizáveis, treináveis e compartilháveis com a maior parte possível da população.

5. **Recursos energéticos e minerais**: disponibilidade de energia limpa, segura e sustentável, além de minerais críticos (como lítio, nióbio e terras raras), essenciais para a alimentação e fabricação de chips, semicondutores, dispositivos e infraestruturas digitais.
6. **Recursos humanos capacitados (*humanware*)**: formação, retenção e valorização de talentos em ciência da computação, engenharia, segurança da informação e áreas correlatas, bem como áreas do conhecimento necessárias para um entendimento interdisciplinar, crítico e ético dos riscos e oportunidades trazidos pelas tecnologias digitais.
7. **Cibersegurança**: mitigação de vulnerabilidades técnicas por meio de pesquisa, desenvolvimento e regulação sistêmica, acompanhadas por uma estrutura de governança que as coordene e execute efetivamente.
8. **Riscos para direitos fundamentais:** sistemas de inteligência artificial podem levar a inúmeras violações de direitos fundamentais, como privacidade, igualdade e liberdade, por meio de vigilância massiva, uso indevido de dados pessoais, discriminação algorítmica, manipulação de informação e decisões automatizadas sem transparência ou controle humano, ameaçando a dignidade, autonomia e segurança jurídica dos indivíduos.
9. **Resiliência cognitivo-informacional**: capacidade de entender e enfrentar a interferência desproporcional e assimétrica de empresas e governos estrangeiros na formulação de políticas públicas, processos decisórios e processos legislativos por meio, sobretudo, da manipulação de narrativas capazes de inviabilizar o desenvolvimento de infraestruturas soberanas.

Diante do exposto, parece-nos necessário adotar uma visão holística para conseguir entender quais são nossos principais ativos e, sobretudo, enxergar as vulnerabilidades sistêmicas que existem e podem surgir. Para

exemplificá-las, é suficiente pensar que os enormes investimentos em capacidade algorítmica e computacional propostos pelo Plano Brasileiro de IA (PBIA)[139] não serão efetivos para os cidadãos brasileiros se a maioria da população do país – 78% segundo os dados do Cetic.br[140] – continuar sem conectividade significativa.

Como destacaremos na seção 3.3, a enorme maioria dos "usuários de internet" no Brasil é, de fato, mera usuária de redes sociais, que estão entre os pouquíssimos aplicativos subsidiados nas franquias dos planos de internet móvel, concentrando a coleta de dados pessoais e a capacidade de inovação em IA – bem como a capacidade de perfilamento populacional – que deriva do tratamento de tais dados. Assim, cabe questionar quais consumidores poderão acessar modelos de IA brasileira em supercomputadores brasileiros se, para acessar tal inovação, continua sendo necessário dispor de um plano de conectividade que somente 22% pode suportar, enquanto redes sociais patrocinadas já estão oferecendo acessos a suas próprias IA "gratuitas", em possível violação à neutralidade da rede.

Nessa ordem de ideias, a fim de estimular o acesso e a distribuição de serviços de IA em pé de igualdade, e reverter a dependência criada pelas práticas de "patrocínio de aplicativos" ou "*zero rating*"[141], necessário se faz realizar a aplicação do princípio da neutralidade da rede, explicitamente consagrado no art. 9º do Marco Civil da Internet (Lei 12.965/2014 ou MCI) e regulado no art. 9º do Decreto 8776/2016. Assim, revela-se preo-

---

139 BRASIL. **Plano brasileiro de IA terá supercomputador e investimento de R$ 23 bilhões em quatro anos**. Ministério da Ciência, Tecnologia e Inovação. Disponível em: <https://www.gov.br/mcti/pt-br/acompanhe-o-mcti/noticias/2024/07/plano-brasileiro-de-ia-tera-supercomputador-e-investimento-de-r-23-bilhoes-em-quatro-anos>. Acesso em: 13 nov. 2025.

140 NIC.BR. **Conectividade significativa: propostas para medição e o retrato da população no Brasil**. São Paulo: CGI.br, 2024.

141 Há pelo menos uma década, pesquisadores alertam sobre o potencial das práticas de zero-rating para aumento de concentração de poder, mercado e dados nos ecossistemas digitais, bem como a incompatibilidade desta prática com o Marco Civil da Internet. BELLI, Luca. **Neutralidade de rede e ordem econômica**. Disponível em: <https://www.omci.org.br/jurisprudencia/207/neutralidade-de-rede-e-ordem-economica/>. Acesso em: 13 nov. 2025; BELLI, Luca. Neutralidade da rede, zero-rating e o Marco Civil da Internet. In: **Governança e regulações da internet na América Latina**. Rio de Janeiro: FGV Direito Rio, 2018, p. 175–204; IDEC; INSTITUTO LOCOMOTIVA. **Acesso à internet móvel pelas classes CDE**, São Paulo: IDEC e Instituto Locomotiva, 2021. Uma coleção de estudos sobre a prática pode se encontrar em www.zerorating.info. Acesso em: 25 ago. 2025.

cupante que, até o presente momento, nenhuma autoridade competente para fiscalização do MCI tenha assinalado que planos de *zero rating* deveriam ser considerados não somente como uma flagrante violação ao MCI, mas como um enorme prejuízo para a própria execução do PBIA. Assim, parece-nos que, ao permitir tais modelos de negócios, cria-se não somente um oligopólio na coleta de dados dos usuários, mas também um hábito irreversível nos próprios usuários, que serão artificialmente acostumados a usar e a treinar somente os serviços patrocinados.

Diante disso, não seria de se espantar caso a enorme maioria da população brasileira nunca use IAs produzidas no Brasil, tornando-se dependente somente dos serviços de IA generativa patrocinados, continuando a treiná-los gratuitamente com seus dados. É justamente por causa deste cenário que as empresas de IA generativas mais abastadas estão começando a patrocinar seus próprios serviços[142], para ter a esperança de competir com a Meta, cujo serviço Meta.AI já foi sabidamente incluído em todas as redes sociais patrocinadas da empresa.

Diversamente, outros países, como a Índia, entenderam o enorme prejuízo que tais práticas poderiam determinar para a transformação digital do país e implementaram as próprias regulamentações de neutralidade de rede no sentido de proibir o *zero rating*. Ou seja, os modelos de conectividade limitados aos aplicativos patrocinados não são admissíveis na Índia, porque são considerados incompatíveis com legislação em vigor e os valores constitucionais que a neutralidade da rede visa a proteger – particularmente, a liberdade de expressão, a concorrência e a distribuição justa dos recursos para evitar a concentração de riqueza.

Essa decisão, apesar de ser frequentemente subestimada, talvez tenha sido a medida que mais fez pela soberania digital da Índia[143]. A maioria

142 TECMUNDO. **Vivo dá um ano de assinatura gratuita da IA Perplexity Pro aos clientes**. TecMundo: Tudo sobre Tecnologia, Entretenimento, Ciência e Games. Disponível em: <https://www.tecmundo.com.br/software/294653-vivo-disponibiliza-1-ano-assinatura-gratuita-ia-perplexity-pro.htm>. Acesso em: 10 out. 2025. TUDOCELULAR. **Claro fecha parceria com OpenAI e inclui ChatGPT como benefício de planos**. Disponível em: <https://www.tudocelular.com/mercado/noticias/n239790/claro-parceria-openai-chatgpt-beneficio-planos.html>. Acesso em: 10 nov. 2025.

143 BELLI, Luca. BRICS Countries to Build Digital Sovereignty, *in*: BELLI, Luca (Org.). **CyberBRICS: Cybersecurity Regulations in the BRICS Countries**. Cham: Springer International Publishing, 2021, p. 271-280; BELLI, Luca et al. **Cibersegurança:** uma visão sistêmica rumo a uma Proposta

dos observadores naquela época perceberam a regulação da neutralidade da rede na Índia como uma grande vitória para a liberdade de expressão e para a promoção dos direitos dos consumidores, mas, na verdade, um dos principais impactos dessa medida foi o fortalecimento da soberania no sentido de autodeterminação e autonomia tecnológica, mitigando os riscos de colonização digital e de desertificação do ecossistema digital nacional e preservando a concorrência e a inovação local.[144]

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[145], passando a ser o terceiro lugar com mais startups do mundo[146]. Parece evidente que a Índia entendeu que uma visão sistêmica é essencial para conseguir implementar uma transformação digital soberana.

Antes de explorarmos a complexidade institucional das camadas da pilha, as próximas seções abordarão individualmente os Facilitadores Essenciais de Soberania em Inteligência Artificial (FESIA) e o seu papel na formação de uma pilha de IA soberana, performante, eficiente e democrática.[147]

---

de Marco Regulatório para um Brasil Digitalmente soberano. Rio de Janeiro, RJ: FGV Direito Rio, 2023.

144 BANSAL. Radhika, Net Neutrality in the Indian Context, 2021.

145 PARSHEERA, Smriti. Net neutrality in India: From rules to enforcement, *in*: BELLI, Luca; PAHWA, Nikhil; MANZAR, Osama (Orgs.). **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.

146 CHOUDHURY, S. P.; SHARMA, S.; JAIN, S., Three Waves: Tracking the Evolution of India's Startups; **Unicorn Hunting 2022: Top Countries & Industries for Unicorn Companies**. Disponível em: <https://tipalti.com/blog/unicorn-hunting-2022/>. Acesso em: 13 nov. 2025.

147 A seção seguinte foi desenvolvida com base na seção 2 de Luca Belli: **Soberania em Inteligência Artificial: O que é e quais facilitadores essenciais podem tornar o Brasil um país soberano em IA?**; (Sovereignty in Artificial Intelligence: What Is It and What Key Enablers Can Make Brazil a Sovereign Country in AI?), 2024.

2.2 Apresentação do *framework* FESIA (Facilitadores Essenciais de Soberania em Inteligência Artificial) e sua aplicação ao contexto brasileiro

A presente seção explora os supramencionados FESIA defendendo o papel fundamental de tais elementos para garantir que um país possa compreender, desenvolver e regular os sistemas de IA de acordo com os seus próprios interesses, valores e objetivos estratégicos nacionais, em vez de estar sujeito ao impacto do exercício da soberania em IA por outras entidades estrangeiras (sejam elas estatais ou empresariais[148]).

É importante notar que o entendimento e a articulação dos FESIA para alcançar – ou não – a soberania em IA é suscetível de se tornar um tópico cada vez mais relevante e estratégico à medida que o desenvolvimento e a evolução e adoção de sistemas de IA continuam a avançar, adquirindo um papel significativo em vários aspectos da sociedade, da administração pública e da governança democrática, não se limitando à economia. Os impactos e avanços da IA estão sendo objeto de considerável investigação, especialmente no âmbito da proteção de dados pessoais[149] e incluem uma vasta gama de setores críticos e serviços públicos essenciais, como a defesa, a segurança nacional, a gestão de infraestruturas, a saúde e a justiça.

Nesse contexto, parece importante sublinhar que a capacidade de desenvolver, utilizar e regular sistemas de IA, em vez de ser regulados por meio dela, não depende exclusivamente da elaboração e aplicação de marcos regulatórios baseados em risco e segurança de produtos. Pelo contrário, a concretização de uma Pilha de Soberania em IA implica a capacidade de exercer agência e autodeterminação em pelo menos nove dimensões diferentes que, em conjunto, permitem a construção de um ecossistema de IA sustentável e estrategicamente autônomo. As próximas subseções apresentarão o *framework* FESIA que compõe a Pilha de Soberania da IA, analisando brevemente como o Brasil está aproveitando cada um dos FESIA.

148 BELLI, Luca et al. Structural Power as a Critical Element of Digital Platforms Private Sovereignty. In: **Constitutionalising Social Media**. London: Hart, 2022.

149 Ver, por exemplo, os resultados da conferência CPDP LatAm. Disponíveis em CPDP LATAM, **Publications**. Disponível em: <https://cpdp.lat/en/publications/>. Acesso em: 13 nov. 2025.

2.2.1 Dados (pessoais)

Os dados são o insumo vital dos sistemas de IA e ter acesso a dados diversificados e de alta qualidade é essencial para treinar e melhorar os modelos de IA. É importante notar que, dependendo do tipo de IA, os dados utilizados para alimentar sistemas podem ser categorizados como dados pessoais, governamentais (dados abertos), confidenciais, protegidos por direitos autorais etc., incluindo, assim, uma certa complexidade e necessidade de conformidade regulamentar no contexto do seu tratamento. Por conseguinte, não só a disponibilidade de grandes volumes de dados heterogêneos é essencial para desenvolver IA, como também a capacidade de garantir que tais dados sejam coletados, armazenados, tratados ou transferidos para países terceiros em conformidade com a legislação em vigor. Um *framework* capaz de lidar de maneira efetiva com tais aspectos é, portanto, um elemento crítico da soberania em IA.

Cabe ressaltar que países com bases de dados abrangentes sobre suas economias diversificadas, populações de grande tamanho e heterogeneidade (composição multiétnica etc.), juntamente com estratégias de dados, práticas consolidadas de abertura de dados, marcos regulatórios de proteção de dados pessoais e segurança da informação bem estruturados, podem ter uma vantagem competitiva. A correta combinação destes elementos e a correta implementação dos marcos normativos que os disciplinam permitem a construção de soberania em matéria de dados e de IA.

No entanto, é importante sublinhar que poucos países gozam do privilégio de ter à sua disposição grandes conjuntos de dados heterogêneos e sistemas sólidos de governança de dados, capazes de facilitar inovação e evitar tratamentos abusivos. Nesse contexto, parece importante considerar a necessidade de uma abordagem mais holística aos dados como ativo capaz de ser explorado no interesse nacional; porém, precisando de sólidas garantias contra tratamentos abusivos. Paralelamente, a fim de estimular uma soberania compatível com a cooperação e comércio internacional, parece essencial estabelecer novos marcos internacionais – regionais ou, idealmente, globais – de governança de dados e explorar os tratados intergovernamentais existentes, como a Convenção 108+, de modo que dados,

sejam eles pessoais ou não, sejam utilizados de maneira lícita com base em normas harmonizadas.[150]

Notadamente, a governança dos dados necessários para alimentar sistemas de IA deve ter um caráter mais abrangente do que a mera proteção de dados pessoais, incluindo normas capazes de disciplinar a utilização e a reutilização de dados abertos e de informações protegidas por direitos autorais, bem como garantias contra a utilização indevida de informações sensíveis e confidenciais. Essa abordagem estratégica, mais complexa e mais abrangente, se bem estruturada e implementada de maneira coordenada, pode atenuar os riscos e colher os benefícios de conjuntos de dados muito maiores e diversificados, proporcionando ao mesmo tempo segurança jurídica aos pesquisadores, desenvolvedores e usuários de IA.

Sendo assim, uma boa governança de dados almeja a proteção de dados pessoais, a proteção de direitos de propriedade intelectual, a garantia da segurança informacional e da segurança nacional, e o aproveitamento do valor dos dados para o desenvolvimento nacional. O Brasil fez progressos consideráveis em termos de governança de dados, estruturando uma das mais progressivas e refinadas políticas de dados abertos[151] e adotando um quadro de proteção de dados de última geração, a Lei Geral de Proteção de Dados ou LGPD. No entanto, a aplicação da LGPD permanece ainda muito tímida e incipiente, especialmente no que diz respeito aos sistemas de IA (particularmente a IA generativa)[152]. Além disso, o Brasil simplesmente não tem uma estratégia nacional de dados.

---

150 Os melhores exemplos de cooperação internacional em matéria de política de dados são fornecidos pelas iniciativas europeias. A Convenção 108 do Conselho da Europa é o exemplo mais conhecido – e até a recente entrada em vigor da Convenção de Malabo, o único – de tratado internacional relativo à proteção de dados pessoais. O exemplo mais refinado de abordagem coordenada da política de dados é oferecido pelo quadro da política de dados da União Europeia, que abrange o Regulamento Geral sobre a Proteção de Dados, a Diretiva "Dados Abertos" e a mais recente Lei dos Dados. É importante salientar que um quadro menos ambicioso, mas relevante, também poderia ser proposto a nível da América Latina, onde a maioria dos países já adotou leis de proteção de dados semelhantes. A esse respeito, ver BELLI, Luca et al. **Hacia un modelo latinoamericano de adecuación para la transferencia internacional de datos personales**, Rio de Janeiro: CPDP LatAm, 2023.

151 MAGALHÃES, Larissa; BEN DHAOU, Soumaya. **Open Data and Emerging Technologies: Connecting SDG Performance and Digital Transformation** [s.l.]: CyberBRICS, 2023.

152 BELLI, Luca. **Por que o ChatGPT descumpre a LGPD e por que peticionei à ANPD**, JOTA Jornalismo, Disponível em: <https://www.jota.info/artigos/por-que-o-chatgpt-descumpre-a-lgpd-e-por-que-peticionei-a-anpd>. Acesso em: 28 mar. 2025.

Portanto, parece altamente improvável que os assuntos destacados acima possam ser enfrentados de maneira orgânica e eficiente até a elaboração de tal documento estratégico e designação de um órgão voltado a sua implementação. Importante, ainda, avaliar o quanto o Brasil pode acabar vindo a ser influenciado pelas recentes discussões europeias no sentido da desregulação, especialmente por meio daquilo que se convencionou designar *Digital Omnibus*.[153]

Por fim, cabe frisar que, no Brasil, a coleta de dados (pessoais) está consideravelmente concentrada nas mãos de gigantes tecnológicos estrangeiros[154], principalmente devido aos já mencionados planos de Internet móvel de *zero rating*[155] ou aplicativos patrocinados. Tais planos subsidiam o acesso móvel principalmente a pouquíssimas redes sociais dominantes, portanto concentrando a coleta e processamento de dados da maioria das comunicações individuais – e boa parte das comunicações comerciais – do país, como discutido na seção sobre conectividade abaixo, e frustrando assim a possibilidade de aproveitar os dados pessoais como um ativo nacional. Por último, a segurança dos dados continua também a ser muito desorganizada, devido à inexistência de uma lei geral sobre cibersegurança e de uma agência reguladora, e à falta de arcabouço regulatório abrangente sobre a segurança de informação, como destacaremos na subseção dedicada à cibersegurança.[156]

2.2.2 Software e modelos algorítmicos

Os algoritmos de software são a base dos sistemas de IA, permitindo-lhes executar tarefas e tomar decisões. É importante notar que os algoritmos podem ser objeto de regulamentação, mas também podem desempenhar um papel instrumental na elaboração da regulamentação.

---

153 EUROPEAN COMMISSION. **Simpler EU digital rules and new digital wallets to save billions for businesses**. Press release. Disponível em: <https://ec.europa.eu/commission/presscorner/detail/en/ip_25_2718>. Acesso em: 25 mar. 2026.

154 LASTRES, Helena M M; CASSIOLATO, José Eduardo; DANTAS, Marcos. **Panorama da economia de dados no Brasil nos anos 2020**. Rio de Janeiro: RedeSist, 2024.

155 BELLI. Neutralidade da rede, zero-rating e o Marco Civil da Internet Para maiores informações sobre as práticas de zero rating, ver http://www.zerorating.info/.

156 BELLI, Luca et al. **Cibersegurança**: uma visão sistêmica rumo a uma Proposta de Marco Regulatório para um Brasil Digitalmente soberano. Rio de Janeiro, RJ: FGV Direito Rio, 2023.

Por um lado, o desenvolvimento e a implantação de algoritmos podem – pelo menos em parte – dar origem a riscos e problemas sociais que desencadeiam a necessidade de intervenção regulamentar. Esses riscos devem ser cuidadosamente considerados, especialmente tendo em conta o fato de poderem variar enormemente em função dos sistemas de IA em questão. Por exemplo, os sistemas chamados "modelos fundamentais" apresentam riscos muito diferentes dos algoritmos treinados em bases de dados hiper personalizadas e localizadas. Nesse sentido, a governança de algoritmos é intrinsicamente conectada com a regulação de riscos de IA, e se justapõe a várias áreas da regulação de plataformas e a regulação de tratamento automatizado de dados pessoais.

Por outro lado, os algoritmos podem apoiar a própria intervenção regulamentar, uma vez que são cada vez mais úteis e utilizados para implementar a própria regulamentação. Nessa perspectiva, o desenvolvimento de softwares, sejam proprietários ou *open source*, proporciona uma vantagem competitiva considerável ao país, ou entidade desenvolvedora, e permitem a incorporação de valores normativos de acordo com as especificidades definidas pelos desenvolvedores. Investir na pesquisa e no desenvolvimento de ferramentas algorítmicas, abordando simultaneamente os riscos e as vantagens que estas representam, pode melhorar enormemente as capacidades tecnológicas e regulatórias de um país e reforçar a soberania da IA. Um exemplo, nesse sentido, é o uso de infraestruturas públicas digitais para regular setores previamente dependentes da atividade de reguladores públicos ou empresas privadas, como no caso dos pagamentos online.

Assim, a promoção da cooperação entre as várias partes interessadas para desenvolver algoritmos de software pode permitir reforçar a soberania da IA, seja quando os atores nacionais são estimulados a desenvolver software proprietário, seja quando o software é desenvolvido em código aberto por meio de um processo colaborativo adotado – ou mesmo liderado – pelas partes interessadas nacionais. Nessa última perspectiva, cabe frisar que o primeiro Governo Lula foi um verdadeiro pioneiro em termos de uma abordagem coletiva à soberania digital[157], promovendo a adoção de

157 BELLI, Luca. Brasil precisa reconstruir sua soberania digital. **Estadão.** Disponível em: <https://www.estadao.com.br/politica/blog-do-fausto-macedo/brasil-precisa-reconstruir-sua-soberania-digital/>. Acesso em: 13 nov. 2025. BELLI; GASPAR; JASWANT. **Data sovereignty and data**

software livre e aberto (FOSS) como objetivo estratégico para o desenvolvimento nacional, já em 2003.

Essa política permitiu não só ser estrategicamente autônomo em relação aos produtores de software estrangeiros, mas também aumentar a compreensão e o desenvolvimento nacionais de software. Infelizmente, tal política foi revertida pela administração Temer em 2016, desencadeando de fato o recente fenômeno de plataformização da administração pública, adotando principalmente software e infraestrutura em nuvem desenvolvidos por provedores estrangeiros.

Como destacamos na seção 1.3, por anos o Brasil foi referência mundial, oferecendo uma visão de como o software pode ser enxergado como ferramenta libertadora, em vez de um instrumento de extração de dados e de colonização digital. Contudo, pode-se indicar como um possível equívoco estratégico do Brasil o fato de ter restringido sua abordagem à mera adoção de software livre, negligenciando o estímulo à sua produção nacional. Tal postura inibiu a formação de um ecossistema vibrante de tecnologias *open source*, que poderia ter sido – e, na nossa opinião, ainda é – essencial para a inovação doméstica.

Consequentemente, vislumbra-se o desperdício do potencial de posicionar o País como exportador relevante de soluções tecnológicas no mercado global. É importante sublinhar que um renascimento do apoio nacional às tecnologias de código aberto poderia ser uma forma significativa de reforçar o desenvolvimento nacional de IA, especialmente tendo em conta a existência de várias opções interessantes de modelos de código aberto, como o GPTNeo e BLOOM e, de maneira mais limitada, DeepSeek, Falcon, Gemma ou Llama,[158] sobre os quais podem ser construídos novos sistemas abertos de IA.

Ademais, é importante reconhecer que o Brasil não precisa necessariamente orientar sua estratégia para a construção de modelos de IA de fronteira ou *frontier models*, cuja criação envolve custos econômicos,

transfers as fundamental elements of digital transformation: Lessons from the BRICS countries. Computer Law & Security Review, v. 54, p. 106017, 2024.

158 O grau variável em que esses modelos podem ser considerados como "abertos" é objeto de intensos debates. Para uma visão geral do problema, veja WIDDER, David Gray; WEST, Sarah; WHITTAKER, Meredith, Open (For Business): Big Tech, Concentrated Power, and the Political Economy of Open AI, 2023.

energéticos e de capacidade computacional extremamente elevados, concentrados hoje em poucos polos globais. Uma alternativa mais realista e potencialmente mais eficaz seria alavancar as vantagens comparativas do País, especialmente em setores altamente digitalizados e ricos em dados, como óleo e gás, finanças, saúde e agropecuária. Nessas áreas, a combinação de bases informacionais extensas, conhecimento técnico acumulado e infraestrutura institucional consolidada oferece condições favoráveis para o desenvolvimento de aplicações de IA especializadas, voltadas a problemas concretos e de alto impacto econômico e social. Ao priorizar a construção de sistemas de IA aplicados, facilmente adotáveis e alinhados às necessidades produtivas e regulatórias nacionais, o Brasil poderia não apenas acelerar a difusão doméstica dessas tecnologias, mas também desenvolver soluções exportáveis, capazes de atender demandas semelhantes em outros países com estruturas econômicas comparáveis.

Por fim, cabe ressaltar que, apesar da turbulência política, nas últimas duas décadas, o Brasil desenvolveu vários instrumentos de política industrial destinados a fomentar a indústria nacional de software e atualmente adota de uma nova política industrial que inclui a transformação digital como um dos seus pilares fundamentais.[159] No entanto, o setor de desenvolvimento de software não se tornou tão próspero como poderia, principalmente devido à falta de consistência das políticas relacionadas ao software nas últimas décadas e à ausência de políticas centradas no estímulo ao desenvolvimento e à implementação de software de forma orgânica, incluindo a facilitação do acesso ao capital para impulsionar a indústria nacional de algoritmos.

Em particular, as políticas brasileiras de software careceram de instrumentos complementares capazes de estimular a procura e a oferta, por exemplo, por meio de aquisições públicas de software desenvolvido

159 O Ministério do Desenvolvimento, Indústria, Comércio e Serviços do Brasil anunciou, em janeiro de 2024, a sua nova política industrial, baseada em seis missões fundamentais. A missão número 4 visa a "transformar digitalmente 90% de todas as empresas industriais brasileiras (hoje apenas 23,5% são digitalizadas) e triplicar a participação da produção nacional nos segmentos de novas tecnologias". Ver BRASIL [MDIC]. **Brasil ganha nova política industrial com metas e ações para o desenvolvimento até 2033**. Ministério do Desenvolvimento, Indústria, Comércio e Serviços. Disponível em: <https://www.gov.br/mdic/pt-br/assuntos/noticias/2024/janeiro/brasil-ganha-nova-politica-industrial-com-metas-e-acoes-para-o-desenvolvimento-ate-2033>. Acesso em: 13 nov. 2025.

em nível nacional, como acontece habitualmente na China, ou mediante a criação de infraestruturas públicas digitais, como fez a Índia com o India Stack[160], ou pela organização de esforços de capacitação destinados a fomentar a procura, como fez a Coreia do Sul no final da década de 1990.

2.2.3 Capacidade computacional

É sabido que a IA pode exigir recursos computacionais substanciais para tarefas como o treinamento de modelos complexos e o processamento de grandes conjuntos de dados. Em particular, os sistemas de IA mais recentes, como a IA generativa, podem ser notavelmente intensivos em termos de capacidade informática, devido à sua maior complexidade. Garantir a existência ou o acesso contínuo a uma capacidade computacional suficiente deve ser visto como uma prioridade estratégica fundamental, sem a qual é impossível tornar escaláveis novos sistemas de IA. Evidências contundentes nesse sentido são as parcerias nas quais as empresas OpenAI e Mistral, de fato, precisaram entrar com a empresa Microsoft, sendo esta última um dos pouquíssimos atores capazes de fornecer a capacidade computacional necessária.

Nesse sentido, cabe enfatizar que o mercado global de computação em nuvem é dominado por um número extremamente reduzido de empresas, sendo que as "Três Grandes" – ou seja, Amazon Web Services, Microsoft Azure e Google Cloud – representam atualmente dois terços do crescente mercado, com uma notável taxa de crescimento anual de 20% no final de 2023, em grande parte devido à explosão da "tecnologia e serviços de IA generativa que tiveram um grande impacto, ajudando a impulsionar ainda mais as despesas com computação em nuvem".[161]

A disponibilidade de infraestruturas de computação de alto desempenho depende de múltiplos fatores, desde a acessibilidade de semicondutores e chips especificamente concebidos para aplicações de IA e de uni-

160 **India Stack**. Disponível em: <https://indiastack.org/>. Acesso em: 25 set. 2025.

161 SRG. **Cloud Market Gets its Mojo Back. AI Helps Push Q4 Increase in Cloud Spending to New Highs**. Synergy Research Group. Disponível em: <https://www.srgresearch.com/articles/cloud-market-gets-its-mojo-back-q4-increase-in-cloud-spending-reaches-new-highs>. Acesso em: 13 nov. 2025.

dades de processamento gráfico ou GPU de última geração, que estão se tornando particularmente relevantes para suportar o funcionamento da IA (generativa), até servidores especializados adaptados às especificidades de sistemas de IA. É importante destacar que o mercado de semicondutores especializados em IA é particularmente concentrado, sendo, nesse momento, dominado por uma única empresa, a Nvidia, apesar dos avanços notáveis de outras empresas americanas, como a AMD e, cada vez mais, a Intel, as sul-coreanas SK Hynix e a Samsung e a chinesa Cambricon. Cabe também frisar que a Nvidia tem uma vantagem esmagadora devido ao seu ecossistema de software, o CUDA, que é o padrão da indústria para o desenvolvimento de IA de alto desempenho.[162]

A esse respeito, é interessante notar que uma das primeiras políticas adotadas pelo terceiro governo Lula foi a reintrodução do programa nacional de apoio ao desenvolvimento de semicondutores (conhecido como "PADIS"), bem como a suspensão da decisão anterior da administração Bolsonaro de vender o Centro Nacional de Tecnologia Eletrônica Avançada (Ceitec), que é o único produtor de semicondutores da América Latina.[163] Mais recentemente, uma das principais prioridades identificadas pela nova política industrial brasileira é o apoio à indústria nacional de semicondutores.[164] Porém, apesar desses avanços positivos, a capacidade de produzir semicondutores e servidores de computação de última geração é ainda muito distante da realidade nacional.

Cabe pontuar que essas medidas não são uma peculiaridade brasileira e que um número crescente de países está considerando-as. Um dos países com a política industrial digital mais estruturada é a China, que, nos últimos anos, investiu pesadamente na infraestrutura de IA, especialmente em seguida às restrições impostas pelos Estados Unidos e seus

162 PAK, Aidan, The CUDA Advantage: How NVIDIA Came to Dominate AI And The Role of GPU Memory in Large-Scale Model Training.

163 BRASIL. **Decreto 11.456**. Disponível em: <https://www.in.gov.br/en/web/dou/-/decreto-n-11.456-de-28-de-marco-de-2023-473390191>. Acesso em: 28 jan. 2025.

164 A visão geral das novas missões e prioridades da política industrial identificadas pelo Governo brasileiro em janeiro de 2024 está disponível em https://www.gov.br/mdic/pt-br/composicao/se/cndi/arquivos/missoes-politica-industrial.pdf. É importante sublinhar, no entanto, que, no momento da redação deste documento, o orçamento específico e a planificação detalhada da forma como esse orçamento será gasto ainda não tinham sido divulgados, não permitindo assim ao autor avaliar a solidez dos compromissos anunciados.

aliados. De acordo com dados da empresa chinesa de análise da indústria de semicondutores JW Consulting, o governo chinês atribuiu mais de 2,1 bilhões de CNY (1,5 bilhões de Reais) a investimentos relacionados com semicondutores entre 2021 e 2022, apoiando 742 projetos de investimento em 25 províncias e regiões chinesas.[165]

Cabe frisar que o Brasil poderia seguir o exemplo da China, particularmente no que diz respeito ao apostar no uso de tecnologias de código aberto como instrumento de autonomia tecnológica e desenvolvimento industrial, especialmente explorando estrategicamente a arquitetura aberta RISC-V, destacada na secção 1.3.1. Tal estratégia, se for implementada promovendo a formação de competências nacionais em hardware e software, é susceptível de reduzir consideravelmente dependências críticas em cadeias globais dominadas por soluções proprietárias. A promoção de IA de código aberto pode ter um papel importante na mitigação da concentração computacional, pois permite o desenvolvimento de sistemas de IA mais econômicos e distribuídos, reduzindo a necessidade de responder a recursos computacionais altamente concentrados[166].

Por fim, é essencial sublinhar que a disponibilidade de recursos de computação em nuvem, por si só, não é suficiente para afirmar a soberania da IA, que exige que os recursos de nuvem estejam não só disponíveis, mas também em total conformidade com a legislação nacional. Um exemplo revelador de como isso está longe de ser a regra é oferecido pelos serviços de computação em nuvem que dão suporte às plataformas de educação online[167], principalmente fornecidos por duas grandes empresas estadunidenses no Brasil, que, até o momento, sequer mencionam políticas de conformidade com a LGPD.

---

165 LIN, Judy. **China invested US$290.8 billion in semiconductor projects between 2021-2022**. DIGITIMES, Asia. Disponível em: <https://www.digitimes.com/news/a20230627VL205/china-ic-manufacturing-semiconductor-chips+components.html>. Acesso em: 10 nov. 2025.

166 CMA, **CMA AI strategic update**. GOV.UK. Disponível em: <https://www.gov.uk/government/publications/cma-ai-strategic-update/cma-ai-strategic-update>. Acesso em: 10 nov. 2025.

167 CHACON, Guilherme et al. **Análise: Termos de Uso e Políticas de Privacidade do Google Workspace for Education e Microsoft 365 (Office 365 Educação)**: Zenodo, 2022.

2.2.4 Conectividade significativa

Uma conectividade significativa[168], que permita aos usuários usufruírem de uma infraestrutura de Internet confiável, com bom desempenho e universalmente acessível a um preço competitivo, desempenha um papel fundamental para que os sistemas de IA sejam utilizáveis pela maior parte possível da população. A conectividade significativa facilita o intercâmbio de dados, a colaboração e o acesso a serviços de IA baseados na nuvem. Ela permite aplicações em tempo real e apoia o desenvolvimento e a implantação de tecnologias de IA em vários setores, contribuindo para a construção da soberania de IA de um país.

Nos últimos dez anos, o Brasil fez enormes progressos em termos de penetração da Internet: o custo da conectividade diminuiu consideravelmente, enquanto a população conectada dobrou em uma década.[169] No entanto, esse quadro otimista esconde brechas digitais menos visíveis, que não afetam a quantidade, mas a qualidade do acesso à internet. A maior parte da população brasileira é considerada como "conectada", mas de fato está apenas parcialmente conectada.

Mais de 70% da população brasileira conectada, e cerca de 85% da população com rendimentos mais baixos, têm acesso principalmente a um conjunto reduzido de aplicativos incluídos nos chamados planos de *zero rating*.[170] Como visto, estes planos baseiam-se na definição de um volume de dados mensal limitado para os usuários e no patrocínio de alguns aplicativos selecionados pelas operadoras de Internet móvel, cujo consumo de

168 Segundo a União Internacional das Telecomunicações da ONU, a conectividade universal e significativa demonstra que todos podem acessar a internet em condições ideais, a um custo acessível, a qualquer hora e em qualquer lugar. Esse quadro é construído em torno de seis dimensões-chave: qualidade rápida e confiável, disponibilidade ubíqua e permanente, acessibilidade, segurança, dispositivos apropriados, habilidades adequadas. ("About Universal and Meaningful Connectivity", n.d.). O conceito foi desenvolvido pela Global Digital Inclusion Partnership ("Meaningful Connectivity", n.d.).

169 CETIC.BR. **TIC Domicílios**. Centro Regional para o Desenvolvimento da Sociedade da Informação. Disponível em: <https://cetic.br/pt/pesquisa/domicilios/publicacoes/>. Acesso em: 10 nov. 2025.

170 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.

dados não é contabilizado nas franquias de dados existentes. O objetivo de tais modelos é a concentração da atenção dos usuários, e a consequente coleta de dados pessoais, num número extremamente limitado de plataformas, percebidas como gratuitas pelos usuários, mas cujo acesso é de fato pago com dados pessoais ao invés de dinheiro.

Portanto, há de se questionar a conduta de um ator de mercado que explora sua capacidade econômica para criar uma conexão direta e exclusiva para coletar dados de usuários em um setor específico.[171] O fato de os aplicativos patrocinados no âmbito dos planos de *zero rating* serem normalmente plataformas de redes sociais dominantes torna particularmente difícil para qualquer outra empresa competir, sendo quase impossível desenvolver conjuntos de dados pessoais tão completos como os que pertencem a tais atores. Assim, além de concentrar artificialmente atenção de usuários, tais empresas consolidaram uma posição extremamente dominante devido a sua capacidade de treinar modelos de IA com suas bases de dados, impossíveis para serem replicadas, e graças a um número de usuários extremamente elevado que somente tais empresas detêm para testar e aperfeiçoar novos sistemas de IA.

Assim sendo, talvez não considerar as modalidades de acesso à internet seja um dos erros mais prejudiciais para o sucesso das políticas voltadas a promover a soberania de IA. Como destacamos na seção 2.1, os enormes recursos que o recém-proposto Plano Brasileiro de IA almeja investir em desenvolvimento de modelos algorítmicos[172] e aumento de capacidade computacional correm o risco de se tornar relativamente inúteis se a maio-

171 Prática parecida, apesar de não alavancar a restrição da conectividade por meio do *zero-rating*, é adotada pela Microsoft, ao inserir o Copilot "gratuitamente" nos sistemas da administração pública federal brasileira. Por meio de tal estratégia, a Microsoft passa a deter um acesso único e exclusivo a um vasto volume de dados sensíveis e estratégicos da máquina pública. Essa concentração de informações cria uma barreira quase intransponível para outras empresas – especialmente nacionais – que desejem desenvolver IA com base em dados públicos de qualidade, uma vez que não terão acesso comparável a esse conjunto privilegiado. Assim, a oferta "gratuita" pode se transformar em um instrumento de desigualdade competitiva, comprometendo a diversificação tecnológica e a soberania digital do país.

172 NETO, Germano P. Johansson; COSTA, Viviane C. Farias da; GASPAR, Walter Britto. Brazil's Artificial Intelligence Plan (PBIA) of 2024: Enabler of AI sovereignty? **The African Journal of Information and Communication (AJIC)**, n. 34, p. 1-15, 2024.

ria da população brasileira[173] continuar sem conectividade significativa, tendo acesso somente a serviços de IA patrocinado por meio de *zero rating*.

2.2.5 Recursos energéticos e minerais

À medida que os sistemas de IA crescem em relevância e dimensão, necessitam de um fornecimento estável e cada vez mais relevante de energia elétrica[174] para funcionarem eficazmente. Assim, garantir uma infraestrutura de energia confiável e o acesso à eletricidade a preços acessíveis é necessário para manter as operações de IA ininterruptas. A esse respeito, pode se dizer que o Brasil é provavelmente um dos países mais bem colocados para apoiar a expansão da infraestrutura da IA, uma vez que não só é independente em termos energéticos, como também entre 70% e 80% das suas necessidades energéticas anuais são satisfeitas por meio de energias renováveis, especialmente a energia hidroelétrica.[175]

Importa sublinhar que o atual grau de independência energética do Brasil e sua posição de liderança em energias limpas não são frutos do acaso, mas de décadas de políticas industriais e energéticas deliberadas: desde programas estratégicos de substituição de importações, como o Pró-Álcool nas décadas de 1970-1990, até políticas públicas, incentivos e regulação voltados para hidrelétricas, bioenergia, eólica e solar, que criaram cadeia produtiva, P&D e capacidade de escala nacional.[176] Essas ações coordenadas combinaram metas, subsídios direcionados, programas de ciência e tecnologia, além de mecanismos regulatórios, permitindo diver-

173 NIC.BR. **Conectividade significativa: propostas para medição e o retrato da população no Brasil**.

174 LUCCIONI, Sasha. **The mounting human and environmental costs of generative AI**. Ars Technica. Disponível em: <https://arstechnica.com/gadgets/2023/04/generative-ai-is-cool-but-lets-not-forget-its-human-and-environmental-costs/>. Acesso em: 10 nov. 2025.

175 BRASIL [MME]. **Brasil registra maior produção de energia limpa dos últimos 12 anos**, Ministério de Minas e Energia. Disponível em: <https://www.gov.br/mme/pt-br/assuntos/noticias/brasil-registra-maior-producao-de-energia-limpa-dos-ultimos-12-anos>. Acesso em: 10 nov. 2025.

176 MERCEDES, Sonia Seger Pereira; RICO, Julieta A. P.; POZZO, Liliana de Ysasa. Uma revisão histórica do planejamento do setor elétrico brasileiro. **Revista USP**, n. 104, p. 13-36, 2015. WERNER, Deborah; LAZARO, Lira Luz Benites, The policy dimension of energy transition: The Brazilian case in promoting renewable energies (2000–2022). **Energy Policy**, v. 175, p. 113480, 2023.

sificar a matriz energética, reduzir a dependência de combustíveis fósseis importados e posicionar o país como referência em bioenergia e altas participações renováveis na geração elétrica.

No entanto, a rede elétrica nacional não está isenta de críticas. A curto prazo, o Brasil não corre o risco de falta de abastecimento de energia graças à complementaridade de várias fontes de energia com a hidrelétrica, além de ter um potencial eólico e solar amplamente subutilizado, mas a falta de planejamento estrutural e a possibilidade de hidrologia adversa – que se tem verificado nos últimos anos – podem alterar o custo da energia, tornando-o consideravelmente mais elevado. Assim, apesar de ter desenvolvido uma forte infraestrutura de energia, a capacidade brasileira de apoiar a implantação de tecnologias de energia irradiada requer um foco mais forte no planejamento para evitar a dependência potencial de fontes externas.

Cabe destacar, outrossim, que o elevado consumo de energia elétrica deve ser considerado como uma evidente externalidade negativa da infraestrutura de IA que pode ter um impacto considerável sobre a disponibilidade energética e a poluição ambiental. Portanto, tal tipo de consumo precisa ser monitorado e idealmente disponibilizado para autoridades reguladoras, considerando que é conhecido e monitorado pelas empresas fornecedoras de computação em nuvem.

O termo computação em nuvem tem como grave defeito a sua incapacidade comunicar a dimensão essencialmente material das "nuvens" que, na realidade, são compostas por servidores de computador, cabos coaxiais, tubos de fibra ótica, condicionadores de ar, unidades de distribuição de energia, transformadores, tubulações de água e muito mais.[177] Para que a temperatura da "nuvem" seja mantida sob controle, e os demais serviços computacionais sejam oferecidos sem interrupção 24 horas por dia, todos os dias, é necessário um abastecimento constante de energia e, frequentemente, água.

Como analisa Monserrate, os condicionadores de ar para salas de computadores consomem uma quantidade extremamente elevada de energia, sendo equipamentos mais básicos, até mesmo nos *data centers* mais

177 AMOORE, Louise. Cloud geographies: Computing, data, sovereignty. **Progress in Human Geography**, v. 42, n. 1, p. 4-24, 2018.

avançados.[178] Particularmente, em estados como Virgínia, onde se concentram cerca de 70% do tráfego mundial da internet e a maioria dos data centers dos EUA, a energia utilizada para esfriar a nuvem é frequentemente produzida por centrais elétricas a carvão.[179]

Por último, um elemento intimamente interligado é a necessidade de um grande abastecimento de água para arrefecer a infraestrutura de computação de IA. De fato, embora as empresas de IA sejam particularmente opacas em relação ao seu consumo de energia e água, estudos recentes ilustram que a pegada hídrica de alguns dos maiores modelos de IA é claramente insustentável.[180] Nesse sentido, cabe destacar que apenas para "treinar o GPT-3 nos seus data centers, estima-se que a Microsoft tenha utilizado 700.000 litros de água doce. É água suficiente para encher a torre de arrefecimento de um reator nuclear".[181]

Graças aos avanços tecnológicos recentes, o consumo de água nos data centers foi notavelmente reduzido, especialmente pelo uso de sistemas de refrigeração com ciclos fechados que minimizam o desperdício hídrico. No entanto, essa redução significativa aplica-se apenas aos *data centers* mais modernos e atualizados, enquanto instalações mais antigas ainda dependem de métodos convencionais de resfriamento que consomem volumes elevados de água. Dessa forma, os benefícios ambientais ficam restritos a uma parcela do parque tecnológico atualmente em operação.

Não obstante a vasta cadeia energética necessária para criação, transmissão e armazenamento de dados, também existem os elementos minerais que correspondem à matéria-prima do hardware que ancora a nuvem computacional. Esses minerais englobam desde o silício até elementos de terras raras, essenciais para a manutenção das capacidades produtivas de

178 MONSERRATE, Steven Gonzalez. The Cloud Is Material: On the Environmental Impacts of Computation and Data Storage. **MIT Case Studies in Social and Ethical Responsibilities of Computing**, n. Winter 2022, 2022.

179 BRASIL [MME]. **Brasil registra maior produção de energia limpa dos últimos 12 anos**.

180 LI, Pengfei et al. Making AI Less "Thirsty": Uncovering and Addressing the Secret Water Footprint of AI Models, 2025.

181 GENDRON, Will. **ChatGPT needs to "drink" a water bottle's worth of fresh water for every 20 to 50 questions you ask, researchers say**. Business Insider. Disponível em: <https://www.businessinsider.com/chatgpt-generative-ai-water-use-environmental-impact-study-2023-4>. Acesso em: 10 nov. 2025.

alta tecnologia, que por sua vez, estruturam toda a cadeia de suprimentos e redes digitais que alicerçam o ciberespaço e as tecnologias de telecomunicações. Recentemente, disputas acerca destes recursos vieram à tona em disputas geopolíticas[182] para acesso a terras raras e outros minerais estratégicos, sendo tema de contenda diplomática entre EUA, China e aliados, além de servir como restituição pelo fornecimento de armamentos norte-americanos para Ucrânia em acordo assinado recentemente.[183]

Contudo, o domínio soberano desses recursos não se resume ao mero acesso ou controle desses minerais. O acesso à matéria-prima é o primeiro passo em uma cadeia produtiva que precisa extrair tais minerais, processá-los (em um processo com seus próprios impactos ambientais) e, após, refiná-los, inserir essa matéria-prima na cadeia de suprimentos de alta tecnologia que poderá, então, ser desenvolvida ao ponto de se tornar hardware de alta tecnologia.[184] Nota-se que isso representa outra oportunidade para a soberania digital nacional, haja vista que o Brasil concentra em torno de 23% das reservas mundial de terras raras; contudo, corresponde a 1% do processamento global.[185]

A ausência de políticas industriais que viabilizem a exploração desse recurso estratégico em toda sua cadeia produtiva corrobora para um papel extrativista que o Brasil vem desempenhando ao longo de toda sua história. Nota-se que o domínio e exploração dessa cadeia produtiva não precisam ser concentrados ou limitados ao território nacional. Na prática, pode fazer parte de um desenvolvimento econômico e coordenado. Como

182 PITRON, Guillame. The Geopolitics of the Rare-Metals Race. **The Washington Quarterly**, v. 45, n. 1, p. 135-150, 2022.

183 CENTER FOR STRATEGIC AND INTERNATIONAL STUDIES (CSIS). **What to Know About the Signed U.S.-Ukraine Minerals Deal**. Disponível em: <https://www.csis.org/analysis/what-know-about-signed-us-ukraine-minerals-deal>. Acesso em: 6 nov. 2025.
DYSA, Yuliia, Ukraine. US launch fund for critical minerals projects with $150 million investment. **Reuters**, 2025. KALANTZAKOS, Sophia. The Race for Critical Minerals in an Era of Geopolitical Realignments. **The International Spectator**, v. 55, n. 3, p. 1–16, 2020; PITRON, The Geopolitics of the Rare-Metals Race.

184 PITRON. The Geopolitics of the Rare-Metals Race; FARRELL, Henry; NEWMAN, Abraham L., Weaponized Interdependence: How Global Economic Networks Shape State Coercion. **International Security**, v. 44, n. 1, p. 42–79, 2019.

185 MENDO, Marcelo; VIANA, Frederico; PASSOS, Thiago. Brazil in the global race for rare earths. **Valor Internacional**. Disponível em: <https://valorinternational.globo.com/economy/news/2025/09/30/brazil-in-the-global-race-for-rare-earths.ghtml>. Acesso em: 6 nov. 2025.

ocorre, por exemplo, no caso da Embraer, quando é impulsionada por programas de desenvolvimento estatal e fragmenta sua cadeia produtiva entre diferentes parceiros comerciais internacionais.[186] Essa fragmentação produtiva, coordenada por uma empresa brasileira, não somente mitiga dificuldades produtivas locais, mas também compõem e consolidam um esforço econômico nacional, dentro de uma lógica soberana.

2.2.6 Humanware: promoção e retenção de talentos

Este ponto é crucial para o desenvolvimento sustentável do país e pode ser dividido em duas áreas extremamente importantes: a educação digital, por meio da qual os talentos são promovidos, e os incentivos pelo meio dos quais os talentos são retidos ou até trazidos de volta ao país, revertendo o fenômeno da chamada "fuga de cérebros" ou *brain drain*.

Melhorar a educação digital da população, mediante reforço das capacidades, da formação e da educação multigeracional, é essencial não só para conseguir uma mão de obra qualificada em IA, mas também para promover a cibersegurança e, em última análise, a soberania nacional[187]. Investir na educação, na pesquisa e no desenvolvimento no domínio da IA ajuda a criar um conjunto de profissionais de IA talentosos, ao mesmo tempo em que difunde uma compreensão de como utilizar a tecnologia da melhor forma. Uma estratégia educativa sólida é, por conseguinte, vital para permitir que a população nacional evolua gradualmente de uma população constituída principalmente por consumidores de tecnologia digital para uma população composta por prossumidores, ou seja, indivíduos que podem desenvolver tecnologia e produzir inovação em vez de serem exclusivamente consumidores.

A criação de uma sólida reserva de talentos de pesquisadores de IA, engenheiros e cientistas de dados permite a um país desenvolver e manter

186 AMARANTE, Jose Carlos Albano; FRANKO, Patrice. Defense Transformation in Latin America: Will It Transform the Technological Base? **Democracy and Security**, v. 13, n. 3, p. 173–195, 2017. ALONSO-GUINEA, Fernando; ALAÑÓN-PARDO, Ángel. On support from National Development Banks for the internationalisation of public Brazilian companies: it's hard to say goodbye (to good companies). **Journal of Economic Policy Reform**, v. 27, n. 4, p. 389–412, 2024.

187 BELLI, Luca et al. **Governança e regulação da cibersegurança no Brasil**.; BELLI; GASPAR (Orgs.). **The Quest for AI Sovereignty, Transparency and Accountability**.

as suas capacidades de IA, aumentando a possibilidade de ser um exportador de tecnologia e reduzindo a probabilidade de se tornar uma colônia digital. Nessa direção, revela-se altamente promissor que o governo federal tenha adotado uma nova política nacional para a educação digital.[188] No entanto, no Brasil, o desafio pode estar menos na formação de profissionais qualificados e mais na capacidade do sistema produtivo de absorvê-los.[189] Há uma mão de obra subutilizada com ensino médio completo ou superior incompleto que poderia ser empregada em setores com médias e altas intensidades tecnológicas. Essa situação indica um potencial inexplorado para promover o desenvolvimento orientado pela inovação, que depende não apenas da qualificação, mas também da oferta de oportunidades compatíveis com essas habilidades.

Assim, a melhor forma de estimular a retenção de talentos e reduzir a fuga de cérebros no Brasil poderia ser criar oportunidades reais de trabalho para jovens, especialmente por meio de programas que facilitem a criação de startups por jovens pesquisadores. Para isso, é essencial simplificar ao máximo a burocracia e implementar políticas de apoio às empresas de tecnologia, como isenções fiscais, *sandboxes* regulatórios e subsídios. Essas medidas incentivam o empreendedorismo inovador, fortalecem o ecossistema tecnológico e promovem o desenvolvimento sustentável do país.

É necessário considerar que a produção de talentos pode ser facilmente frustrada pelo fenômeno da fuga de cérebros, no âmbito do qual os talentos produzidos migram para outros países, atraídos por condições de trabalho mais palatáveis. Uma maneira viável de reter talentos no Brasil e reverter o fenômeno da fuga de cérebros é criar condições efetivas para que jovens e pesquisadores possam empreender com segurança jurídica; facilitar a abertura e o funcionamento de startups, especialmente em ambientes acadêmicos.

Por fim, ainda é problemático constatar que o letramento digital continua a ser considerado uma prioridade apenas para as novas gerações de estudantes, esquecendo que a maioria da população – ou seja, todos aque-

188 BRASIL. **Lei n. 14.533**. Disponível em: <https://www.planalto.gov.br/ccivil_03/_ato2023-2026/2023/lei/L14533.htm>. Acesso em: 10 nov. 2025.

189 GONÇALVES, Naira Teresa A. C.; RAPINI, Márcia Siqueira; ANTIGO, Mariangela Furlan. Formação de competências como desafio à inovação no Brasil: uma análise comparativa regional para o período 2012-2019. **Revista de Economia Contemporânea**, v. 28, p. 1-39, 2024.

les que não são altamente capacitados – precisa desse tipo de educação. Tal situação é especialmente arriscada num contexto de transformação digital acelerada e de automatização, em que a compreensão do funcionamento da tecnologia se torna uma necessidade primária não só para a geração mais jovem, mas sobretudo para todos os indivíduos, cujas condições laborais, sociais e econômicas são suscetíveis de serem afetadas pela implantação de sistemas de IA.

2.2.7 Cibersegurança

Os sistemas de IA podem ser alvo de vários tipos de ameaças à cibersegurança e podem ser utilizados para perpetrar ciberataques. Portanto, medidas robustas de cibersegurança, bem como pesquisa e desenvolvimento nas diferentes áreas da cibersegurança são vitais para qualquer país, mas tornam-se ainda mais importantes no contexto da transformação digital cada vez mais acelerada e da implantação de sistemas de IA.

Em particular, é essencial proteger pessoas usuárias de sistemas de IA e infraestruturas críticas de IA contra ciberataques. O Brasil promulgou recentemente um número considerável de regulamentações setoriais de segurança cibernética, abrangendo o setor de telecomunicações, o setor bancário, o setor elétrico e a Lei Geral de Proteção de Dados.[190] Embora muitos progressos tenham permitido ao país subir no Índice de Cibersegurança da União Internacional das Telecomunicações[191], é de notar que esse avanço positivo deve ser temperado com uma boa dose de pragmatismo.

Na verdade, o Brasil ainda não possui uma Lei Geral de Cibersegurança e uma Agência Nacional de Cibersegurança, embora tais elementos tenham sido propostos por um estudo produzido pelo Centro de Tecnologia e Sociedade da FGV[192] e por um Projeto de Lei formulado pela Presi-

190 BELLI, Luca et al. **Cibersegurança:** uma visão sistêmica rumo a uma Proposta de Marco Regulatório para um Brasil Digitalmente soberano. Rio de Janeiro, RJ: FGV Direito Rio, 2023.

191 **Brazil rises in international cybersecurity ranking**. Serviços e Informações do Brasil. Disponível em: <https://www.gov.br/en/government-of-brazil/latest-news/2022/brazil-rises-in-international-cybersecurity-ranking>. Acesso em: 10 nov. 2025.

192 BELLI, Luca et al. **Cibersegurança:** uma visão sistêmica rumo a uma Proposta de Marco Regulatório para um Brasil Digitalmente soberano. Rio de Janeiro, RJ: FGV Direito Rio, 2023.

dência da República[193]. Além disso, o País registrou um avanço muito positivo com a criação de um Conselho Nacional de Cibersegurança com caráter multissetorial, que pode ser enxergado como a primeira etapa rumo à construção de uma nova arquitetura de governança da cibersegurança.

Tal arquitetura deverá reverter a abordagem altamente fragmentada da cibersegurança no país, impulsionada pelas iniciativas de agências setoriais sem competência geral em matéria de cibersegurança e frustrada pela falta de estratégias nacionais coerentes. É possível argumentar que a falta de coordenação da abordagem brasileira à cibersegurança seja provavelmente uma das principais vulnerabilidades do país, que ainda não conseguiu criar um quadro de governança sólido para ligar, coordenar e alavancar a incrível quantidade de atores que já operam no ecossistema nacional de cibersegurança.[194]

Esse arcabouço político-institucional é essencial em função da transversalidade das tecnologias digitais e do avanço da transformação digital brasileira. Contudo, o uso de tecnologias de IA também vem ganhando grande capilaridade e transversalidade em diferentes setores da economia e da sociedade, inclusive incentivado em políticas públicas nacionais como o Plano Brasileiro para Inteligência Artificial (PBIA). Como destacado diversas vezes ao longo deste livro, a falha em dominar essas tecnologias representa uma fragilização da soberania digital.[195]

Contudo, quanto ao uso da IA para a cibersegurança, é notório que soluções de segurança cibernética representam território fértil no uso da IA, ao passo que a IA viabiliza o rápido processamento de vastas quantidades de dados. Nesse sentido, a IA vem sendo aplicada no âmbito da cibersegurança como uma IA defensiva, atuando na varredura de redes e sistemas visando ao reconhecimento de padrões e assinaturas.[196] Em um cenário de carência de recursos humanos especializados para a cibersegu-

193 BRASIL [GSI]. PNCiber – Apresentação do Projeto.

194 BELLI, Luca et al. **Governança e regulação da cibersegurança no Brasil**. [s.l.: s.n.], 2025.

195 *Ibid*.

196 CSERNATONI, Raluca; MAVRONA, Katerina. The Artificial Intelligence and Cybersecurity Nexus: Taking Stock of the European Union's Approach, 2022; GELUVARAJ, B.; SATWIK, P. M.; KUMAR, T. A. Ashok. The future of cybersecurity: Major role of artificial intelligence, machine learning, and deep learning in cyberspace. **International Conference on Computer Networks and Communication Technologies**, 2018; MALATJI, Masike; TOLAH, Alaa, Artificial

rança, o investimento e treinamento de modelos nativos de IA defensiva surge como uma alternativa viável para mitigar a falta de recursos humanos e simultaneamente, desenvolver tecnologias nacionais para emprego local, tomando as rédeas da soberania de IA e guiando-a de um lado, para a autonomia tecnológica; e, em uma eventual exportação, alavancando a capacidade nacional como ferramenta de influência tecnológica e econômica sobre demais parceiros.

2.2.8 Regulação de riscos

Uma estrutura de governança de IA que englobe considerações éticas, leis de proteção de dados, um marco regulatório baseado em risco, junto com mecanismos de fiscalização, *enforcement* e padronização técnica[197] é crucial para a soberania da IA. Estabelecer diretrizes e padrões claros para o desenvolvimento, a implantação e o uso da IA é fundamental para garantir práticas de IA responsáveis. Nessa perspectiva, o Congresso brasileiro está elaborando um novo Marco Regulatório de IA[198] para ajudar a fortalecer os direitos dos cidadãos, promover segurança jurídica e prevenir riscos potenciais, visando assim a orientar o desenvolvimento, a implantação e o uso de tecnologias de IA de forma sustentável.

É importante notar que, embora essa iniciativa seja certamente louvável e necessária, mesmo que ainda em curso, ainda não é claro até que ponto será capaz de orientar eficazmente a evolução da IA no país. Nos últimos cinco anos, pelo menos quinze projetos de lei extremamente heterogêneos foram apresentados no Congresso para criar um marco regulatório da IA no Brasil, nomeadamente os PLs 3.592/2023; 2.338/2023; 5.691/2019; 5.051/2019; 21/2020; 872/2021; 266/2024; 145/2024; 210/2024; 146/2024; 262/2024; 390/2024; 303/2024; 349/2024; 370/2024. É importante frisar que

intelligence (AI) cybersecurity dimensions: a comprehensive framework for understanding adversarial and offensive AI, **AI and Ethics**, 2024.

197 BELLI, Luca. Regulação da inteligência artificial para inglês ver?. **Jota**. Disponível em: <https://www.jota.info/opiniao-e-analise/colunas/ia-regulacao-democracia/regulacao-da-inteligencia-artificial-para-ingles-ver>. Acesso em: 10 nov. 2025.

198 PACHECO, Rodrigo. **Projeto de Lei n.º 2338/2023**. Senado Federal. Brasília, DF, 2023. Disponível em: <https://www25.senado.leg.br/web/atividade/materias/-/materia/157233>. Acesso em: 10 nov. 2025.

nenhum destes PLs define concretamente qual mecanismo de fiscalização, *enforcement* e padronização técnica deveria ser adotado para garantir a devida implementação do futuro marco regulatório e a consequente conformidade aos princípios e dispositivos normativos tão complexos para se regular.[199]

O PL 2338/2023 é o único que chega a definir as atribuições de uma "autoridade competente", sugerindo a ANPD como tal autoridade, que estaria no vértice, como um órgão coordenador de um Sistema Nacional de Regulação e Governança de Inteligência Artificial, na última versão disponível antes da publicação final deste estudo. Tal incerteza é suscetível de prejudicar enormemente a implementação de futura Lei, enquanto a ausência de uma autoridade, como proposto pela maioria dos PLs, pode ser ainda mais prejudicial.

O PL 2.338/2023, apesar de não ser isento de críticas, é, sem dúvidas, o mais estruturado e completo entre os PLs apresentados até hoje no país. No entanto, apesar de o artigo 19 do referido PL impor que os sistemas de IA incluam "o uso de interfaces ser humano-máquina adequadas" e "medidas de gestão de dados adequadas" e adotem "parâmetros adequados de separação e organização dos dados" e "medidas adequadas de segurança da informação", não indica como tais elementos essenciais poderiam ser determinados "adequados."

Definir um sistema que possa permitir não somente a adoção de um marco normativo moderno, ágil e capaz de maximizar direitos e reduzir riscos, mas também a implementação efetiva de tal marco é essencial. A adoção de normas flexíveis é uma estratégia regulamentar bem-vinda para elaborar leis que se adaptem ao futuro e à evolução tecnológica. No entanto, para serem significativas, as cláusulas flexíveis devem também ser acompanhadas de um mecanismo de aplicação que permita a sua especificação por meio de regulamentação ou normalização.

Na ausência de tal mecanismo, a lei corre o risco de ser altamente ineficaz e vaga, em vez de flexível, e de se tornar simplesmente impossível de aplicar. A esse respeito, é necessário considerar a recente experiência brasileira de regulamentação da proteção de dados para compreender que a adoção de uma lei moderna e a criação de uma nova autoridade reguladora é apenas o início do percurso regulamentar.

199 BELLI, Luca. Regulação da inteligência artificial para inglês ver? **Jota**.

A elaboração de leis flexíveis de proteção de dados tem sido essencial para se chegar a um consenso quanto à aprovação do quadro brasileiro de proteção de dados; mas a eficácia da estratégia regulamentar corre o risco de ser consideravelmente comprometida quando a tarefa premente de especificar a lei não é definida explicitamente pela lei ou é atribuída a uma entidade reguladora com tão poucos recursos que parece ter sido criada propositadamente para ser "ineficaz por padrão"[200].

2.2.9 Resiliência cognitivo-informacional

Não é novidade que países estrangeiros e seus agentes tentam – e por vezes conseguem – interferir em outras nações soberanas por meio do chamado *information warfare*, ou guerra de informação, com o intuito de manipular narrativas e criar confusão no inimigo[201]. No entanto, um fenômeno menos evidente – porém, não menos impactante ou preocupante – é o desenvolvimento de estratégias de influência orquestradas por atores privados para maximização de interesses privados. Nesse sentido, parece-nos essencial atentar-se para a capacidade de entender e enfrentar a interferência desproporcional e assimétrica de empresas e governos estrangeiros na formulação de políticas públicas, processos decisórios e processos legislativos, por meio, sobretudo, da manipulação de narrativas capazes de inviabilizar a autodeterminação e a autonomia nacional.

Ressalve-se, por oportuno, que tal interferência não é a simples atuação de *lobbies* em processos regulatórios de países soberanos, já que esta atividade, ainda que não regulamentada em algumas legislações, é parte integrante do tecido das relações políticas e sociais de todos os países democráticos. A interferência aqui analisada se refere àquela realizada por nações estrangeiras ou empresas privadas, de forma direta ou indireta, com intuito de manipular narrativas em direção à erosão de processos soberanos e democraticamente constituídos de outros países, no que diz res-

200 BELLI, Luca. **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. 2022.

201 BORDEN, Col Andrew, What is Information Warfare?; DOWSE, Andrew; BACHMANN, Sascha Dov. Information warfare: methods to counter disinformation. **Defense & Security Analysis**, v. 38, n. 4, p. 453-469, 2022.

peito à capacidade de formulação livre de suas agendas. Além disso, quando praticada de forma indireta, tal interferência costuma se dar também por meio de *lobby* ou construção de narrativas voltadas à manipulação da população, para influenciar de forma desproporcional à soberania dos países influenciados, atendendo a interesses de nações estrangeiras.

Carlos Saura García, em importante contribuição, examina como grandes potências mundiais, a exemplo dos EUA e da China, usam suas empresas digitais para exercer aquilo que ele designa "expansionismo digital". Segundo ele, o crescimento exponencial dessas plataformas permitiria que as superpotências realizassem "operações geoestratégicas, manipulação social em massa ou influenciar processos democráticos com o objetivo de aumentar seu poder e domínio sobre outras nações".[202]

Ao diferenciar os conceitos de "soberania digital" e "expansionismo digital", o autor ressalta que o primeiro se refere a uma lógica de defesa e controle legítimo de países afetados, enquanto o segundo corresponde a uma postura ativa, isto é, uma contraparte ofensiva, que buscaria afetar, influenciar e até mesmo subordinar outras nações estrangeiras por meio da área digital. Como razões que fundamentariam tal expansionismo, cita a exportação de valores sociais, políticos e econômicos para alcançar conquistas geopolíticas e, também a proteção interna, ou seja, uma forma de blindagem. No entanto, ao fim e ao cabo, essas estratégias expansionistas acabariam aumentando o poder e o domínio de uma nação sobre a outra, assim como ajudariam a enfraquecer a capacidade que uma nação soberana tem de exercer seu próprio poder.[203]

Essa atuação poderia se dar tanto por meio das ameaças de "instrumentalismo", como de "autoritarismo". As primeiras, representadas, segundo o autor pelas ditas *Big Techs* norte-americanas, estariam ligadas à vigilância social em massa que, em última análise, seria utilizada como ferramenta de manipulação do comportamento dos cidadãos, influenciando opiniões e processos eleitorais por meio de técnicas como o *profiling* e

202 SAURA GARCÍA, Carlos. Digital expansionism and big tech companies: consequences in democracies of the European Union. **Humanities and Social Sciences Communications**, v. 11, n. 1, p. 448, 2024.

203 Ibid.

o *microtargeting*.[204] Já o autoritarismo, que, segundo o autor, estaria associado à China, acabaria se valendo de grandes empresas de tecnologia que monitorariam o comportamento dos cidadãos por meio de grandes fluxos de dados.[205] Ou seja, as mesmas dinâmicas podem ser utilizadas por finalidade comercial ou política, sendo a primeira associada ao instrumentalismo e a segunda ao autoritarismo.

Destaca-se, nesse sentido, o caso da atuação do Google que, em 2023, às vésperas da votação pela Câmara dos Deputados do Projeto de Lei conhecido como PL das Fake News, que regularia as plataformas digitais, decidiu colocar na página principal de seu buscador um link que conduzia os internautas a um texto que descrevia como o Projeto de Lei poderia piorar a internet dos brasileiros.[206] O episódio foi bastante relevante porque o impacto da conduta da empresa foi tão grande, que o Projeto de Lei foi retirado de pauta e nunca mais voltou a ser discutido. Importante notar, ainda, que a empresa não forneceu qualquer contraponto a visões distintas, o que acabou aumentando a repercussão do caso.

Como ressaltado por Daniel Cochrane, empresas como Alphabet (Google) e Meta passam a se valer de seu amplo domínio de mercado para moldar o discurso público e as narrativas políticas. Segundo ele, tais plataformas se revelam como atores partidários e tendenciosos, utilizando, ainda, "métodos reativos, proativos e cooperativos para publicar ou controlar informações de maneiras 'não uniformes' que 'podem influenciar as opiniões e escolhas dos usuários nas urnas'."[207] Tal desiderato é alcançado,

---

204 Ibid. Em relação ao conceito de "instrumentarismo", recomenda-se: ZUBOFF, Shoshana. **The Age of Surveillance Capitalism.** New York: PublicAffairs, 2019.

205 SAURA GARCÍA. Digital expansionism and big tech companies. Em relação ao conceito de "instrumentarismo", recomenda-se: ZUBOFF, Shoshana. **The Age of Surveillance Capitalism**. New York: PublicAffairs, 2019.

206 FONSECA, Bruno. Google pagou R$ 670 mil em anúncios contra o PL 2630. **Agência Pública**. Disponível em: <https://apublica.org/2023/05/google-pagou-mais-de-meio-milhao-de-reais-em-anuncios-no-facebook-contra-pl-das-fake-news/>. Acesso em: 10 nov. 2025; RODRIGUES, Alex. Notificada, Google retira link para texto contra PL das Fake News. **Agência Brasil**. Disponível em: <https://agenciabrasil.ebc.com.br/geral/noticia/2023-05/notificada-google-retira-link-para-texto-contra-pl-das-fake-news>. Acesso em: 10 nov. 2025.

207 COCHRANE, Daniel. **Big Tech's Power to Shape Public Discourse**. The Heritage Foundation. Disponível em: <https://www.heritage.org/big-tech/report/big-techs-power-shape-public-discourse>. Acesso em: 13 nov. 2025.

sobretudo levando-se em consideração o poder e a escala inerentes a estas plataformas, o que lhes confere vantagens consideráveis na moldagem das narrativas políticas segundo seus interesses próprios ou segundo interesses de Estado que possam vir a representar.[208]

Dentre os métodos específicos de manipulação elencados por Cochrane, pode-se destacar métodos reativos de manipulação, como restrições baseadas em discurso ou indivíduo, restrição ao alcance de conteúdo (ex: *shadow banning*) e restrição de credibilidade percebida (ex: por meio de rotulagem e *fact-checking*). Além disso, em relação aos métodos proativos de manipulação, o autor alude à manipulação de feeds e resultados de busca, avisos e experiências direcionadas (como visto no caso do Google no Brasil em relação ao PL das Fake News), personalização do ambiente informacional de cada usuário e, finalmente, o chamado *prebunking,* que se referiria a novas técnicas de manipulação social projetadas com o objetivo último de "inocular" psicologicamente os eleitores contra a chamada "desinformação". Finalmente, e não menos importante, Cochrane alude aos métodos cooperativos de manipulação, por meio do qual as Big Techs estariam fazendo parcerias "com outros atores para vigiar e analisar a dissidência política com o objetivo de aprender a moldá-la ou combatê-la por meios abertos e secretos."[209]

Focando no cenário norte-americano, Cochrane destaca que essas novas formas de atuação se diferenciam das tradicionais e já reguladas formas de contribuições políticas, o que as torna especialmente perigosas.[210] Dito de outra maneira, é como se as plataformas exercessem uma espécie de *lobby* social, por meio do qual alteram as narrativas e controlam a integridade informacional que, em última análise, acaba reverberando na atuação dos parlamentares, já que estes querem sempre agradar as suas bases.

Isso não exclui, todavia, as formas tradicionais de pressão política, como o *lobby*, que, no Brasil, não é regulamentado de forma específica, como o é nos Estados Unidos da América. Nessa direção, em recente reportagem, a agência de jornalismo investigativo "Pública" trouxe bastidores inéditos da atuação dos *lobbies* realizados por empresas estrangeiras

208 *Ibid*.

209 *Ibid*.

210 *Ibid*.

neste e em outros episódios, incluindo a descrição de reuniões a portas fechadas com a participação de diversos parlamentares e políticos.[211]

Por fim, é preciso reconhecer que lideranças influentes no campo da IA têm utilizado suas posições de poder em empresas do setor para manipular a opinião pública em benefício de interesses políticos e econômicos pessoais, em detrimento do interesse público.[212] A baixa taxa de sucesso de projetos-piloto de IA generativa, somada à volatilidade dos mercados de infraestrutura digital, indica que o entusiasmo generalizado não corresponde ao estado efetivo de maturidade tecnológica.

Esse tipo de atuação evidencia um uso estratégico e calculado de poder tecnológico para moldar políticas públicas em favor de projetos privados. Tais narrativas, ao serem amplificadas em meios de comunicação e plataformas de redes sociais, frequentemente controladas pelas maiores empresas de IA, moldam a percepção pública e influenciam decisões de investimento, políticas industriais e debates regulatórios.

Nesse contexto, torna-se evidente a necessidade de pesquisa sólida que identifique de forma objetiva os desenvolvimentos tecnológicos reais e reconheça quando narrativas estão distorcidas e informe a capacidade situacional de governos nacionais, e a regulação adequada das plataformas para evitar que narrativas distorcidas cheguem a serem disseminadas junto com desinformação.

Recentemente, a revista The Economist vislumbrava um cenário em que a Alphabet (por meio de Google e YouTube) e a Meta (por meio de Instagram e Facebook) poderiam vir a ser pressionadas, mediante promessas ou ameaças, a alinhar suas políticas de inteligência artificial e moderação de conteúdo a uma agenda política do governo estadunidense.[213] Legalmente, empresas como Alphabet e Meta têm a obrigação fiduciária de maximizar o valor para seus acionistas, o que cria incentivos fortes para que

---

211 SCOFIELD, Laura; VIANA, Natalia. **Como as Big Techs mataram o PL das Fake News**. Agência Pública. Disponível em: <https://apublica.org/2025/09/como-as-big-techs-mataram-o-pl-das-fake-news/>. Acesso em: 10 nov. 2025.

212 MARCUS, Gary. Sam Altman's pants are totally on fire; PAGE, Amba Kakarchive; PAGE, Sarah Myers Westarchive; PAGE, Meredith Whittakerarchive. **Make no mistake - AI is owned by Big Tech**, MIT Technology Review. Disponível em: <https://www.technologyreview.com/2023/12/05/1084393/make-no-mistake-ai-is-owned-by-big-tech/>. Acesso em: 16 nov. 2025.

213 Donald Trump is trying to silence his critics. He will fail. **The Economist**, 2025.

atendam a pressões políticas percebidas, principalmente quando a recusa pode ameaçar a estabilidade e os lucros da companhia.

Essa dinâmica pode acabar resultando, por exemplo, em escolhas estratégicas em relação à moderação de conteúdo que favoreçam determinados partidos políticos. Nota-se, nessa direção, o fato relacionado à rápida desativação do programa de checagem de fatos da Meta e a significativa redução da moderação de conteúdo poucos dias depois da posse do presidente Trump em 2025, o que poderia conduzir à interpretação de se tratar de uma possível – e rápida – resposta a pressões políticas, além da busca pela redução de alegações de "censura" que teriam se traduzido no risco de redução de lucro para acionistas. Essa decisão da liderança da Meta indica, portanto, que a política de conteúdo é claramente definida com base nos interesses políticos do governo estadunidense e dos acionistas da própria empresa, o que pode acontecer caso as empresas decidam seguir as diretrizes políticas.

Como se pode observar, as mudanças na moderação da Meta após 2025 ajudam a demonstrar como essas empresas podem se ajustar rapidamente a cálculos políticos e acionários, revelando uma potencial submissão a interesses de governos e econômicos; o que, em última análise, pode resultar em atuação transnacional que interfira na construção regulatória de outros países, em clara violação à soberania. Essa situação também evidencia as preocupações contínuas sobre a responsabilidade, transparência e legitimidade democrática na governança do conteúdo em plataformas digitais.

Ressalta-se, ademais, que não há problemas em um país soberano buscar pressionar outro país soberano a tomar determinada atitude. O grande problema está na atuação sub-reptícia voltada a manipular a opinião pública ou grupos específicos por meio de estruturas tecnológicas sob seu próprio controle. Tal tendência é particularmente evidente no âmbito do fenômeno de "captura discursiva" pelo qual um certo discurso ou conceito é esvaziado de seu significado original e realinhado para servir a um legado ideológico específico. Isso implica a apropriação e manipulação do sentido para fins opostos ao propósito emancipatório ou progressista do discurso original.

Nesse sentido, Rafael Grohmann e Alexandre Costa Barbosa apresentam o processo de "*sovereignty-as-a-service*" segundo o qual as *Big Techs*, especialmente Microsoft, Amazon e Google/Alphabet, estariam, nos úl-

timos anos, redefinindo, de forma estratégica, o conceito de soberania digital valendo-se de seus programas de infraestrutura em nuvem (*cloud infrastructure*), o qual é amplamente dominado por essas empresas, que teriam um controle de cerca de 2/3 do mercado global. Ou seja: em vez de garantir que as pessoas e também Estados pudessem exercer suas soberanias nas plataformas, as empresas parecem conduzir à ideia de que esta soberania é exercida como uma forma de serviço prestado por elas, seguindo seus próprios termos e lógicas. Segundo os autores, esta estratégia é capaz de esvaziar o próprio conceito de soberania digital, além de permitir a promoção de um alinhamento ideológico com o pensamento do Vale do Silício.[214]

Na literalidade de Grohmann e Barbosa: "Trata-se de uma forma de captura discursiva em que as empresas de plataforma definem as condições sob as quais outros, sejam indivíduos, corporações ou mesmo governos, podem ser considerados "soberanos", dependendo de seus recursos e capacidades infraestruturais. Em vez de a soberania ser exercida sobre as plataformas, ela agora é concedida por elas, por meio de ferramentas e serviços que reproduzem a dependência de suas infraestruturas."[215]

O perigo, ressaltado pelos autores, é que pode acabar havendo uma captura do discurso público, já que, por meio das ditas "nuvens soberanas", os Estados poderiam manter um discurso meramente propagandístico de "soberania digital", enquanto, em verdade, esta não estaria sendo alcançada em termos práticos. Assim, conforme as empresas passam a dominar as agendas nacionais, "a pressão por estruturas regulatórias e políticas que realmente abordem a soberania digital, tanto da perspectiva do Estado quanto da comunidade, enfraquece, reforçando assim a dependência das plataformas (Grohmann, 2025), particularmente em relação às infraestruturas."[216]

Cabe frisar que este perigo é tudo menos teórico, como ilustra o recente anúncio da "OpenAI soberana para a Alemanha", uma iniciativa apresentada como uma inteligência artificial soberana alemã, desenvolvi-

214 Sovereignty-as-a-service: How big tech companies co-opt and redefines digital sovereignty. **Media, Culture & Society**. Disponível em: <https://journals.sagepub.com/doi/epub/10.1177/01634437251395003>. Acesso em: 17 nov. 2025.

215 *Ibid*.

216 *Ibid*.

da em parceria pela OpenAI, Microsoft e SAP.[217] Embora seja promovida como um projeto que reforça a soberania tecnológica e a autonomia nacional no setor público, na prática, a total capitulação alemã é evidente, não somente em termos tecnológicos, mas da própria narrativa divulgada, esvaziando o conceito de soberania digital para justificar o alinhamento a interesses das Big Techs.

2.3 A complexidade institucional das camadas da pilha: rumo a um sistema de soberania digital

Cada componente da "pilha" mencionada acima está inserido em um complexo contexto institucional formado por entidades públicas e privadas e variados conjuntos normativos. Construir uma visão sistêmica[218] sobre a soberania digital, que entenda o funcionamento e as interações de todos os elementos da pilha, requer a capacidade de percepção situacional para mapear e reconhecer a interrelação dinâmica entre os subsistemas de:

- **Políticas públicas**: incluindo os atores que participam da sua elaboração, implementação e avaliação. Isso inclui entidades do Poder Público, especialmente o Executivo por meio de seus Ministérios (particularmente aqueles com competências específicas como MCTI, MGI, MDIC etc.), bem como representantes do setor produtivo, da academia e da sociedade civil.
- **Financiamento**: incluindo atores públicos e privados que atuem no financiamento de ações pertinentes, especialmente pesquisa, desenvolvimento e inovação (PD&I). Atores estatais como FINEP e as fundações de amparo à pesquisa estarão mais proximamente envolvidos em etapas de pesquisa e desenvolvimento,

217 SAP; OPENAI. **SAP and OpenAI partner to launch sovereign 'OpenAI for Germany'**. Disponível em: <https://openai.com/global-affairs/openai-for-germany/>. Acesso em: 13 nov. 2025.

218 CASSIOLATO, José Eduardo; LASTRES, Helena; SOARES, Maria Clara. The Brazilian national system of innovation: challenges to sustainability and inclusive development, *in*: DUTRÉNIT, Gabriela; SUTZ, Judith (Orgs.). **National Innovation Systems, Social Inclusion and Development**, [s.l.]: Edward Elgar Publishing, 2014.

provendo financiamento paciente e de longo prazo[219], enquanto financiadores como bancos de desenvolvimento (BNDES, bancos de desenvolvimento estaduais) e arranjos privados de investimento atuarão em etapas de inovação de menor incerteza.

- **Pesquisa e desenvolvimento**: incluindo instituições científicas e tecnológicas que atuem em pesquisa básica e aplicada, como universidades, fundações e unidades de pesquisa situadas em empresas públicas e privadas.
- **Construção de capacidades**: envolvendo organizações que atuam na formação de profissionais e incorporação do progresso técnico, como universidades públicas e privadas, institutos de pesquisa e redes de formação profissional (e.g., organizações do Sistema S[220]).
- **Monitoramento das evoluções do mercado**: referente à formação de demanda e oferta para tecnologias desenvolvidas no país, incluindo o uso do poder de compra do Estado como força motriz do desenvolvimento tecnológico, bem como a canais de informação e retroalimentação entre atores do mercado de modo a informar trajetórias tecnológicas que se adequem às necessidades da indústria e da sociedade brasileira.
- **Acompanhamento das evoluções do contexto geopolítico**: obrigações derivadas de tratados e outros instrumentos internacionais (e.g., obrigações relativas à propriedade intelectual derivadas do acordo TRIPS[221]), políticas implementadas por outros países, especialmente aqueles que contêm nós importantes de sistemas globais de inovação em tecnologias digitais.

---

219 MAZZUCATO, Mariana. **The Entrepreneurial State**. London: Penguin, 2018.

220 O Sistema S engloba entidades privadas sem fim lucrativo, mantidas por contribuições obrigatórias das empresas associadas, que oferecem serviços sociais de interesse público, incluindo capacitação profissional. Sistema S. Disponível em: <https://pt.wikipedia.org/w/index.php?title=Sistema_S&oldid=71870781>. Acesso em: 25 mar. 2026.

221 Acordo sobre Aspectos de Propriedade Intelectual Relacionados ao Comércio (TRIPS), um acordo, firmado no âmbito da Organização Mundial do Comércio, que estabelece padrões mínimos de proteção à propriedade intelectual pelos Estados signatários.

- **Acompanhamento das evoluções do contexto social e cultural**: as normas sociais e os hábitos funcionam como uma modalidade de regulação que influencia o uso e a adoção de tecnologias ao estabelecer padrões de comportamento compartilhados e expectativas dentro de uma comunidade, regulando indiretamente por meio da pressão social e da internalização de práticas.

Do ponto de vista organizacional, aponta-se para a necessidade de coordenação entre os atores do sistema, especialmente na execução de políticas públicas, sob a lente da soberania digital. Ou seja, que as políticas públicas relativas a cada componente da pilha de soberania digital estejam conectadas sob o objetivo estratégico da promoção da soberania digital do país, e que tal articulação seja institucionalmente estável e coerente, representando uma política de Estado, mais do que uma política de governo. Da mesma forma, é preciso conectar e coordenar os diversos atores dos subsistemas mencionados acima na perspectiva de se garantir estabilidade e coerência para que o sistema de soberania digital possa permitir uma autonomia tecnológica continua e sustentável.

Na prática, isso se traduz na adoção de arranjos de governança que facilitem entendimentos compartilhados a respeito dos objetivos de política pública, e na melhor exploração, dos arranjos existentes, como o Comitê Interministerial para a Transformação Digital (CITDigital) e seu Comitê Consultivo. Por exemplo, na adoção de uma estratégia e plano de ação relativos à Inteligência Artificial no país, é de crucial importância o seu entrecruzamento a esforços pretéritos e prospectivos de planejamento estatal, alavancando as instâncias consultivas existentes para elaboração de uma visão de soberania digital que possa ser embutida numa nova Estratégia Brasileira para Transformação Digital (que deveria ser lançada no segundo semestre de 2026). Desse modo, a condução da IA no país deveria impulsionar a construção de um ecossistema digital soberano enquanto permite o cumprimento dos documentos existentes, como a atual E-Digital 2022-2026, o Plano Nacional de Internet das Coisas, as prioridades para projetos de ciência, tecnologia e inovação do MCTI, a Estratégia Nacional de Governo Digital 2024-2027 e o plano de neoindustrialização "Nova Indústria Brasil" (NIB).

Algumas ações desse último documento em missões específicas revelam algum grau de cruzamento entre prioridades de políticas públicas

no sentido da promoção da soberania digital, com particular atenção à IA. Por exemplo, a consideração de demandas por tecnologias baseadas em IA do Complexo Econômico-Industrial da Saúde brasileiro e a utilização de diversas linhas de financiamento do programa Mais Inovação Brasil relacionadas a transportes, agroindústria, saúde e infraestrutura para promoção de digitalização, desenvolvimento e adoção de soluções de IA na indústria nacional[222].

Como destacamos acima, é importante que esse arranjo institucional e regulatório esteja acompanhado de uma visão estratégica focada na incorporação do progresso técnico e capacidades tecnológicas na cadeia produtiva nacional, ou seja, uma visão de desenvolvimento assentada na inovação e na autonomia tecnológica. Experiências nacionais anteriores, como o esforço de construção e fortalecimento do complexo eletrônico no país por meio da Lei de Informática, indicam caminhos a se tomar e a se evitar. A formação de um quadro institucional voltado para o fortalecimento da demanda no país e a incorporação das etapas produtivas foram dificultados, no desenho e aplicação do sistema idealizado pela Lei de Informática, por evidentes desalinhamentos entre as ferramentas e objetivos construídos no marco legal em um primeiro momento e entre os processos burocráticos e as capacidades dos entes afetados pela lei. Além do mais, as decisões políticas daquele momento levaram a uma mudança de rumo e de horizonte para o desenvolvimento tecnológico nacional.

Nesse sentido, a segunda Lei de Informática deve ser entendida no contexto mais amplo de abertura econômica e reorientação das políticas industriais no início da década de 1990. O abandono da reserva de mercado e a ênfase em incentivos fiscais acabaram abrindo espaço para a entrada de empresas estrangeiras altamente competitivas, o que enfraqueceu ainda mais as empresas nacionais de informática que haviam surgido durante a vigência da primeira lei. Apesar de as duas leis e suas implementações não serem isentas de críticas, essa experiência ilustra eloquentemente que a falta de estabilidade e coerência implementadas podem se demonstrar fatais.

222 COSTA, Viviane da; GASPAR, Walter Britto; JOHANSSON, Germano, Brazilian. AI Sovereignty: an agenda evaluation. In: BELLI, Luca; MAGALHÃES, Larissa (Orgs.). **AI Sovereignty and AI Governance: Perspectives from the BRICS and Beyond**, [s.l.: s.n.], 2026, em preparação para publicação.

A trajetória da Cobra Computadores ilustra esse movimento: criada com forte apoio estatal para garantir autonomia tecnológica em setores estratégicos, a empresa viu sua capacidade de competir internacionalmente enfraquecer diante da nova configuração institucional, sendo posteriormente incorporada pelo Banco do Brasil e convertida em prestadora de serviços de TI. Mais do que o texto legal em si, foi essa mudança desorganizada e incoerente de orientação nas políticas de desenvolvimento que prejudicou o papel da indústria brasileira de informática. O deslocamento do eixo de fortalecimento de capacidades domésticas rumo à integração subordinada e desorganizada às cadeias globais de produção determinou o fracasso das Leis de Informática.

Do conjunto de experiências acumuladas, é possível extrair tanto acertos quanto erros relevantes. Dentre os acertos, destacam-se a formação de mão de obra qualificada, a criação de um ambiente de pesquisa em universidades e centros tecnológicos e o fortalecimento de um debate nacional sobre autonomia tecnológica, elementos que permanecem como ativos estratégicos. Por outro lado, os erros envolvem a dificuldade de alinhar os instrumentos de política aos objetivos declarados, a criação de um regime de incentivos que favoreceu grandes empresas em detrimento de atores emergentes e a incapacidade de sustentar competitividade após a abertura do mercado. Esses aprendizados apontam para a necessidade de políticas – e de mecanismos de implementação de tais políticas – mais consistentes, que combinem estímulo à inovação com apoio estratégico, inclusive por meio de contratos públicos, como destacaremos na seção 5.2., e integração equilibrada às cadeias globais.

Assim, a experiência brasileira com a Lei da Informática evidencia que arranjos institucionais fragmentados e políticas de inovação mal calibradas podem enfraquecer dinâmicas internas e comprometer a sustentabilidade de setores estratégicos. O exemplo demonstra, portanto, a importância uma estratégia de inovação que inclua políticas diretas e indiretas, horizontais e verticais[223] e do alinhamento de incentivos e instrumentos a

223 PROCHNIK, Victor et al. A política da política industrial: o caso da Lei de Informática. **Revista Brasileira de Inovação**, v. 14, p. 133–152, 2015.
GARCIA, Renato; ROSELINO, José Eduardo. Uma avaliação da Lei de Informática e de seus resultados como instrumento indutor de desenvolvimento tecnológico e industrial. **Gestão & Produção**, v. 11, p. 177-185, 2004.

uma estratégia clara de fortalecimento das capacidades nacionais, capaz de combinar mecanismos de proteção, estímulos à concorrência e políticas de compras públicas. Mais do que uma lição histórica, trata-se de um alerta sobre a centralidade de coordenação entre Estado, setor produtivo e instituições de pesquisa para que o esforço de inovação e desenvolvimento tecnológico produza resultados duradouros.

De modo geral, a conjunção entre a consideração dos componentes da pilha da soberania digital e uma visão sistêmica do contexto institucional de desenvolvimento e difusão de novas tecnologias no Brasil desenha o desafio que se interpõe ao país em termos de coordenação regulatória e de políticas públicas. A soberania digital, como eixo orientador dessa coordenação, deverá estar contida nos esforços de composição e implementação de estratégias e políticas para o desenvolvimento brasileiro de maneira autônoma e quanto mais autóctone.

2.4 O *India Stack*: modelo de pilha de soberania digital?

O denominado "*India Stack*"[224] configura-se como um caso paradigmático de estrutura em camadas (que compõem uma pilha ou *stack*, em inglês) destinada a promover soberania digital por meio de uma arquitetura sistêmica construída por meio de blocos essenciais. Tais blocos, baseados em protocolos abertos, agem como componentes interoperáveis: identidade digital (Aadhaar), infraestrutura de pagamentos (UPI), serviços de consentimento e APIs que viabilizam a oferta de serviços públicos e privados integrados. Enquanto estratégia de transformação digital, o *India Stack* expressa uma lógica de modularidade que permite a operacionalização de políticas públicas de escala nacional; enquanto objeto de análise jurídico-política, constitui um exemplo rico para examinar como uma pilha tecnológica pode articular autonomia operacional, inclusão e riscos de concentração de poder.

A literatura acadêmica recente descreve o *India Stack* como um conjunto de "infraestruturas públicas digitais" (ou DPI, do inglês *Digital Public Infrastructure*) que combinam protocolos abertos, registos centrais e

224 **India Stack**. Disponível em: <https://indiastack.org/>. Acesso em: 25 set. 2025.

interfaces padronizadas, criando um ecossistema no qual atores públicos e privados interoperam sob regras técnicas definidas.[225] Essa configuração favoreceu uma rápida difusão de serviços digitais – nomeadamente pagamentos instantâneos (UPI que pode ser considerado como a inspiração para o Pix[226]) e a identificação eletrônica – e gerou externalidades positivas para inclusão financeira e eficiência administrativa. Cabe ressaltar que o sucesso na adoção de tais infraestruturas, porém, não teria sido possível sem o aumento maciço da conectividade significativa ao longo da última década, o que pode ser visto como o impacto extremamente positivo – e até essencial – das regras rigorosas de neutralidade de rede, adotadas em 2016, as quais proibiram as práticas de *zero rating* na Índia, promoveram a concorrência e estimularam o acesso à inovação doméstica, ao mesmo tempo em que garantiram aos indianos uma conexão à Internet não discriminatória e de melhor qualidade.[227]

No entanto, análises críticas enfatizam que a eficácia da pilha depende de enquadramentos legais fortes, governança de dados e salvaguardas de privacidade que limitem desvios e usos indevidos. Smriti Parsheera e outros autores destacam os riscos políticos e econômicos associados à consolidação de uma "Alt-Big-Tech" em torno de DPIs.[228] A crítica central reside em que componentes públicos altamente padronizados podem, paradoxalmente, criar pontos de captura por atores privados que, mediante integração preferencial, transformam vantagens infraestruturais em poder de mercado. Consequentemente, a experiência indiana nos mostra que a soberania digital exige não apenas construção de DPIs, mas também regras explícitas de

225 SENGUPTA, Amrita; BARBOSA, Alexandre Costa; SAMDUB, Mila T. Understanding interrelationships between AI and digital public infrastructure (DPI) in India and Brazil. **The African Journal of Information and Communication (AJIC)**, n. 35, p. 1-11, 2025.

226 BELLI, Luca; JIANG, Min. Conclusion: Digital Sovereignty in the BRICS: Structuring Self-Determination, Cybersecurity, and Control. In: JIANG, Min; BELLI, Luca (Orgs.). **Digital Sovereignty in the BRICS Countries**. 1. ed. Cambridge: Cambridge University Press, 2025, p. 214–238. Disponível em: <https://www.cambridge.org/core/product/identifier/9781009531085%23CN-bp-10/type/book_part>. Acesso em: 23 set. 2025.

227 *Ibid*.; BELLI, Luca. **Building Good Digital Sovereignty through Digital Public Infrastructures and Digital Commons in India and Brazil**. In: BELLI, Luca; MAGALHÃES, Larissa, **AI Sovereignty and AI Governance: Perspectives from the BRICS and Beyond**, [s.l.: s.n.], 2026.

228 PARSHEERA, Stack is the New Black? In: BELLI; MAGALHÃES, **AI Sovereignty and AI Governance: Perspectives from the BRICS and Beyond**.

acesso não discriminatório, gestão de APIs, governança de dados e cibersegurança para garantir direitos, transparência e *accountability*, e regimes de concorrência que evitem a privatização de benefícios públicos.

Em avaliação crítica do percurso indiano em matéria de IA e soberania tecnológica, a pesquisadora Jai Vipra assinala a necessidade de coerência estratégica entre capacidade computacional, proteção de dados e cibersegurança para que uma "pilha de soberania" cumpra seus propósitos sem gerar vulnerabilidades sistêmicas.[229]

A integração de módulos (identidade, pagamentos, serviços de dados) deve, portanto, ser acompanhada por instrumentos jurídicos que assegurem responsabilização, transparência algorítmica e mitigação de riscos sistêmicos, elementos sem os quais a pilha torna-se uma infraestrutura potente, mas juridicamente frágil e incapaz de garantir o pleno gozo de direitos fundamentais.

Sendo assim, do ponto de vista institucional e regulatório, o modelo da pilha apresenta vantagens, mas também impõe desafios complexos: como repartir responsabilidades entre operadores de infraestrutura, fornecedores de serviços e reguladores; como estabelecer padrões de interoperabilidade juridicamente vinculantes; e como garantir recursos para manutenção e atualizações. Estudos comparativos recomendam um quadro tripartido: (i) normas técnicas vinculantes (APIs, padrões de segurança), (ii) obrigações de proteção de dados e de governança de consentimento, e (iii) mecanismos de supervisão independente que tenham capacidade técnica para auditar e sancionar.[230] Sem essas salvaguardas, a pilha pode favorecer a captura e reduzir a *accountability* democrática.

Finalmente, em termos de soberania em IA, o *India Stack* exemplifica como infraestruturas públicas digitais têm o potencial de fornecer bases para modelos de desenvolvimento digital "soberanos", isto é, sistemas treinados sobre bases de dados locais, com acesso fiscalizado e controlado por normas públicas. Contudo, para que a pilha se converta em alavanca

229 VIPRA, Jai. Towards AI sovereignty: The good, the bad, and the ugly of AI policy in India. **The African Journal of Information and Communication (AJIC)**, n. 35, p. 1-11, 2025.

230 DRAPER *et al*, **A Consumer-centric Approach to DPIs for sustainable financial inclusion**; SENGUPTA; BARBOSA; SAMDUB, Understanding interrelationships between AI and digital public infrastructure (DPI) in India and Brazil; In: BELLI; MAGALHÃES, **AI Sovereignty and AI Governance: Perspectives from the BRICS and Beyond**; PARSHEERA, Stack is the New Black?

verdadeira de autonomia tecnológica é necessário: investimento em capacidades computacionais nacionais, políticas de *open source* e interoperabilidade, e regimes legais de acesso, proteção e segurança de dados que conciliem inovação e direitos fundamentais. A experiência indiana ilustra, assim, tanto as possibilidades quanto os riscos da abordagem "por camadas": potencial para inclusão e autonomia; vulnerabilidade à captura e necessidade de governança robusta.

3 Consequências da falta de soberania digital

A ausência de uma configuração institucional, política e regulatória capaz de entender as dimensões da soberania digital expõe países a inúmeros riscos. Como analisaremos neste capítulo, tais riscos abrangem desde a perda de ganhos financeiros até o eventual comprometimento de sua capacidade de entender o funcionamento social, econômico e democrático e organizar a prestação de serviços essenciais, e a perda de controle e autonomia estratégica sobre ativos críticos, como dados, softwares, hardwares, recursos energéticos e minerais, resultando em um esvaziamento da soberania nacional.

Isto é, ao passo que as diferentes camadas da pilha de soberania digital são desafiadas, não somente de forma pontual, mas também de forma sistêmica, desenvolve-se um ciclo vicioso em que a ausência de soberania digital fragiliza fundamentos da autonomia nacional. A história recente evidenciou exemplos ilustrativos de riscos que vêm se concretizando na sociedade brasileira e em países do Sul Global.[231]

3.1 Dependência da nuvem estrangeira, perda de controle informacional e fenômeno do *vendor lock-in*

Em sinergia com a onda de digitalização acelerada pela pandemia de Covid-19, funções básicas de governos, como educação, saúde e finanças, vêm progressivamente sendo adaptadas para o ambiente digital. Esse esforço de digitalização foi impulsionado pela popularização de soluções de armazenamento e processamento em nuvem. A tecnologia de nuvem, por sua vez, é ancorada em servidores e *data centers* concentrados principalmente nos EUA e na Europa, e de maneira crescente na China.[232]

231 BELLI, Luca; GASPAR, Walter Britto (Orgs.). **AI from the Global Majority: Official outcome of the UN IGF Data and Artificial Intelligence Governance Coalition**. Rio de Janeiro: FGV Direito Rio, 2024.

232 **Data Center Map - Colocation, Cloud and Connectivity**, Disponível em: <https://www.datacentermap.com/>. Acesso em: 12 nov. 2025.

Como sublinhamos na seção 2, entidades, tanto da esfera pública quanto privada, têm progressivamente migrado para computação em nuvem, em prol da celeridade e da comodidade operacional. Esse processo se concretiza por meio da implementação de um arcabouço complexo de soluções, usualmente geridas por corporações estrangeiras e fundamentadas em softwares proprietários ou em plataformas no modelo de *Software as a Service* (SaaS) disponibilizadas via computação em nuvem *(cloud computing*). Uma vez incorporadas, tais soluções tornam-se de difícil substituição. Isso ocorre em razão da subordinação tecnológica instituída pela própria arquitetura subjacente a essas inovações que geram, portanto, vulnerabilidades e dependências estruturais.

De um lado, o preço inerente a essa "comodidade" reside na mitigação ou até eliminação da autonomia e do controle sobre informações – podendo abarcar dados pessoais sensíveis ou informações estratégicas e críticas – e sobre as operações cruciais para o funcionamento das empresas ou das administrações públicas. De outro lado, a condição de dependência (*vendor lock-in*) frente a um provedor específico de serviços em nuvem acarreta a materialização de custos de transação exorbitantes para uma eventual migração ou substituição de plataforma.[233] Tais custos abrangem não apenas os encargos financeiros diretos, mas também os riscos operacionais, a necessidade de reestruturação de processos internos e o treinamento de pessoal, configurando uma barreira econômica substancial à portabilidade dos dados e à livre concorrência no setor de tecnologia.

Assim, embora suscite facilidades inerentes às tecnologias digitais para os usuários e clientes destas empresas, o uso da nuvem pode gerar riscos práticos e estratégicos, ao serem fornecidas principalmente por provedores estrangeiros, enquanto o Estado perde a capacidade de entender o funcionamento de tais serviços, desenvolvê-los e regulá-los efetivamente ou até simplesmente mudar a escolha de provedores. Isto é, ao passo que algumas das maiores empresas de tecnologia dominam o mercado de nuvem, elas passam a permear toda a cadeia produtiva de setores que, ao se

233 OPARA-MARTINS, Justice; SAHANDI, Reza; TIAN, Feng. Critical analysis of vendor lock-in and its impact on cloud computing migration: a business perspective. **Journal of Cloud Computing**, v. 5, n. 1, p. 4, 2016;
KUMAR, Purushottam; KUMAR, Dr Prakash. **Vendor Lock-In Situation and Threats in Cloud Computing**, v. 7, n. 9, 2022.

digitalizarem, se tornam intrinsicamente dependentes de tais soluções de nuvem, bem como das informações dos usuários armazenados na nuvem.

Como resultado, gera-se um contexto de dependência de empresas, usuários, pessoas físicas e governos em relação aos serviços de nuvem prestados pelas gigantes dominantes no mercado. Essas *big techs*, por sua vez, além de ganhar os valores pecuniários pagos para prestar os serviços em nuvem, ganham acesso privilegiado às informações e empresas operando em suas nuvens, adquirindo um insight único e extremamente valioso para selecionar quais empreendimentos são estrategicamente relevantes e para direcionar investimentos.

Essa capacidade, por seu turno, resulta na possibilidade de controle de setores tecnológicos inteiros, mediante investimentos e tutorias de startups e empresas emergentes que passam a contar com investidores de *big techs* com ampla compreensão do mercado – oriundo de seu acesso privilegiado às informações armazenadas em seus servidores de nuvem e comportamento de seus clientes. Ao concentrar os serviços de nuvem, portanto, as *big techs* contam com uma consciência situacional que as torna capazes de comprar empresas e encerrar suas atividades ou investir em iniciativas especificas que correspondam aos seus interesses, moldando, portanto, o setor competitivo.[234]

Não obstante a possibilidade de controle setorial do mercado, a dependência de serviços de nuvem estrangeiros também se torna evidente na medida em que infraestruturas críticas e serviços essenciais são continuamente integrados e ancorados nesses serviços de nuvem, de forma que o uso da nuvem estrangeira pode resultar em um esvaziamento da autonomia do Estado – e, por extensão, da de seus cidadãos, empresas e administrações públicas. Isso ocorre porque funções públicas e privadas são fundamentadas em serviços de empresas estrangeiras sobre os quais entidades e população brasileiras perdem o controle e que invariavelmente

234 RIKAP, Cecilia. **Big Tech: Not Only Market But Also Knowledge and Information Gatekeepers**. Institute for New Economic Thinking. Disponível em: <https://www.ineteconomics.org/perspectives/blog/big-tech-not-only-market-but-also-knowledge-and-information-gatekeepers>. Acesso em: 19 set. 2025.
RIKAP, Cecilia, **Dynamics of Corporate Governance Beyond Ownership in AI**. Disponível em: <https://www.common-wealth.org/publications/dynamics-of-corporate-governance-beyond-ownership-in-ai>. Acesso em: 19 set. 2025.

estão sujeitas à soberania de outro Estado. Como resultado, empresas e governos ficam presos (*locked-in)* a soluções específicas de nuvem, pertencentes aos atores dominantes do mercado.

Nesse cenário, além da perda de autonomia estatal, serviços públicos e privados de um país tornam-se vulneráveis a falhas ou decisões unilaterais de provedores e empresas estrangeiras, enquanto bases de dados nacionais, altamente valiosas e únicas, são capturadas e usadas gratuitamente para treinar e melhorar sistemas de IA estrangeiros, que serão em seguida vendidos "como serviço" ("*as a Service*") a quem trabalhou gratuitamente para desenvolvê-los.[235]

A situação na qual somente empresas estrangeiras detêm o controle sobre como serviços essenciais e dados nacionais e de cidadãos brasileiros estão sendo utilizados coloca a população inteira à mercê da lógica decisória de administradores estrangeiros, os quais, por sua vez, obedecem à lógica de mercados, que pode evoluir em tendências extrativistas e a busca de renda[236]– e, em situações específicas, também a determinações dos seus governos de origem. Notoriamente, tal lógica e determinações são frequentemente incompatíveis com a maximização de direitos fundamentais conforme a Constituição brasileira, que é a natureza dos próprios serviços públicos. Ademais, eventuais decisões acerca do tratamento e transferência de dados não necessariamente estarão em consonância com o arcabouço legal local, como a LGPD (ou o RGPD, no caso de usuários europeus), mas acabam sendo estabelecidas essencialmente por meio da arquitetura técnica e a regulação contratual definidas privadamente pelas empresas com base em seus próprios interesses privados na legislação estrangeira.[237]

---

235 BELLI, Luca et al. Proteção de dados, tributação de dados e equidade de dados: equilíbrio entre valores, riscos e obrigações.

236 Este ponto não é incluído para criticar lógicas de mercado mais que legítimas, mas para que o leitor possa entender que o comportamento natural de qualquer empresa não é de considerar impacto socioeconômico, ambiental ou sobre direitos humanos ou evitar uma dinâmica extrativista. Tais impactos serão avaliados e seus efeitos negativos mitigados somente em presença de obrigações legislativas fiscalizadas por autoridades capazes de entender o funcionamento dos sistemas a serem fiscalizados e aplicar sanções de maneira efetiva.

237 BELLI, Luca. **Structural Power as a Critical Element of Social Media Platforms' Private Sovereignty**. In: BELLI, Luca; MAGALHÃES, Larissa (orgs.). *AI Sovereignty and AI Governance: Perspectives from the BRICS and Beyond*. [S.l.: s.n.], 2026. No prelo.

Ainda nessa trilha, os riscos que a privacidade e a proteção dos dados dos usuários já enfrentavam vêm sendo acelerados pela adoção de modelos de IA desenvolvidos e implementados com base nos dados previamente coletados por outras finalidades ou raspados em larga escala na Internet sem que haja uma base legal adequada. Um exemplo é a popularização de sistemas de armazenamento de fotos e vídeos na nuvem, que foi acompanhada de sistemas de IA capazes de editar fotos e/ou de organizar as coleções de fotos, identificando pessoas ou locais ao longo do tempo, recorrendo a um mapeamento efetivo da biometria de usuários ao redor do mundo, que acabam aderindo a estes modelos de negócio de forma compulsória (e por padrão) conforme são embutidos em atualizações de sistemas operacionais de dispositivos conectados como smartphones (sem, portanto, cumprir com as devidas obrigações de transparência e base legal para o respectivo tratamento de dados).[238]

Além disso, a dependência de serviços de computação em nuvem estrangeiros adquire uma clara dimensão geopolítica – ocorrências como o cancelamento da hospedagem do site de denúncias WikiLeaks pela Amazon.com, em 2010, em razão de pressões políticas exercidas pela equipe do então senador Joe Lieberman, à época presidente do Comitê de Segurança Interna do Senado norte-americano[239]; as revelações de Edward Snowden sobre espionagem em escala global, desde 2001; e o recente caso do procurador-chefe do Tribunal Penal Internacional, cujo acesso a serviços Microsoft foi bloqueado como consequência das sanções adotadas contra o tribunal pela administração Trump[240] ilustram de maneira paradigmática como o controle sobre infraestruturas digitais pode ser mobilizado para

238 DAVE, Paresh. This Website Shows How Much Google's AI Can Glean From Your Photos. **Wired**, 2024; LANDYMORE, Frank. **Meta Is Being Incredibly Sketchy About Training Its AI on Your Private Photos**. Futurism. Disponível em: <https://futurism.com/meta-sketchy-training-ai-private-photos>. Acesso em: 10 nov. 2025.

239 MACASKILL, Ewen. WikiLeaks website pulled by Amazon after US political pressure, **WikiLeaks website pulled by Amazon after US political pressure**, 2010.

240 O episódio sucedeu o período em que o então presidente Donald Trump havia imposto sanções ao Tribunal, em resposta à decisão de um painel de juízes que expediu mandados de prisão contra o primeiro-ministro israelense Benjamin Netanyahu e o então ministro da Defesa, Yoav Gallant. **Trump's sanctions on ICC prosecutor have halted tribunal's work**, AP News. Disponível em: <https://apnews.com/article/icc-trump-sanctions-karim-khan-court-a4b4c02751ab84c09718b1b95cbd5db3>. Acesso em: 10 out. 2025.

fins políticos e estratégicos, expondo indivíduos e instituições a riscos extremamente elevados.

Esses acontecimentos revelaram práticas sistemáticas de monitoramento e espionagem envolvendo cidadãos, empresas e líderes mundiais, e uso estratégico da tecnologia para estender globalmente o alcance da jurisdição dos EUA por meio de agentes privados, evidenciando os riscos geopolíticos da dependência tecnológica, além da assimetria de poder informacional entre Estados e *big techs*. A concentração da infraestrutura digital em território norte-americano, notadamente pela localização dos servidores das maiores empresas de tecnologia estadunidenses, constituiu elemento central para a facilitação e legitimação jurídica do acesso da *National Security Agency* (NSA) a dados de usuários em escala global, e a obrigação de cooperação de empresas estadunidenses com a NSA conforme a Seção 702 do FISA[241], levantando debates relevantes sobre soberania digital, extraterritorialidade e governança da internet.[242]

Os Estados Unidos também já expressaram preocupação similar em relação à China, especialmente após a aprovação, em 2017, da Lei de Inteligência Nacional, que determina que empresas chinesas devem "apoiar, cooperar e colaborar com o trabalho de inteligência nacional".[243] Esse dispositivo normativo intensificou receios de que o governo chinês pudesse utilizar equipamentos essenciais para a renovação da infraestrutura de telecomunicações e acesso à Internet como instrumento de vigilância e expansão de sua capacidade de espionagem.[244] Nesse contexto, Estados Uni-

241 A Seção 702 da Lei de Vigilância de Inteligência Estrangeira (FISA) dos Estados Unidos autoriza a coleta do conteúdo de comunicações de pessoas que estejam fora dos EUA, principalmente estrangeiros, sem a necessidade de mandado judicial individual. Essa disposição foi criada para permitir a vigilância de estrangeiros vivendo fora do território americano, com o objetivo de combater terrorismo e crimes cibernéticos, entre outras ameaças. A seção concede amplos poderes para que agências como a NSA coletem dados massivos de comunicações eletrônicas de fornecedores de tecnologia nos EUA, como Meta e AT&T, com supervisão governamental formal, mas é alvo de críticas por causar riscos à privacidade e direitos civis. **Foreign Intelligence Surveillance Act**. Disponível em: <https://irp.fas.org/agency/doj/fisa/>. Acesso em: 9 out. 2025.

242 GASPAR, Walter; BELLI, Luca; JASWANT, Smriti, Data Sovereignty and Data Transfers as Fundamental Elements of Digital Transformation, *in*: **AI Sovereignty and AI Governance: Perspectives from the BRICS and Beyond.**, [s.l.: s.n.], 2026.

243 中华人民共和国国家情报法 (National Intelligence Law of the People's Republic of China).

244 Huawei: Por que os EUA consideram a gigante chinesa de tecnologia uma ameaça à segurança nacional, 2018.

dos, Austrália e Nova Zelândia proibiram o uso da tecnologia da Huawei no desenvolvimento de redes 5G e, paralelamente, países como Canadá, Alemanha, Japão e Coreia do Sul optaram por manter a Huawei sob avaliação regulatória, o que demonstra a difusão global de preocupações sobre a interseção entre soberania digital, segurança cibernética e competição tecnológica estratégica.[245]

Apesar dessas medidas e respostas, insta salientar que os Estados Unidos também dispõem de legislação de natureza semelhante. O CLOUD Act, aprovado em 2018 durante o primeiro governo Trump, autoriza as autoridades norte-americanas a requisitarem dados armazenados por empresas do país, independentemente da localização física dos servidores.[246] Tal ato normativo tem suscitado apreensão em diversas jurisdições, uma vez que projeta a extraterritorialidade da legislação estadunidense sobre fluxos globais de dados. A Holanda, por exemplo, em reação a resultados divulgados em relatório do Tribunal de Contas do país, manifestou preocupação em relação à dependência de órgãos governamentais dos serviços de computação em nuvem fornecidos pelas grandes empresas norte-americanas, reconhecendo os riscos de soberania digital e vulnerabilidade institucional associados a essa concentração.[247]

Por derradeiro, cabe ressaltar o caso emblemático mencionado acima em que a Microsoft cancelou o endereço de e-mail e bloqueou acesso aos próprios serviços de Karim Khan, promotor-chefe do Tribunal Penal Internacional.[248] O episódio evidencia e reforça a vulnerabilidade de pessoas físicas e jurídicas e até de instituições internacionais diante da dependência de infraestruturas tecnológicas controladas por empresas privadas estrangeiras, além de ilustrar os impactos geopolíticos decorrentes da interseção entre sanções estatais, (falta de) soberania digital e poder corporativo. Em

245 *Ibid*.

246 U.S. CONGRESS, Clarifying Lawful Overseas Use of Data Act (CLOUD Act).

247 DESMARAIS, Anna. **Is overreliance on US Big Tech a threat to Europe? The Netherlands may soon find out.** Euronews, 2025.

248 KREMPL, Stefan, Criminal Court: Microsoft's email block a wake-up call for digital sovereignty. **Heise Online**, 2025THE TIMES OF INDIA (TOI). Trump's sanctions on ICC prosecutor said to have halted tribunals work, 2025;
MICROSOFT allegedly blocked the email of the Chief Prosecutor of the International Criminal Court. 2025.

outras palavras, a ausência de alternativas autônomas e soberanas, ou a falta de suporte ao uso de tais alternativas[249], favorece a disponibilidade de dados de usuários nacionais para empresas estrangeiras que exploram estes dados conforme os seus interesses econômicos, estratégicos e/ou sujeitos às pressões dos governos de origem destas empresas.

Esse cenário não é menos preocupante no que se refere ao nível de cooperação estrita entre as empresas de tecnologia e forças armadas estrangeiras. Conforme anunciado pelo Exército dos EUA em junho de 2025, executivos de alto nível da Meta, OpenAI e Palantir ingressaram na Reserva do Exército, recebendo o grau de tenentes-coronéis, integrando o novo *Executive Innovation Corps* "para reduzir a lacuna tecnológica entre os setores comercial e militar, com quatro líderes de tecnologia previstos para se juntar como oficiais".[250] O fato de que executivos de empresas de tecnologia de tamanha relevância global sejam oficiais do exército em tempo parcial torna latente a aproximação entre forças armadas e grandes empresas de tecnologia estadunidenses. Simultaneamente, evidencia o nível de capilaridade e acesso que forças armadas estrangeiras passam a ter nas infraestruturas críticas e serviços sociais nacionais. Como resultado, devido à falta de soberania digital, pode haver, em última consequência, uma erosão da própria soberania nacional.

3.2 Desertificação do ecossistema digital nacional

Cabe frisar que a dependência tecnológica também gera efeitos negativos sobre a própria capacidade do ecossistema local de inovar de forma

249 Cabe ressaltar que existem múltiplas alternativas aos serviços corporativos e educacionais fornecidos por empresas como Microsoft e Google, sendo particularmente evidente a ausência de direcionamento de investimento público em tais alternativas no país. Assim, como destacaremos na próxima seção, as administrações públicas brasileiras gastam enormes recursos em soluções corporativas estrangeiras que poderiam ser substituídas relativamente facilmente por alternativas nacionais, determinando ao mesmo tempo uma poupança para os cofres públicos e um investimento essencial para desenvolver e fortalecer o ecossistema digital nacional.

250 Segundo o site do exército, Shyam Sankar, diretor de tecnologia da Palantir; Andrew Bosworth, diretor de tecnologia da Meta; Kevin Weil, diretor de produto da OpenAI; e Bob McGrew, conselheiro do Thinking Machines Lab e ex-diretor de pesquisa da OpenAI ingressam na nova unidade. **Army Launches Detachment 201: Executive Innovation Corps to Drive Tech Transformation**, www.army.mil, Disponível em: <https://www.army.mil/article/286317/army_launches_detachment_201_executive_innovation_corps_to_drive_tech_transformation>. Acesso em: 10 out. 2025.

independente. A estruturação da inovação como interna às infraestruturas predominantes não somente é suscetível de comprometer o crescimento da economia nacional, mas pode enviesar a forma em que o processo de inovação acontece, reduzindo ou até eliminando inovações disruptivas que poderiam levar à adoção de novos paradigmas tecnológicos.

Esse conjunto de dinâmicas revela um fenômeno mais profundo do que a mera concentração econômica: trata-se de um processo ecossistêmico de exaustão da inovação alheia e de homogeneização tecnológica. À medida que as grandes plataformas assumem o papel de infraestruturas universais, a margem de autonomia dos atores locais se estreita, e as possibilidades de inovação independente se reduzem. Essa transformação progressiva pode ser descrita como um processo de desertificação do ecossistema digital, isto é, o esvaziamento da diversidade tecnológica, institucional e cognitiva, que se agrava ainda mais em um sistema nacional dependente, diante da concentração estrutural de poder computacional e informacional em poucos centros globais.

O fenômeno que definimos como desertificação digital se torna uma consequência estrutural de dependência tecnológica e informacional[251]. Ocorre quando um ecossistema digital perde, ou reduz, sua capacidade de gerar inovação de forma autônoma e plural, passando a reproduzir padrões, modelos de negócios e tecnologias definidas externamente. Assim como a desertificação ambiental resulta do uso predatório de recursos naturais[252], a desertificação digital decorre do uso predatório dos dados[253], da atenção dos usuários[254] e da infraestrutura pública. Em ambos os casos, o resultado é o

---

251 COULDRY, Nick; MEJIAS, Ulises A. Data Colonialism: Rethinking Big Data's Relation to the Contemporary Subject. **Television & New Media**, v. 20, n. 4, p. 336–349, 2019; ROVENSKAYA, Elena *et al*, An ecological perspective to master the complexities of the digital economy, **npj Complexity**, v. 2, n. 1, p. 16, 2025.

252 NETO, José Francisco da Cruz *et al*. Desertificação: uma visão geral dos processos e conceitos, fundamentados em aplicação de índices orbitais através do sensoriamento remoto. **Research, Society and Development**, v. 10, n. 11, p. e585101119950–e585101119950, 2021.

253 CHAGNON, C. W. et al. **From extractivism to global extractivism: the evolution of an organizing concept**, n. 49(4), p. 760-792;
WU, Tim. **The Age of Extraction: How Tech Platforms Conquered the Economy and Threaten Our Future Prosperity**, [s.l.]: Knopf, 2025.

254 ZUBOFF, Shoshana. **The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power**. New York: PublicAffairs, 2019.

mesmo: a perda da (bio)diversidade – natural ou informacional – e a dependência estrutural de quem detém os meios de produção e circulação.

No contexto brasileiro, esse processo manifesta-se de maneira particularmente clara na combinação entre a ausência de coordenação estatal[255], migração de infraestruturas públicas para nuvens estrangeiras[256], fragilidade das políticas industriais[257] e limites na fiscalização da regulamentação sobre proteção e segurança de dados. A dependência estrutural de provedores estrangeiros para serviços essenciais, desde armazenamento de dados até inteligência artificial, cria um cenário em que a inovação local se torna residual, dependente de interfaces e padrões impostos por quem define as arquiteturas – tipicamente proprietárias – dos sistemas.

Como destacamos nesta seção, as consequências desse processo são múltiplas. No plano econômico, a desertificação digital enfraquece as cadeias nacionais de valor tecnológico, esvazia o investimento privado em inovação autônoma e consolida assim uma espécie de "inovação subordinada", onde inovações locais ou disruptivas são absorvidas, contidas ou inviabilizadas por grandes plataformas que definem o padrão dominante[258]. No plano político, limita a capacidade à autonomia política e desestrutura o espaço público informacional, transformando o país em mero usuário de tecnologias, incapaz de influenciar seus próprios destinos; e, no plano social, reforça as desigualdades regionais e dependências estruturais, criando vazios digitais, onde pode até existir níveis de conectividade e letramento digital, mas faltam alternativas locais de produção, inovação e controle de dados.

Particularmente, *big techs* controladoras de infraestruturas de nuvem podem definir prioridades, elaborar e aplicar seletivamente as suas políticas de forma a incentivar inovações que pressupõem a utilização da sua

255 BARRIOS, Lucas de Góis. Soberania, Planejamento Estatal e Transformação Digital: análise comparada dos instrumentos jurídicos da União Europeia e do Brasil, v. 2, n. 1, 2023; MELLO, Gustavo Bernardes, **Governança por missões no Brasil: um olhar sobre os desafios de Coordenação na Nova Indústria Brasil a partir da transformação digital.** Escola Nacional de Administração Pública - Enap, 2025.

256 GINGLASS, Mário Roberto. **Soberania e uso de tecnologias emergentes e de serviços de computação em nuvem por empresas públicas federais no Brasil**. Escola Superior de Guerra, 2024.

257 MELO, Ricardo Lacerda de. Soberania Digital e Desenvolvimento: um olhar crítico sobre as possibilidades e limites do Brasil nas tecnologias digitais. Entrevista com José Eduardo Cassiolato, v. 26, n. 3, 2024.

258 SHAXSON, Nicholas; ROCK, Brianna; BLANKERTZ, Aline. **Google's Hidden Empire**, 2025.

própria infraestrutura. Essa tendência é demonstrada, por exemplo, pela grande utilização desses provedores no setor público na Holanda, onde em recursos humanos é registrado um número sempre crescente de funcionários com competências específicas da Amazon Web Services[259].

No contexto latino-americano, o Banco Interamericano de Desenvolvimento afirma que o tipo mais comum de empresas de base tecnológica é composto por empresas regionais de internet voltadas para o consumidor que replicam e adaptam ao mercado local o modelo de empresas americanas bem-sucedidas que ainda não se estabeleceram na região. Rikap et al. acrescentam a isso um estudo de caso do Mercado Livre[260] que corrobora a visão de Sunkel sobre o potencial efeito negativo da aliança entre corporações multinacionais e setores manufatureiros locais no Brasil, que, segundo ele, reproduziu padrões de consumo e tecnológicos do núcleo, levando a um setor industrial cada vez mais dependente e transnacionalizado.[261] Rikap também ilustra em outro estudo de casos a captura pela Microsoft, Amazon, Meta e Google da inovação no contexto da inteligência artificial por meio de estratégias diferentes, mas que em geral dependem da colaboração com outros atores e o fornecimento de tecnologia.[262]

A tendência de trabalhar em harmonia com, e não contra os grandes provedores de infraestrutura, se encontra nas empresas que atuam como complementadores de um orquestrador: ou seja, de quem oferece a infraestrutura em cima da qual diversos produtos e serviços podem ser distribuídos, no intuito de produzir valor para o consumidor de forma conjunta. Nesse contexto, a capacidade de empresas complementares evoluírem em conjunto com o ator central de um ecossistema torna-se especialmente pressionada quando as inovações introduzidas pelo orquestrador afetam a estrutura de

259 CATH, Corinne. **Clouds Over the Netherlands: Preserving Public Interest Internet Governance in the Era of Hyperscaler Clouds**. Amsterdam: Zenodo, 2025.

260 FRANCO, Sebastián Fernández; GRAÑA, Juan M.; RIKAP, Cecilia. Dependency in the Digital Age? The Experience of Mercado Libre in Latin America. **Development and Change**, v. 55, n. 3, p. 429-464, 2024.

261 SUNKEL, Oswaldo. **Capitalismo Transnacional y desintegración nacional en américa latina**. Buenos Aires: Ediciones Nueva Visión, 2025.

262 RIKAP, Cecilia. Varieties of corporate innovation systems and their interplay with global and national systems: Amazon, Facebook, Google and Microsoft's strategies to produce and appropriate artificial intelligence. **Review of International Political Economy**, v. 31, n. 6, p. 1735-1763, 2024.

interconexão das soluções.[263] Nesses casos, não se trata de reinventar o núcleo tecnológico, mas de reorganizar a forma como os elementos se articulam entre si – alteração que, embora sutil em aparência, costuma redistribuir funções, competências e dependências dentro do ecossistema.[264]

Em arranjos desse tipo, o foco estratégico não consiste apenas em "vencer" os concorrentes, mas em construir compatibilidade e coordenação entre os participantes. Como observa Adner, a lógica dos ecossistemas desloca a preocupação central da busca por superioridade competitiva para a busca por alinhamento entre os agentes que compõem o sistema[265]. Portanto, os complementadores que conseguem ajustar tanto sua base tecnológica quanto seus ritmos operacionais ao líder do ecossistema estão mais preparados para absorver – e eventualmente aproveitar – os efeitos provocados por mudanças estruturais dessa natureza. Segundo Zheng et al., esse ajuste ocorre em duas frentes[266]. A primeira consiste em adotar tecnologias e componentes definidos pelo líder, internalizando os padrões técnicos dominantes. A segunda envolve sincronizar processos, etapas de implementação e timing com a sequência ditada pelo centro do ecossistema. Quando combinadas, essas duas dimensões funcionam como engrenagens de coordenação, permitindo navegar transições arquitetônicas com menor atrito.

Além disso, não se trata apenas de uma questão de alinhar a oferta dentro de determinado padrão tecnológico, mas também de incentivos a investir em tecnologias que destoam desse padrão ou que tentam competir com o orquestrador do ecossistema. Por exemplo, uma pesquisa de Kamepalli et al. encontrou um efeito negativo referente às aquisições acima de US$ 500 milhões realizadas por grandes operadoras de plataformas, em particular Google e Facebook: a queda de mais de 40% no investimento de capital de risco em startups no mesmo setor de uma empresa adquirida

263 ZHANG, Pengxiang *et al*. Marching to the Beat: The Role of Complementor Alignment in the Architectural Evolution of Ecosystems. **Journal of Management**, p. 01492063251368267, 2025.

264 HENDERSON, Rebecca M.; CLARK, Kim B. Architectural Innovation: The Reconfiguration of Existing Product Technologies and the Failure of Established Firms. **Administrative Science Quarterly**, v. 35, n. 1, p. 9, 1990.

265 ADNER, Ron. Ecosystem as Structure: An Actionable Construct for Strategy. **Journal of Management**, v. 43, n. 1, p. 39-58, 2017.

266 ZHANG et al. Marching to the Beat.

pelo Google e Facebook, e de 20% no número de negócios, nos três anos seguintes à aquisição[267].

Segundo os autores, isso sugere a existência de uma chamada "kill zone", ou seja, uma área onde uma operadora de plataforma consegue usar as informações que recebe para copiar e reproduzir versões de baixo custo dos produtos de melhor desempenho na plataforma, desviando os consumidores do produto original.

Ao mesmo tempo, as preocupações por trás da "zona morta" não precisam ser medidas necessariamente pelos efeitos sobre os investimentos: efeitos prejudiciais na dinâmica da concorrência no mercado de complementadores após a entrada de uma plataforma também podem ser apresentados como evidência de algum tipo de "zona morta". Nesse sentido, a literatura empresarial documentou que vendedores terceirizados afetados pela entrada da Amazon são desencorajados e oferecem menos produtos[268], e até mesmo a mera ameaça de entrada do Google em um mercado de aplicativos Android é suficiente para fazer com que os fornecedores de aplicativos estabelecidos aumentem os preços e reduzam os esforços de inovação[269].

Assim, enfrentar a desertificação digital de maneira efetiva exige estratégias de reconstrução do ecossistema, articulando capacidades estatais, políticas industriais e regulação ativa. A soberania digital pode, nesse sentido, ser entendida como um projeto que busca reverter a desertificação e restaurar as condições de diversidade, autonomia e redistribuição de poder no ambiente digital.

3.3 Plataformas digitais patrocinadas como concentradoras de dados, intermediadoras da economia e mediadoras da esfera pública

Como já destacamos, os dados pessoais são considerados o "recurso mais valioso do mundo" há mais de duas décadas e, para coletá-los, alguns

267 KAMEPALLI, Sai Krishna; RAJAN, Raghuram G.; ZINGALES, Luigi. Kill Zone, 2020.

268 ZHU, Feng; LIU, Qihong. Competing with complementors: an empirical look at Amazon.com. **Strategic Management Journal**, v. 39, n. 10, p. 2618–2642, 2018.

269 WEN, Wen; ZHU, Feng. How Do Complementors Respond to the Threat of Platform Owner Entry? Evidence from the Mobile App Market. **SSRN Electronic Journal**, 2016.

provedores de aplicativos chegam a patrocinar taxas de acesso aos seus próprios aplicativos. Apesar de ser potencialmente muito mais valioso "cloudificar" serviços públicos e privados, criando dependências duradouras graças às quais pode ser extraído valor por períodos de tempos muito maiores, a coleta de dados permanece um objetivo essencial de grandes empresas de tecnologia, especialmente em amplos mercados emergentes sobre os quais existe um potencial ainda inexplorado, em termos de coleta de dados. Nesse contexto, para o seleto grupo de provedores com capacidade econômica necessária, vale a pena subsidiar taxas de acesso aos próprios aplicativos para conseguir concentrar artificialmente a atenção e, consequentemente, a coleta de dados do usuário – e, cada vez mais, documentos e material que possa ser usado para treinar sistemas de IA – em seus aplicativos patrocinados.

Modelos de patrocínio de aplicativo, conhecidos como as práticas já referidas de "*zero rating*" surgiram no contexto de uma verdadeira "Corrida por Dados"[270] ao longo da última década, período em que os participantes do mercado lutam para capturar a atenção dos usuários e, consequentemente, concentrar a coleta de seus dados pessoais. Nesse contexto, para os provedores mais abastados – tipicamente redes sociais dominantes como as aplicações do grupo Meta – revela-se vantajoso patrocinar taxas de acesso aos próprios aplicativos para concentrar artificialmente a atenção e acostumar o usuário a seus serviços.

Assim, cabe destacar que uma estratégia cada vez mais adotada por provedores de aplicativos é buscar criar verdadeiras "dependências"[271] dos próprios usuários por seus serviços, por meio de configurações de aplicativos viciantes e estratégias de mercados voltadas a manter o engajamento por meio de hábitos artificialmente criados, partindo do pressuposto de que o aplicativo mais bem-sucedido não é aquele com os melhores recursos, mas aquele que consegue capturar e manter a atenção dos usuários por mais tempo.[272] Cabe lembrar que a criação de um hábito é uma maneira extremamen-

---

270 BELLI, Luca. **The scramble for data and the need for network self-determination**. OpenDemocracy. Disponível em: <https://www.opendemocracy.net/en/scramble-for-data-and-need-for-network-self-determination/>. Acesso em: 10 nov. 2025.

271 EYAL; HOOVER, **Hooked**.

272 HARRIS, Tristan, **How Technology is Hijacking Your Mind — from a Former Insider**, Thrive Global. Disponível em: <https://medium.com/thrive-global/how-technology-hijacks-peoples-minds-from-a-magician-and-google-s-design-ethicist-56d62ef5edf3>. Acesso em: 10 nov. 2025.

te efetiva de se regular o comportamento humano e, neste sentido, o patrocínio de aplicativos visa cada vez mais alavancar o hábito e até a dependência psicológica do usuário, como estratégia de regulação do comportamento.

Especialmente quando o acesso subsidiado a alguns aplicativos é combinado com a imposição de franquias de dados muito limitadas, como acontece na maioria dos países do sul global[273], os usuários da Internet podem ter um forte incentivo para acessar apenas aplicativos patrocinados. Com efeito, somente os aplicativos patrocinados, que são apresentados e percebidos como "de graça", serão acessados sem limites e constantemente pelo usuário, enquanto o acesso ao resto da Internet será artificialmente reduzido porque percebido como caro, implicando a necessidade de consumar a franquia e, portanto, ter um gasto monetário para a enorme maioria da população que usa planos pré-pagos[274]. Tal raciocínio pode ser especialmente relevante para os usuários menos abastados, que são a grande maioria dos usuários, especialmente em países de renda média e baixa como o Brasil.[275] Ao patrocinar uma seleção limitada de aplicativos enquanto prevê um pagamento pelo acesso aberto à Internet, há um risco tangível de transformação da Internet, como uma rede de propósito geral, em uma rede de propósito pré-definido onde os usuários se tornam consumidores passivos, cuja atenção pode ser direcionada facilmente para serviços pré-selecionados, em vez de escolherem com base em critérios de qualidade e até serem capazes de produzir inovação e compartilhá-la livremente, para competir em pé de igualdade com os serviços já existentes.

De fato, desde 2018 o IBGE destaca que 94,5% dos usuários de Internet móvel no país utilizam sua conexão principalmente por meio de

---

273 Para mais informações, ver **Zero Rating**. Disponível em: <https://zerorating.wordpress.com/>. Acesso em: 12 nov. 2025.

274 NIC.BR. **Conectividade significativa: propostas para medição e o retrato da população no Brasil**. São Paulo: CGI.br, 2024.

275 No Brasil, aproximadamente 80% da população faz parte das chamadas classes C, D e E, que representam os indivíduos menos ricos, de acordo com estatísticas oficiais. Embora os números mais recentes disponíveis tenham sido alterados – negativamente – pela pandemia de Covid-19, dados muito recentes nos permitem afirmar que 63% da população combinada das classes C, D e E autoimpõem restrições no uso da internet, para evitar o consumo da franquia mensal de dados. Veja IDEC; INSTITUTO LOCOMOTIVA. **Acesso à internet móvel pelas classes CDE**.

aplicativos de mensagens instantâneas e redes sociais[276]: revela-se legítimo, então, questionar se esse uso exorbitante das redes sociais representa uma escolha voluntária dos brasileiros ou um hábito artificialmente formado, sendo as redes sociais com tarifa zero a única opção para os usuários mais desfavorecidos (ou seja, a enorme maioria da população). Portanto, pode-se argumentar que, sem nem perceber, os brasileiros estão se acostumando a usar serviços patrocinados, devido ao seu hábito (ou vício) em tais serviços patrocinados, que é propositalmente estimulado não apenas pela natureza viciante do design desses serviços, mas também pelo fato de serem os únicos percebidos como gratuitos (porém de fato pagos com dados).

Em uma economia orientada por dados, limitar e direcionar a navegação dos usuários para pouquíssimos serviços – ou até eliminar esta necessidade ao fornecer diretamente respostas elaboradas por IA generativa, cujo conteúdo será subsequentemente monetizado por meio de propaganda direcionada[277] – torna-se muito mais lucrativo do que deixar os indivíduos explorarem livremente a rede e construírem novos serviços inovadores e concorrentes. O Brasil é um exemplo revelador de como a adoção generalizada de ofertas de z*ero rating* tende a reduzir a abertura da internet, visto que esses planos de internet móvel direcionam e, *de fato,* restringem a experiência da internet móvel a um número limitado de aplicativos subsidiados.[278] No Brasil, apenas as redes sociais dominantes – notadamente as de propriedade da Meta, como Facebook, WhatsApp e Instagram – e um número muito limitado de aplicativos que, geralmente, são integrados verticalmente com operadoras de telefonia móvel estão incluídas em planos de zero rating.

---

276 **PNAD Contínua TIC 2016: 94,2% das pessoas que utilizaram a Internet o fizeram para trocar mensagens |** Agência de Notícias - IBGE. 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: 14 out. 2025.

277 **Meta pretende usar chats com IA para anunciar produtos**. CNN Brasil. Disponível em: <https://www.cnnbrasil.com.br/tecnologia/meta-pretende-usar-chats-com-ia-para-anunciar-produtos/>. Acesso em: 10 out. 2025.

278 **Neutralidade da rede, o zero-rating e o Marco Civil da Internet**, vLex. Disponível em: <https://vlex.com.br/vid/neutralidade-da-rede-zero-800704285>. Acesso em: 15 nov. 2025; **Neutralidade de rede e ordem econômica**. Omci.gov.br. Disponível em: <https://www.omci.org.br/jurisprudencia/207/neutralidade-de-rede-e-ordem-economica/>. Acesso em: 15 nov. 2025.

Essa perspectiva adquire particular relevância no cenário atual, em que *chatbots* de IA generativa estão sendo instalados automaticamente nas redes sociais patrocinadas (é o caso do Meta.AI nas redes sociais do grupo) para fornecer respostas diretas a qualquer consulta do usuário, a fim de direcionar a atenção do internauta para o conteúdo gerado por IA, em vez de direcioná-la à página da web usada para produzir a resposta gerada por IA. Neste contexto, cabe reiterar que parece altamente improvável que, apesar dos investimentos previstos no recente PBIA, os consumidores brasileiros usem as tecnologias de IA que tais investimentos visam produzir, considerando que a enorme maioria da população continuará tendo acesso somente aos sistemas embutidos em planos de zero rating. Não é à toa que as empresas OpenAI e Perplexity resolveram assinar acordo com as operadoras Claro e Vivo para oferecer os próprios serviços de IA generativa em modalidade *zero-rating*[279]: como evidenciado pelas escolhas das duas empresas mencionadas acima, para os atores do mercado, se tornou essencial patrocinar seus próprios serviços para competir com os demais atores que vêm patrocinando, e portanto robustecendo, seu acesso a usuários e clientes ao redor do mundo, em especial em populações de países emergentes.[280]

Assim, essa prática concentra a atenção e a coleta de dados de toda uma população em acelerado processo de digitalização, nas mãos de um número muito limitado de provedores estrangeiros, que extraem e exportam ativos de dados extremamente valiosos – sem que sejam tributados – ao passo que os usuários treinam seus próprios serviços. Parece importante destacar que tais práticas podem ter um enorme impacto na concorrência, na capacidade de inovar, bem como na circulação de desinformação no país, quando a comunicação social se concentra em redes sociais patrocinadas, todas partes de um mesmo grupo econômico, com clara tendência a se alinhar politicamente com o governo estadunidense.[281]

---

279 TECMUNDO, **Vivo dá um ano de assinatura gratuita da IA Perplexity Pro aos clientes**; Claro fecha parceria com OpenAI para incluir ChatGPT em planos fixos e móveis.

280 **N° 82 - Novembre 2025**, Arcep. Disponível em: <https://www.arcep.fr/newsletters/le-post-new/n-82-novembre-2025.html>. Acesso em: 13 nov. 2025.

281 META, Mike IsaacMike Isaac has reported on; SINCE 2010, Its Apps, Mark Zuckerberg Defends Embrace of Trump Administration in Meta Q&A, **The New York Times**, 2025. JR, Gilberto Scofield, **Alliance between Meta and Trump is likely to create informational, economic and geopolitical conflicts around the world**, The Conversation. Disponível em: <http://

Nesse cenário, cabe sublinhar que a concentração de debates políticos, econômicos e sociais em plataformas patrocinadas cria riscos à integridade do processo democrático e à autonomia informacional do país.[282]

Como destacado recentemente pela revista The Economist, é mais que realista um cenário em que as maiores empresas de tecnologia estadunidenses possam eventualmente vir a ser pressionadas por promessas ou ameaças a alinhar suas políticas de inteligência artificial e moderação de conteúdo a uma agenda política do governo estadunidense.[283] Tal cenário, vislumbrado pela revista britânica, é menos hipotético do que poderia parecer, como destacaremos na seção seguinte.

3.4 Vulnerabilidade à manipulação cognitivo-informacional

Nos últimos anos, investimentos bilionários em infraestrutura de inteligência artificial têm sido fortemente impulsionados por narrativas estrategicamente construídas, que exploram tanto o "FOMO" (*fear of missing out* - medo de ficar para trás) quanto à falta de estratégias governamentais sobre soberania tecnológica e competitividade global. Essas narrativas são propagadas com grande eficácia pelas próprias empresas, que se beneficiam diretamente desses aportes, construindo um senso de urgência que muitas vezes supera análises críticas sobre os reais benefícios, riscos e alternativas. Assim, pode-se acabar criando uma percepção de que não investir imediatamente e em grande escala significaria comprometer o futuro econômico, militar e tecnológico de um país, o que, em verdade, revela-se como uma narrativa conveniente para quem vende as soluções.

Exemplo marcante está no discurso de Jensen Huang, CEO da NVIDIA, e outros líderes do setor, que frequentemente reforçam a ideia de que os Estados Unidos estão perdendo terreno para a China na corrida pela supremacia tecnológica, insinuando que a única forma de reverter esse cenário é por meio de investimentos massivos em infraestruturas de IA

theconversation.com/alliance-between-meta-and-trump-is-likely-to-create-informational-economic-and-geopolitical-conflicts-around-the-world-246872>. Acesso em: 10 out. 2025.

282 BELLI, Soberania em Inteligência Artificial: O que é e quais facilitadores essenciais podem tornar o Brasil um país soberano em IA?

283 "Donald Trump is trying to silence his critics. He will fail."

controladas por suas próprias empresas.[284] Essa retórica não só incentiva gastos públicos e privados exorbitantes, como também perpetua um ciclo de dependência tecnológica e concentração de poder nessas corporações. Com isso, tais empresas passam a moldar políticas públicas e mercados segundo seus interesses comerciais, ampliando sua influência e consolidando sua posição central no ecossistema tecnológico global.

Nesse contexto, a percepção situacional se torna essencial para conseguir tomar decisões com base em fatos e evitar narrativas enviesadas. Porém, como analisado no item referente ao FESIA da resiliência cognitivo-informacional, empresas estrangeiras, aliadas ou não a seus governos de origem, podem até chegar a interferir por meio do chamado *information warfare* em outros países, ou seja, implementando estratégias extremamente sofisticadas de manipulação de narrativas. Nesse contexto de Guerra Informacional, a atuação dessas empresas pode chegar a configurar aquilo que Pramod Kumar denomina Gestão da Percepção (*Perception Management*), e que consistiria, em síntese, em ações estratégicas levadas a cabo para fornecer ou ocultar informações selecionadas a audiências externas, com o intuito de influenciar suas emoções, motivações e raciocínio.[285] Nesse sentido, o objetivo final dessa tática é conseguir moldar as percepções de determinados grupos populacionais – como grupos de eleitores ou consumidores ou os próprios tomadores de decisões – a fim de assegurar que as ações e o comportamento dos alvos sejam favoráveis aos objetivos e intentos de quem as lança.

Cabe ressaltar que o *information warfare* se mostra como uma ferramenta que pode ser utilizada para induzir os alvos a cursos de ação de interesse do orquestrador.[286] Ou seja: impulsionadas ou não por seus países

---

284 LESWING, Kif, **Nvidia CEO Jensen Huang warns China is "not behind" in AI**, CNBC. Disponível em: <https://www.cnbc.com/2025/04/30/nvidia-ceo-jensen-huang-says-china-not-behind-in-ai.html>. Acesso em: 19 nov. 2025; PUBLISHED, Jowi Morales, **'China is going to win the AI race' — Nvidia CEO Jensen Huang decries the price of electricity in the US, contrasts it with China's subsidized pricing**, Tom's Hardware. Disponível em: <https://www.tomshardware.com/tech-industry/artificial-intelligence/china-is-going-to-win-the-ai-race-nvidia-ceo-jensen-huang-decries-the-price-of-electricity-in-the-us-contrasts-it-with-chinas-subsidized-pricing>. Acesso em: 19 nov. 2025.

285 KUMAR, Pramod, THE EVOLUTION OF INFORMATION WARFARE: FROM PROPAGANDA TO CYBERATTACKS.

286 *Ibid*.

de origem, empresas com capacidade de implementar *information warfare* podem se valer dessas táticas com o objetivo de manipular narrativas e consolidar suas agendas, que, ao fim e ao cabo, visam a atender a interesses de seus acionistas com os quais têm o dever jurídico de maximizar os lucros, ainda que isso signifique vilipendiar a soberania e a própria autonomia de um país soberano que se revele incapaz de resistir às investidas por elas perpetradas.

Nesse sentido, a corroborar esse risco, pode-se fazer referência a uma investigação transnacional coordenada pela Agência Pública, CLIP e Reporters Without Borders (RSF), que identificou quase 3000 ações de *lobby* de Google, Meta e outras empresas em dez países e na União Europeia. No entanto, a atuação dessas empresas vai além do exercício – por vezes, legítimo – do *lobby*. Isso porque, segundo achados do relatório, as empresas teriam lançado campanhas agressivas para enfraquecer ou até mesmo impedir a aprovação de leis sobre temas diversos, que envolviam desde a proteção de dados e a remuneração de conteúdo jornalístico até a transparência da moderação de conteúdo. O relatório ainda identificou as principais táticas utilizadas pelas empresas, como, por exemplo, contratações de ex-funcionários públicos (*revolving door lobbying*), financiamento de iniciativas civis ou acadêmicas que aparentam independência (*astroturfing*), argumentação de que leis nacionais não se aplicam a dados processados no exterior e, finalmente, campanhas de desinformação que apresentam regulação como censura ou ameaça à inovação.[287]

Como principal exemplo dessa atuação, pode-se retomar o já apresentado caso da atuação do Google que, em 2023, às vésperas da votação pela Câmara dos Deputados do Projeto de Lei conhecido como PL das Fake News, que regularia as plataformas digitais no Brasil, decidiu colocar na página principal de seu buscador um link que conduzia os internautas a um texto que descrevia como o Projeto de Lei poderia piorar a internet dos brasileiros.[288] Para agravar, “”[i]nvestigações apuraram que a empresa estaria indexando prioritariamente resultados de busca que referendavam

287 ROMEU, Artur, Big tech's attempts to weaken information space regulations worldwide exposed by new cross-country investigation supported by RSF, **Reporters Without Borders**, 2025.

288 FONSECA, **Google pagou R$ 670 mil em anúncios contra o PL 2630**. RODRIGUES, **Notificada, Google retira link para texto contra PL das Fake News**.

seus posicionamentos políticos contrários ao Projeto de Lei, em detrimento a outros posicionamentos."[289] Como consequência, a "Secretaria Nacional do Consumidor (SENACON) expediu ordem contra a Google para que retirasse a carta aberta de sua página principal, sob pena de multa milionária, uma vez que a empresa não diferenciou, para os usuários, que se tratava de uma publicidade em interesse próprio, e não de um resultado de pesquisa."[290]

Como visto, a relevância do episódio foi imensa, já que a conduta da empresa assumiu tamanha proporção, que o Projeto de Lei em causa foi retirado de pauta e nunca mais voltou a ser discutido, de modo a solapar, ainda que temporariamente, as tentativas brasileiras de regulação das plataformas de mídias sociais. Segundo Camila Pinheiro e Edwaldo Costa, a decisão de arquivamento do projeto "foi criticada por especialistas e organizações civis, que apontam prejuízos à democracia e à responsabilização das *big techs*, que continuam operando sem regulamentação eficaz, facilitando a propagação de desinformação e discursos de ódio no ambiente digital."[291] Importante, assim, verificar que a atuação do Google, atendendo aos seus interesses particulares, foi encarada pelos especialistas como danosa à democracia brasileira.

Ainda segundo os autores, "o papel das *big techs*, especialmente durante a tramitação legislativa, mostrou como interesses econômicos podem se sobrepor ao interesse público, moldando o debate a partir da lógica de engajamento e lucro."[292] E isso é fundamental num contexto em que a capacidade de regulação algorítmica desses agentes, que se caracteriza por métricas de atenção e também de opacidade decisória, acaba funcionando como "mecanismo estruturante do espaço público digital, afetando diretamente os processos de formação da opinião pública. Essa lógica não apenas amplia a circulação de conteúdos polarizadores, como restringe a

289 PEREIRA, Laurence Duarte Araújo; JÚNIOR, José Luiz de Moura Faleiros. Regulação das plataformas digitais no Brasil e a defesa da soberania nacional. **Revista de Ciências do Estado**, v. 9, n. 1, p. 1–22, 2024, p. 11.

290 *Ibid*.

291 PINHEIRO, Camilla; COSTA, Edwaldo. AS FAKE NEWS SOBRE O PL DAS FAKE NEWS: MANIPULAÇÃO ALGORÍTMICA NO DEBATE SOBRE REGULAÇÃO DAS PLATAFORMAS DIGITAIS NO BRASIL. **ARACÊ**, v. 7, n. 6, p. 30432–30455, 2025, p. 30451.

292 *Ibid*.

pluralidade informativa e compromete os princípios fundamentais da deliberação democrática."[293]

Dito diversamente, os países que ainda não conseguiram alcançar sua soberania tecnológica acabam por se tornar especialmente vulneráveis a essa influência na construção das narrativas e formação das agendas políticas, comprometendo sobremaneira a própria autonomia e autodeterminação que lhes deveria ser assegurada. E se isso é uma questão séria em um país de dimensões continentais e pujante desenvolvimento econômico como o Brasil, pode, certamente, ser ainda mais grave em países que não têm ainda a capacidade de resistir minimamente a esse tipo de influência estrangeira na erosão de seu tecido socioinformacional e, em última análise, de sua democracia.[294]

Nessa ordem de ideias, cabe ressaltar o trabalho do pesquisador Robert Epstein, que apresentou ao Senado norte-americano uma série de evidências de que o Google exibiria resultados de busca tendenciosos em favor de certos candidatos, naquilo que ele denominou de "Efeito de Manipulação do Mecanismo de Busca (*Search Engine Manipulation Effect*)."[295] Segundo Epstein, esta seria uma das formas de influência mais poderosas já descobertas e se daria quando resultados de busca tendenciosos passam a alterar as opiniões e preferências de voto de eleitores indecisos de maneira invisível ou "subliminar". Ainda, de acordo com seus achados, em razão da natureza apertada de muitas disputas ao redor do mundo e do grande poder de persuasão do Google, Epstein aponta que a empresa provavelmente "tem determinado os resultados de até 25% das eleições nacionais em todo o mundo desde pelo menos 2015."[296] Como exemplo local, ele menciona que nas eleições presidenciais norte-americanas de 2016, "resultados de busca tendenciosos gerados pelo algoritmo de busca do Google

293 *Ibid*., p. 30452.

294 PERSILY, Nathaniel; TUCKER, Joshua A. (Orgs.). **Social Media and Democracy**. Cambridge: Cambridge University Press, 2020. VAIDHYANATHAN, Siva. **Antisocial Media: How Facebook Disconnects Us and Undermines Democracy** [s.l.]: Oxford University Press, 2022.

295 EPSTEIN, Robert. **Why Google Poses a Serious Threat to Democracy, and How to End That Threat**. AIBRT, 16 jun. 2019. Disponível em: <https://www.judiciary.senate.gov/imo/media/doc/Epstein%20Testimony.pdf>. Acesso em: 15 nov. 2025.

296 *Ibid*.

provavelmente impactaram eleitores indecisos, resultando em um ganho de pelo menos 2,6 milhões de votos para Hillary Clinton."[297]

Corroborando esses argumentos em relação à violação à soberania, Laurence Duarte Araújo Pereira e José Luiz de Moura Faleiros Júnior observam que a atuação dessas Big Techs "tem impactado diversos governos e regimes políticos, ora servindo como meio para o exercício do debate e da atuação política online, ora atuando, as próprias plataformas, como agentes políticos em favor de seus interesses próprios ou de terceiros."[298] Isso porque "por meio do *lobby*, da mediação da comunicação e da opinião pública por meio de algoritmos e, não menos importante, por meio de seu grande poderio econômico, estas impõem limitações às próprias iniciativas regulatórias dos diversos Estados em que estão situadas."[299]

Por fim, como destacamos anteriormente, observa-se um relevante componente de distorção de narrativa por autopromoção empresarial. Um exemplo eloquente é a prática de vários atores do setor que consiste em propagar a narrativa de uma suposta iminência da inteligência artificial geral (AGI) não apenas por convicção técnica, mas porque tal narrativa funciona como instrumento para estimular investimentos contínuos em computação, infraestrutura e capital. Conforme críticas recentes, a AGI passou a operar quase como uma "construção ideológica" ou um arcabouço narrativo mobilizado para legitimar expansões massivas de infraestrutura e, em alguns casos, para postergar debates regulatórios indispensáveis.[300]

Essa dinâmica atende a interesses privados, e não ao interesse público. Se os tomadores de decisões, a comunidade regulatória e acadêmica, bem como o público *lato sensu* não se mostrarem capazes de resistir a tais manipulações narrativas, corre-se o risco de que recursos sejam direcionados a promessas especulativas em detrimento da análise das falhas já evidentes, dos limites técnicos presentes e das necessidades concretas de governança.

---

297 *Ibid*.

298 PEREIRA; JÚNIOR. Regulação das plataformas digitais no Brasil e a defesa da soberania nacional, p. 12.

299 *Ibid*.

300 PAGE, Will Douglas Heavenarchive. **How AGI became the most consequential conspiracy theory of our time**, MIT Technology Review. Disponível em: <https://www.technologyreview.com/2025/10/30/1127057/agi-conspiracy-theory-artifcial-general-intelligence/>. Acesso em: 16 nov. 2025.

Com efeito, um dos perigos mais imediatos diz respeito a decisões de investimento público e privado baseadas em premissas tecnológicas exageradas.[301] Outro risco significativo reside no uso estratégico do discurso sobre a necessidade de se avançar com urgência, para justificar a ausência de padrões robustos de segurança, gestão de riscos, auditoria e governança, criando um ambiente no qual sistemas imaturos são implementados sem avaliação adequada de impactos sociais ou jurídicos.

Além disso, a narrativa da iminência de uma Inteligência Artificial geral tem sido instrumentalizada para influenciar debates regulatórios, muitas vezes sugerindo que qualquer tipo de regulação poderia "atrasar" um progresso inevitável e essencial para os países. Essa estratégia, calculada e pensada, pressiona formuladores de políticas a adotar posições permissivas, ainda que faltem evidências concretas da proximidade de tais desenvolvimentos. No plano social, a circulação de desinformação em plataformas digitais intensifica percepções equivocadas, impactando a opinião pública, o consumo e a formulação de políticas.

Como se pode perceber, a atuação dessas empresas pode produzir impactos em países dos mais variados tamanhos e níveis de desenvolvimento. O que os difere, no entanto, é a maior ou menor vulnerabilidade a essas tentativas de manipulação cognitivo-informacional e a capacidade em resistir soberanamente.

3.5 Plataformas como entidades soberanas privadas com controle absoluto sobre seus ecossistemas digitais

De fato, uma das implicações da ausência de soberania digital estatal é a ocupação de posições economicamente estratégicas no espaço digital por agentes privados, que podem ser cooptados por governos estrangeiros nos quais tais atores são sediados.[302] Esses atores, ao se estabelecerem em pontos centrais da cadeia de valor – como no fornecimento de serviços de nuvem, destacado anteriormente –, passam a definir as estruturas técnicas essenciais para operar no ecossistema, tornando-se as únicas entidades capazes de sa-

301 **How AI Is Transforming Data Centers and Ramping Up Power Demand**.

302 BELLI, Structural Power as a Critical Element of Social Media Platforms' Private Sovereignty.

ber como todos os atores do sistema se comportam e de impor regras a seus usuários e parceiros comerciais, portanto reforçando seu poder econômico e adquirindo a capacidade de se apropriar do valor produzido por terceiros. Esse é justamente o desafio regulatório trazido pelos ecossistemas digitais[303], compreendidos como "um grupo de empresas que interagem e que dependem das atividades umas das outras… dependentes da liderança tecnológica de uma ou duas empresas que fornecem uma plataforma em torno da qual outros membros do sistema, fornecendo insumos e bens complementares, alinham os seus investimentos e estratégias".[304]

Tais ecossistemas controlados por grandes empresas de tecnologia lidam com complementaridades específicas e positivas, que não podem ser reproduzidas genericamente, o que exige a formação de uma rede particular de relações e alinhamentos voltados à geração de valor. Isso confere poder estrutural às plataformas[305]. Em outras palavras, as plataformas criam um ambiente de colaboração com terceiros – os chamados complementadores – a partir do qual os consumidores percebem valor. Para tanto, os operadores de serviços digitais assumem o papel de "orquestradores" do ecossistema, definindo e implementando, tanto por meio de contratos quanto de soluções técnicas, uma visão de valor que é transmitida a esses terceiros e que influencia tanto os comportamentos dentro da plataforma quanto a criação de inovações futuras[306].

Nesse cenário, os fatores que moldam a dinâmica competitiva dos ecossistemas digitais não são mais os listados por Porter na década de 1970 (ameaça de substitutos, ameaça de novos entrantes, rivalidade no setor e poder de barganha de clientes e fornecedores)[307], mas aqueles que afetam

303 ZINGALES, Nicolo; AZEVEDO, Paula Farani de. **A aplicação do direito antitruste em ecossistemas digitais: desafios e propostas**, Rio de Janeiro: FGV Direito Rio, 2022.

304 TEECE, David J. Next-generation competition: New concepts for understanding how innovation shapes competition and policy in the digital economy. **JL Econ. & Pol'y**, v. 9, p. 97, 2012.

305 JACOBIDES, Michael G.; LIANOS, Ioannis. Ecosystems and competition law in theory and practice. **Industrial and Corporate Change**, v. 30, n. 5, p. 1199-1229, 2021.

306 ZINGALES, Nicolo; FARANI DE AZEVEDO, Paula. Direito antitruste e ecossistemas digitais: mapeando o debate. In: ZINGALES, Nicolo; FARANI DE AZEVEDO, Paula (Orgs.). Rio de Janeiro: FGV Editora, 2022, p. 13-46.

307 PORTER, Michael E., How Competitive Forces Shape Strategy. **Harvard Business Review**, v. 57, 1979.

diretamente o poder e a atratividade do ecossistema no mercado. Essa nova lógica se organiza em quatro dimensões principais: a gestão dos efeitos de rede, a conexão entre diferentes redes e a contenção da desintermediação e do *multi-homing*[308].

O primeiro aspecto refere-se ao aumento do valor de um produto na medida em que cresce o número de usuários. Para estimular esse processo, as plataformas frequentemente oferecem produtos a preços reduzidos — ou até mesmo subsidiados ao ponto de serem gratuitos. A corrida por uma base maior de consumidores explica por que tantas empresas mantêm serviços gratuitos, mesmo sem retorno imediato, priorizando a coleta de dados e a possibilidade de desenvolver competências de previsão que trarão vantagens no longo prazo[309].

O segundo elemento relaciona-se ao fortalecimento dos efeitos de rede pela integração de serviços distintos. Como exemplo, tem-se a hipótese em que um mesmo operador de marketplace também disponibiliza serviços de pagamento. Nesses casos, o consumidor se beneficia de maior conveniência ou de ganhos econômicos graças ao "efeito *spillover*" gerado pela interação entre as duas redes, fenômeno denominado *network bridging*.

Já o terceiro e o quarto aspectos correspondem a riscos que podem reduzir o poder das plataformas e, por isso, são monitorados de perto pelos orquestradores. O primeiro deles é o chamado "efeito carona", que ocorre quando a rede da plataforma é utilizada para captar usuários, mas a transação é concluída fora do ambiente da própria plataforma. Para evitar isso, os operadores impõem barreiras técnicas e contratuais.

O outro risco é a migração dos usuários para serviços concorrentes, ou ainda a utilização simultânea de diferentes ecossistemas (*multi-homing*). Nesse caso, os orquestradores procuram dificultar a interoperabilidade e a portabilidade de conteúdos e serviços, aumentando os custos de mudança e erguendo verdadeiras "trincheiras" de proteção (familiarmente denominadas *moats*) em torno de seu mercado principal. Tais barreiras podem assumir a forma de estratégias conglomeradas (explorando sinergias entre

308 ZHU, Feng; IANSITI, Marco. Why Some Platforms Thrive and Others Don't. **Harvard Business Review**, v. 97, p. 118, 2019.

309 LIANOS, Ioannis. **Competition Law for the Digital Era: A Complex Systems' Perspective**. Rochester, NY: Centre for Law, Economics and Society - UCL, 2019, p. 103-104.

linhas de negócio), de *self-preferencing* ou de alavancagem, estruturando o ecossistema como um conglomerado. Nessas condições, os usuários tendem a permanecer vinculados (efeito *lock-in*), já que migrar para outro ecossistema significaria perder benefícios acumulados.

Por fim, cabe ressaltar que riscos elevados podem ser determinados pela exposição a interrupções em cadeias de suprimentos devido a fatores geopolíticos que podem ser voltados ou não a impactar diretamente o Brasil.

3.6 A necessidade de regulação de plataformas digitais e sistemas de IA por elas utilizados

Como visto anteriormente, a lógica econômica das grandes plataformas digitais é, por natureza, orientada à maximização de lucro e à redução de custos. Nomeadamente, para empresas de capital aberto, essa orientação não é apenas um objetivo, mas uma obrigação fiduciária perante seus acionistas.

A ausência de uma legislação específica sobre regulação de plataformas reforçou esse quadro, ao permitir que tais empresas assumissem, na prática, a função de estruturar e disciplinar o espaço digital por meio de seus termos de uso, políticas internas e arquiteturas tecnológicas.[310] Nesse arranjo, as plataformas consolidaram um poder estrutural, capaz de moldar o comportamento dos usuários e organizar fluxos informacionais sem mecanismos claros de responsabilização ou salvaguarda dos direitos fundamentais.[311]

Assim, tais plataformas deixam de ter incentivos econômicos reais para priorizar a saúde psíquica dos usuários, limitar a circulação de conteúdo de ódio ou reduzir práticas nocivas à convivência social.[312] Seu foco permanece, portanto, na maximização da retenção da atenção e, em úl-

310 LESSIG, **Code: And Other Laws of Cyberspace**..

311 BELLI, Luca et al. Structural Power as a Critical Element of Digital Platforms Private Sovereignty. In: BELLI; MAGALHÃES, **AI Sovereignty and AI Governance: Perspectives from the BRICS and Beyond**.

312 VAIDHYANATHAN, Siva. **Antisocial Media: How Facebook Disconnects Us and Undermines Democracy.** New York: Oxford University Press, 2018. POPIEL; VASUDEVAN. Platform frictions, platform power, and the politics of platformization. PINHEIRO; COSTA. AS FAKE NEWS SOBRE O PL DAS FAKE NEWS.

tima análise, do engajamento, que é elemento central de seus modelos de negócios baseados em publicidade e monetização de dados.[313]

Pesquisas recentes demonstram, de forma consistente, que as externalidades negativas desse modelo são profundas e já constituem um problema social de larga escala. Dentre as consequências mais graves, destacam-se: desinformação, o assédio sistemático e o discurso de ódio dirigidos especialmente a grupos vulneráveis[314], fenômenos amplificados por sistemas de recomendação que promovem conteúdo polarizador[315], além de danos significativos à saúde mental dos usuários, sobretudo crianças, adolescentes e pessoas em situação de vulnerabilidade.[316]

Em período eleitoral, esses problemas se tornam mais graves pela possibilidade de afetar o jogo democrático. Exatamente por esse motivo é que o Tribunal Superior Eleitoral (TSE) tem desempenhado um papel protagonista durante pleitos eleitorais recentes, principalmente com a popularização da inteligência artificial. O Código Eleitoral (artigo 23, inciso IX) e a Lei das Eleições (Lei 9.504/1997, artigos 57-J e 105) conferem competência a esse tribunal para disciplinar a matéria.

Na perspectiva de se preservar a higidez dos processos democráticos, algumas resoluções já foram editadas, como a Resolução n.º 23.610/2019,

313 COUTO, Natalia de Macedo, O papel regulatório do Estado na moderação de conteúdo exercida pelas plataformas de redes sociais, 2022.

314 LENHART, Amanda et al. Online Harassment, Digital Abuse, and Cyberstalking in America. **Data & Society Research Institute**, 2016. FARIS, Robert et al. Understanding Harmful Speech Online | Berkman Klein Center, **Berkman Klein Center for Internet & Society Publication**, 2016. NADIM, Marjan; FLADMOE, Audun, Silencing Women? Gender and Online Harassment. **Social Science Computer Review**, v. 39, n. 2, p. 245-258, 2021.

315 COBBE, Jennifer; SINGH, Jatinder. Regulating Recommending: Motivations, Considerations, and Principles. **European Journal of Law and Technology**, v. 10, n. 3, 2019. MOZILLA, **Mozilla Investigation: YouTube Algorithm Recommends Videos that Violate the Platform's Very Own Policies**. Mozilla Foundation. Disponível em: <https://www.mozillafoundation.org/en/blog/mozilla-investigation-youtube-algorithm-recommends-videos-that-violate-the-platforms-very-own-policies/>. Acesso em: 4 dez. 2025. GILLESPIE, Tarleton, Do Not Recommend? Reduction as a Form of Content Moderation. **Social Media + Society**, v. 8, n. 3, p. 20563051221117552, 2022.

316 RIBEIRO, Márcio Moretto; ORTELLADO, Pablo, O que são e como lidar com as notícias falsas. **Sur - Revista Internacional de Direitos Humanos**, v. 15, n. 27, p. 71-83, 2018. BIDARE, Pranav Majesh; DREYER, Stephan; KELLER, Clara Iglesias. **Between evidence and policy: bridging the gap in disinformation regulation**. Internet Policy Review. Disponível em: <https://policyreview.info/articles/news/between-evidence-and-policy-bridging-gap-disinformation-regulation/1667>. Acesso em: 4 dez. 2025.

a Resolução n.º 23.714/2022 e Resolução n.º 23.732/2024, com o objetivo de disciplinar a propaganda eleitoral na esfera digital e estabelecer mecanismos mínimos de enfrentamento à desinformação durante o processo eleitoral. Em que pese sua importância, contudo, tais normativas possuem alcance temporal estritamente limitado ao período eleitoral (que se inicia a partir de 15 de agosto do ano eleitoral), não configurando um regime contínuo de regulação no ambiente digital.

Esses impactos, hoje amplamente documentados, evidenciam que deixar a moderação de conteúdo e o desenho dos sistemas algorítmicos sob controle exclusivo das plataformas e de seus termos de uso coloca a coletividade em risco. Por isso, multiplicaram-se iniciativas que exigem maior transparência das plataformas digitais.[317]

Nesse sentido, o Projeto de Lei n.º 2630/2020, atualmente com tramitação suspensa, representou uma tentativa para instituir deveres de cuidado para as plataformas e práticas de transparência. Em que pese sua tramitação tenha sido marcada por inúmeras controvérsias, esse projeto alinhava-se, de forma geral, a boas práticas internacionais e a regulação europeia do *Digital Service Act*.[318]

A falta de transparência constitui um problema grave que precisa ser enfrentado. As plataformas digitais não informam de maneira clara e expressa os direitos e restrições aplicáveis aos usuários, e tampouco tornam públicos, de forma suficiente, os procedimentos relativos aos sistemas de recomendação de conteúdo que orientam a filtragem, priorização e organização do ambiente informacional online.

Pesquisa realizada por Zingales *et al.*[319] analisou o grau de comprometimento das principais plataformas utilizadas no Brasil em relação às normas de transparência estabelecidas pela legislação brasileira. Consi-

317 GORWA, Robert; ASH, Timothy Garton. Democratic Transparency in the Platform Society. In: TUCKER, Joshua A.; PERSILY, Nathaniel (Orgs.). **Social Media and Democracy**, Cambridge: Cambridge University Press, 2020, p. 286–312. RESNICK, Mitchel; BERG, Robbie; EISENBERG, Michael, Beyond Black Boxes: Bringing Transparency and Aesthetics Back to Scientific Investigation. **Journal of the Learning Sciences**, v. 9, n. 1, p. 7–30, 2000.

318 COUTO, Natália, Regulação de redes sociais no Brasil: grupos de interesse e o caso do PL 2630/2020. In: **Os caminhos da internacionalização e o futuro do Direito**. São Paulo: Conpedi (prelo), 2025.

319 ZINGALES, Nicolo et al. Análise de obrigações de transparência das plataformas de rede social: evidências empíricas no Brasil. **Revista de Direito Econômico e Socioambiental**, v. 17, n. 1, 2026.

derando que transparência envolve duas dimensões – visibilidade e compreensibilidade –, os autores verificaram ambas nas políticas e nos termos de uso disponibilizados aos usuários. Os resultados empíricos confirmam o diagnóstico amplamente discutido na literatura: há falhas significativas na transparência promovida por essas empresas, especialmente no que diz respeito à compreensibilidade, isto é, aos critérios de clareza, precisão e uso adequado da língua portuguesa.

Além disso, a emergência de sistemas de inteligência artificial voltados à interação pessoal, como *chatbots* "companheiros" ou *AI companions*, agentes conversacionais que simulam empatia ou proximidade emocional, expõe a sociedade a riscos graves de manipulação comportamental e de danos psicossociais.[320] Esses sistemas podem fomentar dependência emocional, reforçar distorções cognitivas, agravar vulnerabilidades psicológicas e até incentivar comportamentos autopunitivos ou autodestrutivos. Particularmente, diversas pesquisas comprovam que interações intensivas com *chatbots* podem levar a "feedback loops" nocivos, nos quais indivíduos com fragilidades mentais são levados a manter crenças delirantes ou tendências suicidas frente a respostas manipulativas ou excessivamente condescendentes da IA.[321] A própria capacidade dessas ferramentas de simular intimidade, criando laços emocionais artificiais, torna vulneráveis especialmente crianças, adolescentes, pessoas isoladas ou com histórico de sofrimento psíquico.[322]

Além dos riscos à saúde mental e bem-estar individual, sistemas de IA interativos têm demonstrado capacidade de influenciar convicções políticas, comportamento eleitoral e opinião pública de forma mais eficaz que propagandas tradicionais, explorando vulnerabilidades cognitivas

320 **Friends for sale: the rise and risks of AI companions**. Disponível em: <https://www.adalovelaceinstitute.org/blog/ai-companions/>. Acesso em: 6 dez. 2025.

321 DOHNÁNY, Sebastian et al. Technological folie à deux: Feedback Loops Between AI Chatbots and Mental Illness, 2025.
Emotional risks of AI companions demand attention. **Nature Machine Intelligence**, v. 7, n. 7, p. 981-982, 2025.

322 **Why AI companions and young people can make for a dangerous mix**. News Center. Disponível em: <https://med.stanford.edu/news/insights/2025/08/ai-chatbots-kids-teens-artificial-intelligence.html>. Acesso em: 6 dez. 2025. DOHNÁNY et al. ***Technological folie à deux: Feedback loops between AI chatbots and mental illness.***

e afetivas.[323] A título de exemplo, um levantamento recente revelou que *chatbots* projetados para persuasão podem moldar posicionamentos eleitorais com maior eficiência do que anúncios políticos, ao entregar conteúdo "sob medida" a usuários vulneráveis ou indecisos.[324] Esse potencial de manipulação eleitoral e social impõe urgência ao desenvolvimento de regulamentações específicas para sistemas de IA de interação pessoal, que estão sendo incluído em vários tipos de plataformas, como redes sociais do grupo Meta[325], a fim de que sejam estabelecidos critérios de transparência, auditabilidade, responsabilidade, restrições para uso com menores ou pessoas vulneráveis, e mecanismos de supervisão pública.

Diante desses riscos, a regulação de plataformas e sistemas de IA voltados a interações pessoais não se configura como obstáculo à inovação, mas como condição necessária para proteger direitos fundamentais, preservar a integridade psicológica e a saúde mental de cidadãos, além de salvaguardar processos democráticos.

A recente adoção do chamado ECA Digital (Lei n.º 15.211/2025) representa um avanço importante na direção da definição de obrigações mais contundentes para as plataformas, especialmente no que diz respeito à proteção de crianças e adolescentes em ambientes digitais. Ao atualizar os princípios do Estatuto da Criança e do Adolescente para o contexto tecnológico contemporâneo, a nova normativa sinaliza um compromisso institucional com a redução de riscos, a contenção de práticas abusivas e a promoção de ambientes digitais mais seguros para essas pessoas humanas em desenvolvimento. No entanto, para que esse marco regulatório produza efeitos concretos, é fundamental que sua implementação seja efetiva, contínua e venha acompanhada de mecanismos robustos de fiscalização, que, agora ficará a cargo da Agência Nacional de Proteção de Dados (ANPD).

---

323 LIN, Hause *et al*, Persuading voters using human–artificial intelligence dialogues. **Nature**, p. 1–8, 2025.

324 HACKENBURG, Kobi et al. The levers of political persuasion with conversational artificial intelligence. **Science**, v. 390, n. 6777, 2025.

325 Lonely? Meta CEO Mark Zuckerberg's got you covered with AI friends, **The Economic Times**, 2025; HOOVER, Amanda, **Mark Zuckerberg destroyed friendship. Now he wants to replace it with AI.**, Business Insider. Disponível em: <https://www.businessinsider.com/mark-zuckerberg-destroyed-friendship-replace-ai-companions-loneliness-2025-5>. Acesso em: 6 dez. 2025.

Apesar dos inegáveis avanços trazidos pelo ECA Digital, é fundamental reconhecer, ainda, que a regulação das plataformas não pode ser limitada apenas aos impactos sobre crianças e adolescentes, na medida em que os danos causados por sistemas algorítmicos e pela dinâmica econômica das plataformas são amplos, estruturais e afetam toda a sociedade, em diversos graus. Afinal, adultos também enfrentam desinformação, manipulação emocional, vigilância comercial excessiva, práticas abusivas de coleta de dados, polarização política artificialmente amplificada e discriminação algorítmica, entre outros problemas.[326]

Portanto, focar exclusivamente no público infantojuvenil — embora essencial — não é suficiente para enfrentar a totalidade dos riscos gerados por modelos de negócios baseados em maximização de engajamento e coleta massiva de dados. Uma regulação eficaz precisa ser abrangente, cobrindo todas as faixas etárias, todos os tipos de uso e todas as externalidades negativas associadas às plataformas digitais. Somente assim será possível garantir um ecossistema digital saudável, transparente e seguro para todos os cidadãos.

Em vista dessa inércia legislativa parcial, que pode ser explicada, em grande medida, pelos riscos de manipulação cognitiva ressaltados anteriormente, em 2025, o Supremo Tribunal Federal brasileiro, em paradigmática e histórica decisão, ao analisar os Recursos Extraordinários (RE) de números 1037396 (Tema 987) e 1057258 (Tema 533), que versavam sobre a constitucionalidade do artigo 19 do Marco Civil da Internet, acabou recrudescendo o regime jurídico de responsabilidade civil aplicável às plataformas digitais, além de impor obrigações específicas que envolvem, em algum grau, até mesmo o dever de cuidado diante de situações consideradas mais graves e criminosas.

Diante desse cenário, regular o ecossistema digital de modo amplo torna-se não apenas uma medida de proteção de direitos fundamentais,

326 LAZER, David M. J. *et al*, The science of fake news, **Science**, v. 359, n. 6380, p. 1094–1096, 2018. JUDGE, E.F.; KORHANI, A.M. Disinformation, Digital Information Equality, and Electoral Integrity. **Election Law Journal: Rules, Politics, and Policy**, v. 19, n. 2, p. 240-261, 2020. CARAMANCION, Kevin Matthe et al. The Missing Case of Disinformation from the Cybersecurity Risk Continuum: a Comparative Assessment of Disinformation with Other Cyber Threats, **Data**, v. 7, n. 4, 2022. BARTOLOMÉ, Mariano. Redes sociales, desinformación, cibersoberanía y vigilancia digital: una visión desde la ciberseguridad. **Revista de Estudios en Seguridad Internacional**, v. 7, nº. 2, n. Revista de Estudios en Seguridad Internacional, p. 167-185, 2021.

mas também uma afirmação da soberania nacional e do compromisso com o Estado de Direito. Para ser eficaz, essa regulação deve abordar, de modo integrado, quatro prioridades estruturantes:

1. Regras claras sobre conteúdo, assegurando que práticas abusivas, ilegais ou que violem direitos fundamentais possam ser prevenidas, moderadas e responsabilizadas de maneira transparente e proporcional, com base na recente decisão do Supremo Tribunal Federal sobre a constitucionalidade do artigo 19 do Marco Civil da Internet.
2. Transparência, fiscalização e explicabilidade dos sistemas de IA usados pelas plataformas, especialmente no que diz respeito aos mecanismos de recomendação algorítmica, priorização de conteúdo e personalização, garantindo que decisões automatizadas possam ser compreendidas e auditadas por autoridades competentes.
3. Políticas de tributação e incentivos econômicos que revertam o modelo atual de coleta massiva de dados, promovendo o cumprimento do princípio da minimização de dados previsto em lei e desincentivando práticas que dependem da extração indiscriminada de informações pessoais para maximizar engajamento e lucro.
4. Fomento ao desenvolvimento de plataformas alternativas e obrigação de interoperabilidade, de modo a reduzir a dependência estrutural das plataformas dominantes, ampliar a diversidade do ecossistema digital, incentivar inovação e garantir que usuários, criadores e empresas não fiquem presos a ecossistemas fechados, sem possibilidade real de migração, competição ou escolha.

À luz disso, é possível afirmar que uma regulação abrangente, que não seja limitada somente aos possíveis impactos negativos para crianças e adolescentes, seja essencial para equilibrar inovação com proteção social, assegurando que as plataformas digitais operem de forma compatível com os valores democráticos, com a segurança dos cidadãos e com o respeito aos direitos fundamentais. Tal regulamentação precisa ser desenvolvida no âmbito de uma abordagem sistêmica, entendendo não somente os impactos que as plataformas podem representar para seus usuários, mas também como as plataformas digitais se inserem no âmbito de cadeias produtivas digitais que adquirem uma dimensão global, como será explicado na próxima seção.

3.7 Capilaridade das cadeias produtivas e vulnerabilidades geopolíticas

Não obstante as estratégias e práticas de captação de usuários descritas anteriormente, observa-se que, à medida que países emergentes iniciam ou aceleram a digitalização de serviços essenciais e infraestruturas críticas, muitos acabam se tornando dependentes de fornecedores e provedores estrangeiros, em razão da industrialização (e digitalização) tardia em relação às grandes potências econômicas. Embora tardiamente, este recente processo de industrialização incorpora práticas, processos e serviços desenvolvidos internacionalmente em diferentes instâncias da sua cadeia produtiva e de suprimentos.

Nesse cenário, tecnologias digitais assumem uma capilaridade profunda na capacidade produtiva nacional, abarcando desde os setores industriais mais desenvolvidos, como montadoras automobilísticas, exploradoras de petróleo, mineradoras, entre outras; mas também parcelas da população que trabalham como prestadores de serviço e/ou no terceiro setor, que recorrem a redes sociais para captar clientes ou a plataformas de comércio digital para comercializar seus produtos.[327] Como resultado, a dependência de países emergentes para com infraestruturas e serviços privados não se limita aos usuários, mas abarca toda a esfera produtiva e econômica dos países emergentes.

Sendo assim, a falta de tecnologias autóctones coloca países emergentes à mercê dos interesses e pressões de empresas estrangeiras e, em última instância, das nações e governos destas empresas. Essa realidade, na qual a cadeia produtiva de um país não está necessariamente limitada a componentes, serviços e mão de obra nacionais, é emblemática da globalização. Contudo, em decorrência da falta de soberania digital, a realidade desses países e de seus setores produtivos é uma na qual acordos comerciais e de desenvolvimento tecnológico são instrumentalizados para afirmar dominância de em-

327 SANTOS, Naedja Karla Petrucio dos et al. Revolução digital e mercado de trabalho: da uberização às plataformas digitais. **Caderno Pedagógico**. v. 21, n. 10, p. e9933–e9933, 2024. ROBERTO, José; GERALDO, Murilo Afonso; BIASOTO JR, Viana. Economia digital, micronegócios, máxima produtividade. **Revista Conjuntura Econômica**, v. 74, n. 2, p. 22-25, 2020.

presas (e seus governos) sobre países em processo de digitalização, mediante práticas de colonialismo digital e exploração de mercados emergentes.[328]

Holística em sua compreensão, a dependência nacional para com tecnologias e plataformas digitais afeta diferentes parcelas produtivas da sociedade. Contudo, decisões unilaterais, e eventuais tensionamentos entre empresas e governos locais vêm gerando consequências latentes e diretas para terceirizados e prestadores de serviços que dependem de aplicativos e plataformas digitais para sua subsistência.[329] Motoristas de aplicativo, por exemplo, são alvos de tensionamentos regulatórios por parte do governo brasileiro e decisões empresariais estrangeiras, por vezes tendo como consequência a paralisação dos serviços e afetando diretamente os motoristas e usuários destes tipos de transporte.[330]

Somam-se a esses, embates acerca do acesso a informações criptografadas de aplicativos de mensageria por parte de forças policiais e investigativas, recebida com resistência por big-techs[331]. Nesses embates de adaptação regulatória por parte das empresas, serviços como WhatsApp e Telegram[332] já foram suspensos mais de uma vez.[333] Essa suspensão afeta,

---

328 COULDRY, Nick; MEJIAS, Ulises A. The Costs of Connection: How Data Are Colonizing Human Life and Appropriating It for Capitalism. **ResearchGate**, 2024. PINTO, Renata Ávila. **Digital Sovereignty or Digital Colonialism? New tensions of privacy, security and national policies. | EBSCOhost**. Disponível em: <https://openurl.ebsco.com/contentitem/gcd:133035238?sid=ebsco:plink:crawler&id=ebsco:gcd:133035238>. Acesso em: 11 mar. 2025. JIANG; BELLI, Luca. *Digital Sovereignty in the BRICS Countries*. In: BELLI, Luca; MAGALHÃES, Larissa (orgs.). *AI Sovereignty and AI Governance: Perspectives from the BRICS and Beyond*. [S.l.: s.n.], 2026. No prelo.

329 SANTOS et al. **Revolução digital e mercado de trabalho**. ROBERTO; GERALDO; BIASOTO JR, **Economia digital, micronegócios, máxima produtividade**.

330 MOURÃO, Giovanni, O Globo, **Justiça suspende regulamentação de Uber e 99 em Niterói**, 2018.

331 SHIONA MCCALLUM, BBC. **WhatsApp diz que nenhum governo o fará enfraquecer sua criptografia**. G1. Disponível em: <https://g1.globo.com/tecnologia/noticia/2022/07/30/whatsapp-diz-que-nenhum-governo-o-fara-enfraquecer-sua-criptografia.ghtml>. Acesso em: 29 out. 2025.

332 VALOR ECONÔMICO. Por que o Telegram foi suspenso no Brasil? Entenda. **Valor Econômico**. Disponível em: <https://valor.globo.com/empresas/noticia/2023/04/26/por-que-o-telegram-foi-suspenso-no-brasil-entenda.ghtml>. Acesso em: 29 out. 2025. BARROS, Mateus. Justiça dá 30 dias para Telegram e Signal se adequarem às leis brasileiras. G1 REDAÇÃO. **WhatsApp já foi bloqueado por decisão judicial em 2015 e 2016 no Brasil**, G1. Disponível em: <https://g1.globo.com/tecnologia/noticia/2022/03/18/whatsapp-ja-foi-bloqueado-por-decisao-judicial-em-2015-e-2016-no-brasil.ghtml>. Acesso em: 29 out. 2025.

333 LILIAN CUNHA, **Apagão de WhatsApp e cia. traz prejuízo a empresas, que podem processar serviços**, CNN Brasil. Disponível em: <https://www.cnnbrasil.com.br/tecnologia/apagao-de-

além de usuários, funcionários, prestadores de serviços, profissionais autônomos e pequenos negócios que estruturam seu modelo de negócios via contato direto com fornecedores e clientes nestas plataformas de mensageria. Assim, a aplicação estadual ou mesmo nacional de sanções jurídicas sobre estas empresas acaba afetando diretamente uma crescente parcela da população e do setor produtivo do país.

Não bastasse as eventuais tensões decorrentes da adaptabilidade regulatória de empresas de tecnologias, o cenário de dependência possibilita que eventuais tensões geopolíticas comprometam o acesso a serviços ou a componentes de hardwares essenciais para a cadeia produtiva e esforço industrial de diferentes países. A título de exemplo, enquanto países na Europa e América Latina vinham atualizando sua infraestrutura de telefonia móvel para redes de 5G, uma possível liderança de empresas chinesas – em especial a Huawei –, nesse processo, foi recebida com grande resistência por gigantes de telecomunicações ocidentais.[334] A expansão destas empresas para o Brasil e outros aliados norte-americanos foi percebida como uma eventual vulnerabilidade estratégica pelos EUA, ao passo que empresas – e eventualmente o governo chinês, por intermédio da Lei de Inteligência Nacional – passariam a ter acesso à estrutura fundacional das conexões nacionais.

Nesse contexto, na percepção norte-americana, empresas chinesas passariam a ter uma capilaridade profunda nas infraestruturas digitais e, portanto, em toda a cadeia produtiva dos países que recebessem a infraestrutura de 5G chinesa. Esse nível, segundo autoridades norte-americanas, colocaria em risco alianças militares e implicaria na restrição no compartilhamento de inteligência entre aliados.[335]

A ocorrência colocou o pragmatismo da diplomacia econômica brasileira à prova, enquanto sinalizava o interesse de adoção das tecnologias

whatsapp-e-cia-traz-prejuizo-a-empresas-que-podem-processar-servicos/>. Acesso em: 29 out. 2025.

334 BARIFOUSE, Rafael, **Por que 5G da Huawei põe Brasil em saia-justa com China e EUA**, BBC News Brasil. Disponível em: <https://www.bbc.com/portuguese/brasil-50468237>. Acesso em: 12 nov. 2025.

335 WINTOUR, Patrick, **US defence secretary warns Huawei 5G will put alliances at risk**, The Guardian. Disponível em: <https://www.theguardian.com/us-news/2020/feb/15/us-defence-secretary-warns-us-alliances-at-risk-from-huawei-5g>. Acesso em: 27 ago. 2025.

de 5G da China, simultaneamente advogando por padrões de segurança americanos.[336] Contudo, demandas regulatórias por parte da Agência Nacional de Telecomunicações (ANATEL) levaram à adoção de um modelo que integrasse redes de 5G *standalone* (sem a obrigação de conexão com redes de 4G preexistentes) e 5G *non-standalone* (alicerçada em conexões e tecnologias de 4G). O resultado foi uma maximização da cobertura em território nacional.[337]

Na sequência, embora o debate inicial sobre segurança, fornecedores e modelo de implementação ainda estivesse latente no início das discussões sobre a implementação, esta preocupação acabou assumindo um papel secundário ao passo que o ritmo de implantação e a escala da infraestrutura avançaram para a fase de implementação ativa mediante leilão de espectro, arranque comercial das redes, escalando cobertura.[338] Como resultado, atualmente, a cadeia produtiva do país depende de uma expansiva e já robusta cobertura de 5G no território nacional. Esta malha de 5G, por sua vez, embora de origem estrangeira, se encontra sob regulação da ANATEL e evidencia como esforços de diplomacia, guiados por princípios soberanos, foram instrumentais na absorção de tecnologias estrangeiras e alavancagem do setor produtivo nacional.

Outro ponto de tensionamento geopolítico se deve à permeabilidade de microchips em cadeias produtivas de alto valor. A centralidade desses

---

336 JIA, Liu *et al*, STRATEGIC MANEUVERING IN BRAZIL'S 5G DEPLOYMENT AMIDST UNITED STATES-CHINA TECHNOLOGICAL RIVALRY, **Revista Tempo do Mundo**, n. 34, p. 419–451, 2024; MEDEIROS, Breno Pauli; GOLDONI, Luiz Rogério Franco; SILVA, Carla Morena Vitoria Gomes, Brazil, *in*: CHRISTOU, George *et al* (Orgs.), **The Palgrave Handbook on Cyber Diplomacy**, Cham: Springer Nature Switzerland, 2025, p. 673–688; BARIFOUSE, **Por que 5G da Huawei põe Brasil em saia-justa com China e EUA**; JÚLIO WIZIACK, **Para liberar Huawei, Bolsonaro obriga teles a construírem uma rede de telefonia só para o governo**, Folha de S. Paulo. Disponível em: <https://www1.folha.uol.com.br/mercado/2021/01/para-liberar-huawei-bolsonaro-obriga-teles-a-construirem-uma-rede-de-telefonia-so-para-o-governo.shtml>. Acesso em: 29 out. 2025.

337 WESTHUIZEN, Janis van der, Huawei or the US way? Why Brazil and South Africa did not securitize 5G, **Revista Brasileira de Política Internacional**, v. 67, p. e016, 2024; JIA *et al*, STRATEGIC MANEUVERING IN BRAZIL'S 5G DEPLOYMENT AMIDST UNITED STATES-CHINA TECHNOLOGICAL RIVALRY.

338 Huawei: Por que os EUA consideram a gigante chinesa de tecnologia uma ameaça à segurança nacional; JIA *et al*, STRATEGIC MANEUVERING IN BRAZIL'S 5G DEPLOYMENT AMIDST UNITED STATES-CHINA TECHNOLOGICAL RIVALRY; PRESTES, Elisa Gomes, The digital geopolitics of 5G: elements to understand the Chinese technological development of the fifth generation of mobile telephony, **GEOUSP**, v. 26, p. e194823, 2022.

microchips em cadeias produtivas relacionadas a computação, telecomunicações, Inteligência Artificial e computação quântica está no cerne de debates geopolíticos entre EUA e China na atualidade. Nesse contexto, medidas como leis de incentivo à produção industrial, como o CHIPS Act de 2022, ou a aplicação de controle de exportações se tornaram recorrentes.[339] Ao passo que disputas tarifárias se tornaram mais frequentes e voláteis, como o tarifaço de Donald Trump, por exemplo, para economias emergentes como o Brasil, que buscam integrar microchips em suas cadeias de valor, este controle de exportações tem consequências diretas e indiretas, que abarcam desde o acesso aos chips em si, até pressões na cadeia de suprimentos globais e reestruturação de fornecedores.[340]

Em uma ocorrência mais recente, a adesão de chips para o desenvolvimento de IA vendidos pela Huawei se tornou tema central de um alerta do governo norte-americano.[341] Segundo a administração Trump, a compra e uso de chips da Huawei estaria em violação dos controles de exportação estadunidenses devido ao fato de que estes chips teriam sido desenvolvidos mediante acesso indevido a tecnologias norte-americanas.[342] Não obstante as críticas, a Huawei recentemente abriu o código de seus modelos de IA

339 HYATT, Katherine; RYLE, Patrick M.; MCKNIGHT, Mark A., Semiconductor production, geopolitics and the CHIPS ACT of 2022: a theoretical analysis, **Digital Policy, Regulation and Governance**, v. 27, n. 1, p. 1–16, 2024; BINGJIE LI, Export Effect of Trade Facilitation in Asian "Belt and Road" Coastal Countries on China's Cross-border E-commerce, **Journal of Coastal Research**, v. 104, p. 628–632, 2020; HRYNKIV, Olga; LAVRIJSSEN, Saskia, Not Trading With the Enemy: The Case of Computer Chips, **Journal of World Trade**, v. 58, n. 1, 2024.

340 LEE, Keun; MALERBA, Franco; PRIMI, Annalisa, The fourth industrial revolution, changing global value chains and industrial upgrading in emerging economies, **Journal of Economic Policy Reform**, v. 23, n. 4, p. 359–370, 2020; JIA *et al*, STRATEGIC MANEUVERING IN BRAZIL'S 5G DEPLOYMENT AMIDST UNITED STATES-CHINA TECHNOLOGICAL RIVALRY; BORTOLASO, Ingridi Vargas *et al*, Trajectory of the Brazilian Semiconductor Industry and Supply Chain: Economic, Governmental, and Technological Perspectives, **Journal of Operations and Supply Chain Management**, v. 6, n. 2, p. 20–39, 2013; CASAGRANDE, Dieison; MALLMANN, Conrado; FEISTEL, Paulo Ricardo, US-China Trade War: The Effects of Trade Conflict on Brazilian Exports, **SSRN Electronic Journal**, 2023.

341 PHAM, Sherisse, **US move against Huawei could slow the global rollout of 5G**, CNN Business. Disponível em: <https://www.cnn.com/2019/05/16/tech/huawei-us-5g-rollout>. Acesso em: 12 nov. 2025.

342 MCMORROW, Ryan *et al*, **US warns against using Huawei chips 'anywhere in the world'**, Financial Times. Disponível em: <https://www.ft.com/content/2033b5b3-974d-4d40-8498-1c46d3a8db79>.

em uma iniciativa para impulsionar a adesão de seus produtos no mercado internacional.[343] Em outra instância, a empresa Nvidia também vem enfrentando restrições de exportação do governo norte-americano para comercializar seus chips H20, direcionados ao desenvolvimento e treinamento de modelos de IA, na China.[344]

Os eventuais controles de exportação sobre chips ou outras tecnologias digitais evidencia como tensões geopolíticas podem ter consequências práticas, comerciais e estratégicas, ao passo que microchips são a base de processamento de tecnologias como *cloud computing*, automação, data centers e de tecnologias emergentes como IA e computação quântica. Assim, a imposição de controles de exportação sobre estes produtos corre o risco de travar cadeias produtivas mundo afora. Naturalmente, os atores nacionais que possuem acesso regulatório sobre as empresas líderes destas tecnologias exercem seu poder para moldar a corrida de inovação conforme seus interesses.[345]

Para além da dependência tecnológica que marca a estrutura produtiva nacional, a inexistência de mecanismos institucionais aptos a compreender as diversas dimensões da soberania digital e a atuar proativamente em seu fortalecimento — identificando e mitigando riscos — torna países como o Brasil suscetíveis não apenas a vulnerabilidades tecnológicas, mas também a riscos geopolíticos e econômicos expressivos advindos de decisões unilaterais de potências estrangeiras.

Nesse contexto, destaca-se o recente memorando presidencial dos Estados Unidos intitulado *Defending American Companies and Innovators*

---

343 COELHO, Cido, **Huawei abre código de modelos de IA enquanto busca adoção no mercado global**, Times Brasil - Licenciado Exclusivo CNBC. Disponível em: <https://timesbrasil.com.br/empresas-e-negocios/tecnologia-e-inovacao/huawei-abre-codigo-de-modelos-de-ia-enquanto-busca-adocao-no-mercado-global/>. Acesso em: 12 nov. 2025.

344 SHAPERO, Julia. **Nvidia navigates US-China "tightrope" in AI chip sales**. The Hill. Disponível em: <https://thehill.com/policy/technology/5441397-nvidia-us-china-ai-chips/>. Acesso em: 27 ago. 2025.

345 DEVANNY, Joe. Artificial Intelligence and Cyber Power. **Research Publications**, 2024. SÁNCHEZ, C.H., Export control on cybertechnologies: An analysis of the Wassenaar Agreement and its implications for cybersecurity. **Revista Chilena de Derecho y Tecnologia**, v. 7, n. 1, p. 61-78, 2018. SCHMID, Stefka *et al*, Arms Race or Innovation Race? Geopolitical AI Development, **Geopolitics**, v. 0, n. 0, p. 1–30, 2025; FRANKE, Ulrike, Artificial Intelligence diplomacy | Artificial Intelligence governance as a new external policy tool, 2021.

from Overseas Extortion and Unfair Fines and Penalties.[346] O documento estabelece diretrizes para a imposição de tarifas e outras medidas retaliatórias contra países que adotem políticas consideradas discriminatórias, desproporcionais ou direcionadas à transferência de receitas e propriedade intelectual de empresas norte-americanas para governos ou companhias domésticas estrangeiras.

Entre as medidas previstas, o memorando autoriza o Representante de Comércio dos Estados Unidos (USTR no acrônimo em língua inglesa) a renovar ou iniciar investigações ao amparo da *Section 301* do *Trade Act of 1974*, instrumento que historicamente fundamenta sanções comerciais unilaterais. A ação concentra-se especialmente sobre a adoção de *Digital Services Taxes* (DSTs) por países como França, Áustria, Itália, Espanha, Turquia e Reino Unido, mas se estende a qualquer regime tributário ou regulatório que, na interpretação dos EUA, discrimine empresas americanas ou afete sua competitividade global.

Para o Brasil, em um contexto no qual iniciativas nacionais como o Pix já são questionadas[347], os riscos decorrentes desse novo arranjo são múltiplos. Em primeiro lugar, eventuais iniciativas de tributação de serviços digitais ou tributação de dados[348] – em discussão no país como forma de ampliar a base fiscal frente ao crescimento da economia de plataformas – poderiam ser interpretadas como prática discriminatória, sujeitando o país a sanções tarifárias.

Em segundo lugar, políticas de regulação do audiovisual ou de plataformas de streaming que imponham cotas de produção nacional correm o risco de serem caracterizadas como barreiras injustas ao capital estrangeiro, acionando dispositivos de retaliação. Em terceiro lugar, marcos regulatórios voltados à proteção de dados ou à regulação de riscos relacionados

346 THE WHITE HOUSE. **Defending American Companies and Innovators From Overseas Extortion and Unfair Fines and Penalties**, The White House. Disponível em: <https://www.whitehouse.gov/presidential-actions/2025/02/defending-american-companies-and-innovators-from-overseas-extortion-and-unfair-fines-and-penalties/>. Acesso em: 12 nov. 2025.

347 ALVIM, Mariana; GALLAS, Daniel, **Pix investigado por EUA: como Brasil defende sistema de pagamentos**, BBC News Brasil. Disponível em: <https://www.bbc.com/portuguese/articles/cm2vrnq17vdo>. Acesso em: 27 ago. 2025; SPADONI, STF, Anatel, Banco Central.

348 BELLI *et al*, Proteção de dados, tributação de dados e equidade de dados: equilíbrio entre valores, riscos e obrigações.

a sistemas de IA, exigência de transparência algorítmica ou políticas de moderação de conteúdo podem ser percebidos como formas de regulação desproporcionais que forçam alterações no modelo de negócios das grandes corporações digitais, ensejando igualmente respostas unilaterais.

As implicações econômicas e estratégicas são significativas. Tarifações retaliatórias sobre exportações brasileiras – particularmente, em setores estratégicos como agronegócio, manufaturas ou mineração – representariam não apenas perdas financeiras imediatas, mas também a erosão do capital político necessário para sustentar a autonomia (tecnológica) do país para definir suas próprias políticas de regulação. Nesse sentido, a soberania digital conecta-se diretamente à soberania econômica: iniciativas legítimas de defesa do interesse público por meio de regulação, e até política industrial direcionada ao estímulo do setor digital, podem ser restringidas por mecanismos de coerção comercial, criando um dilema permanente para países em desenvolvimento.

Diante desse cenário, torna-se imperativo que o Brasil adote sistemas de análise de risco e estratégias de mitigação de tais riscos. Dentre elas, destacam-se a necessidade de estruturar políticas digitais com alto grau de transparência, objetividade e embasamento em dados empíricos, e alinhamento a padrões internacionais, de modo a reduzir a margem para alegações de discriminação; a intensificação da atuação em fóruns multilaterais de comércio e de governança digital, buscando contrabalançar práticas unilaterais com intuito de definir regras comuns que possam favorecer interoperabilidade com sem sacrificar a possibilidade de preservar os valores constitucionais; e o fortalecimento do ecossistema tecnológico doméstico, de modo a permitir maior resiliência frente a sanções externas.

3.8 Uso coercitivo das interdependências

A análise do fenômeno do uso coercitivo de interdependências globais revela uma transformação profunda na natureza das relações internacionais. Como destacamos nas seções precedentes, a globalização das últimas décadas, longe de ter simplesmente fragmentado o poder estatal ou dispersado a influência em redes difusas e igualitárias, produziu uma reestruturação no centro de gravidade do poder: das negociações estatais

multilateralistas para redes econômicas, financeiras e informacionais, dominadas por poucos "hubs" centrais, frequentemente por meio de sistemas gerenciados por organizações privadas.[349]

Esses nós centrais, localizados predominantemente em economias avançadas, acumulam grau de conexão muito superior à maioria dos demais atores da rede, gerando desigualdades estruturais duradouras entre Estados. Esse desenho assimétrico de redes constitui a base material daquilo que a doutrina define *como weaponized interdependence* ou uso coercitivo das interdependências.[350] A partir da junção de dois fatores essenciais, o controle jurisdicional ou institucional sobre nós centrais da rede e existência de normas e instituições domésticas que permitam sua exploração, alguns Estados adquirem a capacidade de usar essas redes como instrumentos de coerção internacional.[351]

Nesse contexto, a coerção assume duas formas principais: o efeito "panóptico" e o efeito "ponto de estrangulamento" (*chokepoint*).[352] No primeiro, o Estado controlador utiliza sua posição central para monitorar fluxos de informação, transações financeiras e comunicações, obtendo vantagem informativa e visibilidade sobre atividades de outros atores. No segundo, ele é capaz de interromper ou bloquear o acesso de adversários ou Estados-alvo às redes globais: cortando canais de informação, logísticas ou financeiras essenciais, impondo custos econômicos e pressionando por mudanças políticas ou de comportamento.

O trabalho de Farrell e Newman é particularmente interessante a esse respeito, porque os autores testam esse modelo por meio de casos concretos, notadamente o sistema de mensagens financeiras SWIFT[353] e as redes de comunicação que sustentam o funcionamento da internet. No âmbito

349 BELLI *et al*, Structural Power as a Critical Element of Digital Platforms Private Sovereignty.

350 FARRELL, Henry; NEWMAN, Abraham L., Weaponized Interdependence: How Global Economic Networks Shape State Coercion, **International Security**, v. 44, n. 1, p. 42–79, 2019.

351 *Ibid*.

352 *Ibid*.

353 **The Society for Worldwide Interbank Financial Telecommunication (SWIFT): Cooperative governance for network innovation, standards, and community**, Routledge & CRC Press. Disponível em: <https://www.routledge.com/The-Society-for-Worldwide-Interbank-Financial-Telecommunication-SWIFT-Cooperative-governance-for-network-innovation-standards-and-community/Scott-Zachariadis/p/book/9780415631648>. Acesso em: 26 nov. 2025.

financeiro, por exemplo, a centralidade da SWIFT - controlado por uma organização com finalidade não lucrativa com base na Bélgica - nas transferências internacionais de fundos conferiu a Estados com jurisdição sobre este hub a capacidade de impor sanções, excluir instituições financeiras e punir adversários.[354] Assim, infraestrutura de eficiência de mercado teoricamente neutra pode ser transformada em instrumento coercitivo para questões de segurança, terrorismo e não proliferação.

Exemplos recentes demonstram com clareza a operacionalização prática da interdependência coercitiva. De um lado, os Estados Unidos, ocupando posição central na rede global de semicondutores e na infraestrutura jurídica e tecnológica do setor de software, utilizam sua autoridade jurisdicional sobre empresas como NVIDIA, Intel, Microsoft e entidades reguladoras como o Bureau of Industry and Security (BIS) para impor controles unilaterais à exportação de chips avançados, tecnologia de litografia e licenças de software estratégico para a China.[355] Esses controles representam um típico uso do efeito chokepoint, ao limitar o acesso chinês a tecnologias críticas de alto desempenho em inteligência artificial, supercomputação e segurança nacional.

De outro lado, em reação às restrições estadunidenses, a China empregou sua própria forma de uso coercitivo de interdependências, explorando sua posição quase-monopolista da cadeia de produção e refino de minerais estratégicos, como gálio, germânio e antimônio, componentes essenciais na fabricação de semicondutores, sensores, sistemas ópticos e diversos produtos de alta tecnologia.[356] Tais restrições acabam expondo a vulnerabilidade estrutural americana (e global) diante da dependência de cadeias produtivas críticas. Ainda que tais minerais sejam geologicamente comuns, a China detém domínio sobre o refino global, consolidando sua

354 **The New Politics of Interdependence - Henry Farrell, Abraham Newman, 2015**. Disponível em: <https://journals.sagepub.com/doi/10.1177/0010414014542330>. Acesso em: 26 nov. 2025.

355 US BIS 2025 Commerce Closes Export Controls Loophole for Foreign-Owned Semiconductor Fabs in China; US BIS Export Controls to Restrict China's Capability to Produce Advanced Semiconductors 2024; GUPTA, Ritwik; WALKER, Leah; REDDIE, Andrew W., Whack-a-Chip: The Futility of Hardware-Centric Export Controls, 2024.

356 Ministry of Commerce Notice 2024 No. 46: Notice Concerning Strengthening Controls on Exports of Relevant Dual-Use Items to the United States. KLIMEK, Peter *et al*, **Systemic Trade Risk Suppresses Comparative Advantage in Rare Earth Dependent Industries**, arXiv.org. Disponível em: <https://arxiv.org/abs/2508.00556v1>. Acesso em: 26 nov. 2025.

capacidade de impor custos severos ao sistema produtivo norte-americano e demonstrando, assim, sua habilidade de utilizar interdependências econômicas como instrumentos estratégicos.

Assim, como pontuamos nas seções precedentes, a capacidade de controle é uma função da dependência tecnológica, reforçando o poder estrutural de certos Estados, mesmo sem recorrer a bloqueios.[357] Importa enfatizar, ainda, que essas formas de coerção não dependem necessariamente de rivalidades militares ou hostilidades bélicas tradicionais: elas se baseiam na arquitetura estrutural da economia global, construída originalmente por atores privados em busca de eficiência, e não como parte de uma estratégia geopolítica deliberada. Essas redes, uma vez cristalizadas, tornam-se difíceis de contestar ou reconfigurar, dado o elevado custo de romper dependências e substituir os hubs dominantes por estruturas alternativas. Por isso, mesmo países menores ou em desenvolvimento – sem necessariamente dispor de vasto poder militar ou econômico – podem encontrar-se sob coerção indireta, caso dependam em demasia de redes controladas por outros.

Dessa forma, o uso coercitivo de interdependências coloca em xeque premissas tradicionais de soberania e autonomia estatal: a interdependência econômica e informacional, longe de garantir cooperação e reciprocidade, pode repercutir em dominação estrutural. Nesse panorama, emergem desafios jurídicos e políticos relevantes: como preservar a autonomia decisória de Estados vulneráveis? Como regular redes transnacionais que operam fora de instâncias multilaterais democráticas? Como garantir que infraestruturas essenciais (financeiras, de dados, comunicações) não sejam convertidas em armas de pressão econômica ou espionagem?

Por fim, diante desse novo paradigma de poder – em que a topografia das redes globais confere vantagens estratégicas a poucos –, torna-se imperativo que Estados, especialmente aqueles fora dos centros tradicionais de rede, elaborem estratégias de soberania digital com base não somente na autonomia tecnológica, mas também na abertura e na cooperação. Isto significa reconhecer que a mera participação na economia global não garante autonomia: é necessário desenvolver capacidades domésticas de tec-

357 JONES, Erik; WHITWORTH, Andrew, The Unintended Consequences of European Sanctions on Russia, **Survival**, v. 56, n. 5, p. 21–30, 2014.

nologia, com base em base em padrões abertos e sistemas *open source* que limitem a vulnerabilidade a efeitos panópticos ou *chokepoints* externos, como destacamos na seção 1.3.

Assim, uma estratégia de soberania digital robusta deve levar em conta essas interdependências estruturais para assegurar que o desenvolvimento econômico e tecnológico não se traduza em dependência estratégica e vulnerabilidade coercitiva. O próximo capítulo analisará os atores que devem ser considerados para que seja construída uma governança efetiva da soberania digital.

4 Governança da soberania digital

O fortalecimento da soberania digital exige a articulação simultânea de atores de diferentes naturezas em múltiplas camadas interdependentes, a fim de organizar, de maneira consistente e eficiente, a pesquisa, o desenvolvimento e a regulação dos demais componentes do ecossistema digital. Tal necessidade é ainda mais evidente quando consideramos a soberania em IA, no âmbito da qual se inserem os FESIAs analisados na seção 2. Cada uma dessas camadas demanda arranjos regulatórios e institucionais próprios, com estruturas e burocracias específicas destinadas ao desenvolvimento de políticas públicas.

Ou seja, a governança da soberania digital deve ser considerada como um sistema de subsistemas, capaz de facilitar a comunicação, a coordenação e a colaboração entre os demais atores que atuam em cada camada e cada elemento dos sistemas. Porém, cabe ressaltar que, na enorme maioria dos países, a governança dos sistemas digitais não é enxergada de maneira sistêmica. Portanto, os arranjos existentes não são necessariamente estruturados seguindo um modelo ideal que combinaria política industrial voltada a promover pesquisa, desenvolvimento e inovação, com regulação voltada a evitar riscos e sancionar comportamentos abusivos, e governança multissetorial capaz de articular e organizar os atores de cada setor de maneira sinérgica e orgânica.

Particularmente, conforme será destacado nesta seção, no Brasil ainda não existe um mecanismo de governança capaz de integrar, ainda que de forma parcial, os diversos elementos setoriais relacionados aos Facilitadores Essenciais da Soberania em Inteligência Artificial (FESIAs). Essa situação se torna ainda mais complexa diante da fragmentação interna do Estado, entendida não apenas como divisão física em órgãos, ministérios, agências e setores especializados, mas também autonomia funcional – isto é, a existência de unidades que desenvolvem suas próprias agendas, regras internas e prioridades não necessariamente coordenadas[358]. Quando um objetivo de

358 SCHNEIDER, Volker. Redes de políticas públicas e a condução de sociedades complexas. **Civitas-Revista de Ciências Sociais**, v. 5, n. 1, p. 29-58, 2005. Disponível em: https://doi.org/10.15448/1984-7289.2005.1.33.

política pública envolve múltiplos setores, como é o caso da soberania digital, os desafios de coordenação tornam-se evidentes, pois, em cada camada, surgem subespaços decisórios com práticas e lógicas próprias.

Além da fragmentação estatal, é importante pontuar a inadequação do modelo tradicional hierárquico de desenvolvimento de políticas públicas, no qual a formulação e implementação das ações e iniciativas era uma prerrogativa exclusiva do Executivo e Legislativo. Atualmente, a literatura sobre governança em redes aponta para a crescente incapacidade dos recursos estatais e capacidades organizacionais alcançarem isoladamente os objetivos estabelecidos em políticas públicas complexas[359], como é o caso da soberania digital. A implementação da política pública, nesse novo paradigma, emerge de interações complexas entre uma variedade de atores estatais e não estatais.

É nesse contexto que ganha força a noção de governança multissetorial, entendida como subsídio à capacidade estatal.[360] O conceito de governança multissetorial transcende o conceito tradicional de condução de política pública exclusivamente pelo Estado, de maneira *top-down,* e remete a formas adicionais de condução social, envolvendo múltiplos atores públicos em diferentes níveis hierárquicos[361]. A política de soberania digital, portanto, não pode ser compreendida como um produto exclusivo da hierarquia governamental, mas como o resultado de interações entre diferentes instâncias da administração pública e outros atores de natureza não pública.

Esse cenário aponta para a conformação de uma governança em rede, em que políticas públicas deixam de ser implementadas exclusivamente pelo Estado e passam a incorporar a participação de diversos atores da sociedade. Além disso, conforme mencionado, a própria fragmentação da

---

359 RHODES, Roderick Arthur William. The new governance: governing without government. **Political studies**, v. 44, n. 4, p. 652-667, 1996. Disponível em: https://journals.sagepub.com/doi/10.1111/j.1467-9248.1996.tb01747.x. STOKER, Gerry. Governance as theory: five propositions. **International social science journal**, v. 50, n. 155, p. 17-28, 1998. MASSARDIER, G.. Redes de Política Pública. In: **Políticas Públicas** (Col.). Brasília: ENAP, v. 2, p. 161-186, 2007. Disponível em: http://www.enap.gov.br/index.php?option=com_docman&task=doc_view&gid=2870.

360 BELLI, **De la gouvernance à la régulation de l'internet**. p. 17-32

361 STOKER, Gerry, Governance as theory: five propositions, **International Social Science Journal**, v. 68, n. 227–228, p. 15–24, 2018; OFFE, Claus, Governance: An "Empty Signifier"?, **Constellations**, v. 16, n. 4, p. 550–562, 2009; LEVI-FAUR, David, **From "Big Government" to "Big Governance"?**, [s.l.]: Oxford University Press, 2012.

Administração Pública em múltiplos centros decisórios reforça a ideia de que a governança da soberania digital depende de mecanismos de coordenação e articulação efetivos.

No atual contexto político-institucional brasileiro, são vários os atores e interesses a serem coordenados e processados em uma eventual política pública sobre soberania digital – burocracias de diferentes níveis de governo, empresas de tecnologia, universidades e centros de pesquisa, sociedade civil etc. A próxima seção irá detalhar esses atores e suas respectivas atuações.

4.1 Principais atores na governança digital no Brasil

A governança da soberania digital no Brasil demanda a consideração de uma multiplicidade de atores com diferentes papéis, interesses e capacidades. A articulação e coordenação entre esses atores é fundamental para a implementação de políticas públicas eficazes e desempenha um papel vital para a construção da *situational awareness*, isto é, a aptidão institucional de manter uma percepção contínua do ambiente tecnológico, abrangendo não apenas o reconhecimento e acompanhamento de seus próprios recursos digitais, mas também a detecção, análise e resposta rápida a ameaças e oportunidades geradas pelas mudanças externas no cenário das tecnologias digitais. Abaixo, são listados alguns dos atores que fazem parte desse ecossistema da governança digital, que precisam ser considerados para a construção da soberania digital brasileira.

4.1.1 Atores públicos

I. Agência Nacional de Proteção de Dados (ANPD): criada pela Lei Geral de Proteção de Dados (Lei n.º 13.709/2018), a ANPD é o órgão responsável por zelar pela proteção de dados pessoais e fiscalizar o cumprimento da LGPD no Brasil. Sua atuação é importante, vez que a proteção de dados é um pilar fundamental para a autonomia dos cidadãos e do Estado no ambiente digital. A ANPD atua na regulamentação, fiscalização e aplicação de sanções em caso de descumprimento da lei, influenciando dire-

tamente a forma como dados são coletados, armazenados e utilizados no país. Cabe ressaltar que o Decreto nº 12.622/2025 ampliou as competências da ANPD consolidando-a como autoridade responsável para fiscalização do Estatuto Digital da Criança e Adolescente (Lei n.º 15.211/2025), além de converter sua natureza jurídica de autoridade em agência, com o objetivo de lhe conferir ainda mais autonomia e independência.

II. Agência Nacional de Telecomunicações (ANATEL): a ANATEL é a agência reguladora do setor de telecomunicações no Brasil. Sua função é regulamentar, fiscalizar e outorgar serviços de telecomunicações, garantindo a competição, a qualidade dos serviços, a cibersegurança das redes de telecomunicação e da infraestrutura de conectividade. Para a soberania digital, a ANATEL desempenha um papel crucial na regulação da infraestrutura de rede, na segurança das comunicações e na implementação de políticas que visam à universalização do acesso e à proteção dos direitos dos usuários de telecomunicações. A agência também atua na homologação de equipamentos, o que pode influenciar a adoção de tecnologias nacionais ou estrangeiras. A eventual ampliação das competências da Agência para abranger a governança e a fiscalização geral da cibersegurança, como previsto em várias propostas legislativas, tornará seu papel ainda mais central.

III. Conselho Administrativo de Defesa Econômica (CADE): o CADE é a autoridade responsável pela defesa da concorrência no Brasil, atuando na prevenção e repressão a práticas anticompetitivas e na análise de atos de concentração econômica. No contexto da economia digital, sua atuação torna-se particularmente relevante diante da crescente concentração de mercado em torno de grandes empresas de tecnologia e da centralização de dados e capacidades computacionais. A autoridade exerce papel estratégico ao assegurar condições competitivas nos mercados digitais, prevenindo abusos de posição dominante, práticas de exclusão e aquisições predatórias que possam limitar o desenvolvimento de empresas nacionais inovadoras. Além disso, por meio da análise de fusões e aquisições envolvendo empresas de tecnologia, dados e infraestru-

tura digital, o órgão pode contribuir para preservar a autonomia econômica e tecnológica do país, promovendo um ambiente concorrencial que favoreça a inovação, a abertura, a interoperabilidade e o fortalecimento do ecossistema digital brasileiro.

IV. Ministério da Ciência, Tecnologia e Inovação (MCTI): O MCTI desempenha um papel central no direcionamento da pesquisa, do desenvolvimento e da inovação tecnológica no Brasil. Para a soberania digital, o Ministério é vital para a promoção de tecnologias nacionais, para o apoio a centros de pesquisa e universidades e para a formulação de políticas que visem à redução da dependência tecnológica externa, como, por exemplo, o Plano Brasileiro de IA. Iniciativas relacionadas à inteligência artificial, à computação quântica e ao desenvolvimento de software livre frequentemente passam por sua alçada.

V. Ministério do Desenvolvimento, Indústria, Comércio e Serviços (MDIC): o MDIC, por meio de programas como o Nova Indústria Brasil, busca fortalecer a indústria nacional, incluindo o setor de tecnologia e incorporando aspectos de soberania digital às ações de suas seis missões – e.g., sua previsão de "desenvolver tecnologias da informação e da comunicação, com *domínio nacional de dados*"[362] (destaque nosso). Sua atuação é relevante para a soberania digital ao incentivar a produção local de hardware, software e serviços digitais, criando um ecossistema tecnológico robusto e menos dependente de importações. A política industrial voltada para o setor digital é essencial para a construção de capacidades tecnológicas próprias.

VI. Ministério da Gestão e da Inovação em Serviços Públicos (MGI): o MGI, por meio da Secretaria de Governo Digital, é responsável por coordenar a transformação digital da administração pública federal. A Rede Nacional de Governo Digital (Rede GOV.BR), sob sua coordenação, busca integrar e digitalizar os serviços públicos em todos os níveis de governo. Sua atuação é fundamental

362 CNDI, **Nova Indústria Brasil: Plano de ação para a Neoindustrialização**, Brasília: Conselho Nacional de Desenvolvimento Industrial, MDIC, 2024, p. 39.

para garantir que a digitalização do Estado seja feita de forma segura, eficiente e com foco na autonomia tecnológica, preferencialmente utilizando soluções nacionais e de código aberto.

VII. Ministério das Comunicações (MCom): o MCom é responsável pelas políticas de telecomunicações e radiodifusão no Brasil. Sua atuação impacta a soberania digital ao definir diretrizes para a infraestrutura de conectividade, como a expansão da banda larga e o desenvolvimento de redes 5G. A garantia de uma infraestrutura de comunicação robusta e segura é um pré-requisito para a soberania digital. Entre as medidas, destacam-se os investimentos do Fundo para o Desenvolvimento Tecnológico das Telecomunicações (Funttel), que destinou mais de R$ 1,5 bilhão para o BNDES e a Finep, para financiarem projetos de inovação e fabricação nacional de equipamentos[363], e cerca de R$ 58 milhões para projetos estratégicos conduzidos pelo CPQD[364]. Também se incluem a política de incentivo à instalação de redes de alta capacidade em obras públicas, conforme o Decreto n.º 10.480/2020, e a criação de programas de apoio a data centers e cabos submarinos nacionais, visando reduzir a dependência externa de infraestrutura crítica[365]. Essas ações reforçam a capacidade tecnológica interna e fortalecem a autonomia digital do país, consolidando a infraestrutura de comunicação como pilar essencial da soberania digital.

VIII. Ministério da Defesa: embora não seja um ator diretamente ligado à formulação de políticas digitais civis, o Ministério da Defesa e as Forças Armadas têm um papel crucial na ciberdefesa e

363 **MCom libera R$ 1,5 bilhão do Funttel para BNDES e Finep financiarem inovação em telecom até 2027**, Tele.Sintese. Disponível em: <https://telesintese.com.br/mcom-libera-r-15-bilhao-do-funttel-para-bndes-e-finep-financiarem-inovacao-em-telecom-ate-2027/>. Acesso em: 6 nov. 2025.

364 AGÊNCIA ESTADO, **Comunicações obtém aval para investir R$ 58 mi em infraestrutura**, CNN Brasil. Disponível em: <https://www.cnnbrasil.com.br/economia/macroeconomia/ministerio-das-comunicacoes-obtem-aval-para-investir-r-58-mi-do-funttel-em-infraestrutura>. Acesso em: 6 nov. 2025.

365 AQUINO, Miriam, **Redes de telecom voltam a ter prioridade na construção de obras de infraestrutura**, Tele.síntese. Portal de Telecom, internet e TIC. Disponível em: <https://telesintese.com.br/redes-de-telecom-voltam-a-ter-prioridade-na-construcao-de-obras-de-infraestrutura>. Acesso em: 6 nov. 2025.

na proteção de infraestruturas críticas, bem como na pesquisa e desenvolvimento de tecnologias digitais de uso militar. A defesa cibernética é um componente essencial da soberania digital, garantindo a resiliência do país em face de ataques e interferências externas. No âmbito da pesquisa e desenvolvimento tecnológico, o MD mantém uma rede institucional com esse propósito. Pode-se ilustrar tal atuação com o exemplo do Centro Tecnológico do Exército (CTEx), que é a unidade responsável pela pesquisa aplicada, pelo desenvolvimento e pelos testes de sistemas e equipamentos de defesa, abrangendo áreas de comunicação seguras, guerra eletrônica, sensoriamento remoto e IA, e da Fundação de Apoio à Pesquisa do Exército Brasileiro (FAPEB), entidade civil vinculada ao Exército que promove e coordena atividades de pesquisa científica, inovação e transferência tecnológica em cooperação com universidades, empresas e órgãos públicos.

IX. Conselho Interministerial sobre Transformação Digital (CITD): esse conselho tem como finalidade a coordenação da política industrial e digital, reunindo representantes de diversos ministérios, como Ciência e Tecnologia, Defesa, Comunicações, Educação e Economia. Sua atuação é essencial para garantir a comunicação, cooperação e coordenação, harmonizando as ações governamentais e garantindo uma abordagem integrada para a soberania digital, superando a fragmentação de políticas e promovendo a sinergia entre os diferentes órgãos.

X. Congresso Nacional (Câmara dos Deputados e Senado Federal): o Poder Legislativo é responsável pela criação e revisão das leis que regem o ambiente digital, como o Marco Civil da Internet, a Lei Geral de Proteção de Dados e o ECA Digital[366]. A atuação

366 Pode-se mencionar também a tramitação no Congresso Nacional de dois projetos de lei diretamente relacionados à consolidação do arcabouço jurídico da soberania digital no país. O Projeto de Lei n.º 2.338/2023, atualmente em análise na Câmara dos Deputados após aprovação no Senado Federal, propõe a criação de um marco regulatório para a Inteligência Artificial, estabelecendo princípios, direitos e deveres para o desenvolvimento e a utilização responsável de sistemas algorítmicos no Brasil. Há também o Projeto de Lei n.º 428/2024, em tramitação na Câmara dos Deputados, propõe alterações ao Marco Civil da Internet (Lei nº 12.965/2014) com o intuito de instituir um Marco Legal de Cibersegurança, disciplinando a comunicação de

de parlamentares e comissões especializadas é fundamental para moldar o arranjo institucional da soberania digital, refletindo os interesses da sociedade e as necessidades do país.

XI. Poder Judiciário: o Judiciário, em suas diversas instâncias, atua na interpretação e aplicação das leis digitais, resolvendo conflitos e garantindo o cumprimento dos direitos e deveres no ambiente digital. Decisões judiciais podem ter um impacto significativo não somente no que diz respeito a direitos relativos à proteção de dados, à privacidade e à liberdade de expressão, mas também na possibilidade do desenvolvimento e do uso de tecnologias digitais, na responsabilização de intermediários como provedores de plataformas etc.; portanto, influenciando diretamente as dinâmicas da soberania digital.

XII. Escritório do Embaixador Extraordinário para Tecnologia e Inovação: criada pela Portaria MRE n.º 621, de 8 de outubro de 2025, essa função institucional no Itamaraty reforça a diplomacia tecnológica brasileira, posicionando o país de forma estratégica em fóruns globais de inovação. O escritório atua como catalisador de cooperação internacional em ciência, tecnologia e inovação, promovendo parcerias com organismos multilaterais, governos estrangeiros e entidades privadas. Além disso, serve como canal de articulação para incorporar a agenda de tecnologia nos acordos diplomáticos, o que pode elevar a influência do Brasil nas políticas digitais globais.

XIII. Financiadora de Estudos e Projetos (FINEP): vinculada ao MCTI, a FINEP é a principal agência de fomento à ciência, tecnologia e inovação no Brasil. Sua atuação é fundamental para a soberania digital ao apoiar financeiramente projetos de pesquisa e desenvolvimento em áreas estratégicas, como inteligência artificial, cibersegurança e tecnologias digitais, tanto em empresas quanto em instituições de pesquisa.

incidentes, a proteção de infraestruturas críticas de informação e a adoção de padrões mínimos de segurança cibernética por entes públicos e privados.

XIV. Conselho Nacional de Desenvolvimento Científico e Tecnológico (CNPq): vinculado ao MCTI, o CNPq atua por meio de concessão de bolsas de pesquisa para estudantes, apoiando o desenvolvimento de projetos de pesquisa e desenvolvimento, além de promover a formação de recursos humanos qualificados em diversas áreas do conhecimento, incluindo as tecnologias digitais. Ele contribui para o fortalecimento da base científica e tecnológica nacional, essencial para a autonomia do país no ambiente digital.

XV. Coordenação de Aperfeiçoamento de Pessoal de Nível Superior (CAPES): vinculada ao Ministério da Educação (MEC), a CAPES desempenha um papel crucial no fomento à pós-graduação e na formação de recursos humanos no Brasil. Para a soberania digital, a CAPES contribui ao apoiar programas de pós-graduação em áreas de tecnologia, conceder bolsas de estudo para mestrado, doutorado e pós-doutorado, e promover a cooperação internacional em pesquisa. Sua atuação é essencial para a capacitação de profissionais que atuarão no desenvolvimento e na gestão de tecnologias digitais no país.

XVI. Banco Nacional de Desenvolvimento Econômico e Social (BNDES): o BNDES é o principal instrumento de financiamento de longo prazo para a realização de investimentos em todos os segmentos da economia brasileira. No contexto da soberania digital, o BNDES atua no apoio a projetos de infraestrutura digital, no financiamento de empresas de tecnologia nacionais e no desenvolvimento de cadeias produtivas ligadas ao setor, contribuindo para a autonomia tecnológica do país.

XVII. O Serviço Federal de Processamento de Dados (Serpro) desempenha papel central na promoção da soberania digital brasileira. Criado em 1964, o Serpro é responsável pelo desenvolvimento, gestão e proteção de sistemas digitais da administração pública federal, incluindo a Receita Federal, o Ministério da Economia e a Polícia Federal. Sua atuação busca a adoção de soluções inteligentes para transformação e inclusão digital, bem como assegura que dados sensíveis do Estado e dos cidadãos permaneçam sob

guarda e processamento em território nacional, reduzindo a dependência de plataformas privadas estrangeiras e fortalecendo a autonomia tecnológica do país. Além disso, o Serpro tem se destacado na oferta de soluções em identidade digital, segurança da informação e infraestrutura de nuvem governamental, elementos essenciais para a consolidação de uma governança digital soberana.

XVIII. A Dataprev – Empresa de Tecnologia e Informações da Previdência –, por sua vez, exerce função estratégica na gestão de dados e sistemas voltados à seguridade social e às políticas públicas de inclusão e proteção social. Responsável pelo processamento de benefícios previdenciários e trabalhistas, a empresa garante a integridade e a confidencialidade das informações de milhões de cidadãos brasileiros. Seu papel é crucial para assegurar que o Estado mantenha controle sobre informações sociais sensíveis, evitando vulnerabilidades decorrentes da terceirização tecnológica. Ao desenvolver internamente soluções de automação, interoperabilidade e inteligência de dados, a Dataprev contribui para a eficiência administrativa e para a preservação da soberania informacional do Brasil.

XIX. Os Centros Estaduais de Processamento de Dados (PRODEs), criados em diversas unidades da federação, desempenham papel relevante na consolidação da soberania digital em nível regional. Esses centros fornecem infraestrutura tecnológica essencial para secretarias estaduais, órgãos de segurança, educação e saúde, garantindo a gestão autônoma de dados públicos e a interoperabilidade entre sistemas governamentais. Ao fomentar o desenvolvimento de software público e a capacitação técnica de servidores, os PRODEs fortalecem a resiliência tecnológica do Estado e contribuem para um ambiente digital mais seguro, inclusivo e alinhado aos interesses nacionais.

XX. Por fim, as empresas públicas de tecnologia em nível estadual, como a Companhia de Tecnologia da Informação e Comunicação do Paraná (CELEPAR) ou a Companhia de Processamento

de Dados da Paraíba (CODATA), complementam esse sistema, atuando como vetores de inovação e infraestrutura nas administrações regionais. Elas são responsáveis por prover serviços de processamento de dados, redes seguras, sistemas de gestão pública e plataformas digitais de atendimento ao cidadão. Essas entidades fortalecem a capacidade técnica dos Estados, promovem a descentralização tecnológica e ampliam a autonomia administrativa dos entes federativos, assegurando que as políticas públicas digitais sejam implementadas de acordo com as necessidades locais e com respeito à proteção de dados e à transparência.

4.1.2 Atores da sociedade civil e academia

I. Instituições acadêmicas e de pesquisa. A participação de pesquisadores e instituições de ensino superior assegura rigor metodológico, visão crítica e capacidade de análise prospectiva, elementos indispensáveis para orientar decisões estratégicas em ciência, tecnologia e inovação. Além disso, o envolvimento da comunidade científica fortalece a legitimidade das políticas públicas, promove a transferência de conhecimento para o setor produtivo e estimula a formação de redes colaborativas que ampliam a autonomia tecnológica nacional.

II. Organizações da Sociedade Civil (OSCs) e Movimentos Sociais: diversas entidades, movimentos sociais, pesquisadores e ativistas atuam pela defesa da autonomia tecnológica e incidência política para a construção de um Plano Nacional para Soberania Digital. As OSCs representam uma voz importante na pressão por políticas mais alinhadas aos interesses nacionais e populares. Exemplos incluem o Instituto Brasileiro de Defesa do Consumidor (Idec) e o Núcleo de Informação e Coordenação do Ponto BR (NIC.br), que, embora seja uma entidade privada sem fins lucrativos, atua em prol da internet no Brasil e hospeda o CGI.br.

III. Comitê Gestor da Internet no Brasil (CGI.br): o CGI.br é um modelo multissetorial de governança da internet no Brasil, reunin-

do representantes do governo, setor empresarial, terceiro setor e comunidade acadêmica e tecnológica. Sua função é estabelecer diretrizes estratégicas para o uso e desenvolvimento da internet no Brasil, promovendo princípios como a neutralidade de rede, a proteção de dados, a liberdade de expressão e a inclusão digital. O CGI.br é um espaço fundamental para o debate e a construção de consensos sobre a governança da internet, incluindo aspectos da soberania digital.

IV. Empresa Brasileira de Pesquisa e Inovação Industrial (EMBRAPII): a EMBRAPII é uma organização social que atua por meio da cooperação com instituições de pesquisa tecnológica e empresas para o desenvolvimento de projetos de inovação. Ela não é uma empresa pública, pois não integra a administração direta ou indireta do Estado, e não possui capital público majoritário, mas é uma entidade privada de interesse público. Contudo, atua sob contrato de gestão com o Governo Federal, especialmente o MCTI, recebendo recursos públicos para apoiar projetos de inovação tecnológica em parceria com empresas e instituições de pesquisa. Sua missão é apoiar a indústria brasileira na superação de desafios tecnológicos, sendo um ator relevante para a soberania digital ao fomentar a pesquisa aplicada e a inovação em tecnologias digitais, com foco na demanda do setor produtivo.

V. Rede Nacional de Ensino e Pesquisa (RNP): constitui ator estratégico na consolidação da soberania digital brasileira, ao articular infraestrutura, serviços e políticas públicas voltadas à comunidade de ensino e pesquisa. Criada em 1989 pelo então Ministério da Ciência e Tecnologia, com participação do CNPq, sua trajetória acompanha os primórdios da internet no país e revela a centralidade da coordenação estatal na construção de capacidades nacionais em redes avançadas. Estruturada como Organização Social desde 2002, a RNP opera sob contrato de gestão com o Ministério da Ciência, Tecnologia e Inovação (MCTI), mantendo financiamento interministerial e desempenhando funções que extrapolam a mera conectividade. Dentre essas funções, pode-se mencionar serviços estratégicos de identidade digital, certifica-

ção, comunicação acadêmica e segurança cibernética, fortalecendo a autonomia tecnológica do ecossistema científico.

4.1.3 Atores do setor privado

I. Pequenas e Médias Empresas de Tecnologia Nacionais: empresas brasileiras de software, hardware e serviços digitais são fundamentais para a construção de uma base tecnológica própria. O fomento a essas empresas, por meio de políticas de incentivo e de compras governamentais, é crucial para reduzir a dependência de fornecedores estrangeiros e fortalecer a soberania digital.

II. Federações e Associações Setoriais: entidades representativas de segmentos da economia digital, como associações de empresas de tecnologia, telecomunicações, comércio eletrônico e startups, desempenham um papel relevante na formulação de políticas públicas e na mediação entre o setor privado e o governo. Essas organizações contribuem com informações técnicas, análises de impacto regulatório e posicionamentos coletivos que ajudam a orientar decisões governamentais. Além disso, atuam como espaços de coordenação entre empresas, promovendo boas práticas, padrões técnicos e iniciativas de autorregulação que influenciam diretamente a governança do ecossistema digital.

III. Grandes Empresas de Tecnologia: empresas de grande porte, como Google, Meta, Amazon, Microsoft, Tiktok, entre outras, possuem um poder significativo no ambiente digital brasileiro devido à sua vasta infraestrutura, serviços e base de usuários. Embora sejam atores importantes na provisão de serviços, como visto, sua atuação também levanta preocupações sobre o controle de dados, a concorrência e a influência sobre o ecossistema digital nacional. A regulação dessas empresas é um desafio central para a soberania digital.

Todos os atores mapeados acima, em suas interações e dinâmicas, compõem o ecossistema da governança da soberania digital no Brasil. Em

torno de cada política, configuram-se mecanismos de coordenação, bem como espaços de negociação e decisão que reúnem diferentes atores estatais e sociais. Por essa razão, considerando a interseção de muitos atores de forma híbrida, a combinação de elementos heterogêneos na forma de incentivos e controles (técnicos e políticos) impõe dinâmicas de interação que devem ser gerenciadas por um centro estratégico, tal como colocado por Ronaldo Fiani[367]. A próxima subseção propõe a existência de uma estrutura destinada a articular e coordenar essa rede de atores voltada para o desenvolvimento da soberania digital.

4.2 Arranjo institucional para a coordenação da soberania digital: rumo a um Sistema Nacional para Autonomia Tecnológica

Para promover uma abordagem de política pública guiada pela soberania digital é necessário um arranjo institucional híbrido capaz de articular os diferentes tipos de atores mencionados acima, com o intuito de implementar, de maneira coordenada, uma visão de transformação digital fundamentada na autonomia tecnológica.

Considerando que as ações voltadas à construção da soberania digital necessitam de um agente com a capacidade de se sobrepor aos interesses individuais para promover uma visão de interesse público, considera-se que o Estado se situa em uma posição mais adequada para exercer o papel estratégico e central dessa rede de atores[368].

Justificando uma posição central do Estado, Ronaldo Fiani destaca três funções para os casos de desenvolvimento de ativos específicos: (i) coordenar investimentos privados para alcançar um equilíbrio superior; (ii) atuar de forma empreendedora, particularmente de médio a longo

367 FIANI, Ronaldo. Arranjos institucionais e desenvolvimento: o papel da coordenação em estruturas híbridas. Texto para Discussão, 2013. Disponível em: https://portalantigo.ipea.gov.br/agencia/images/stories/PDFs/TDs/td_1815.pdf.

368 Nesse sentido, esse trabalho se alinha aos trabalhos de Mazzucato para entender o Estado como agente promotor de desenvolvimento capitalista MAZZUCATO, Mariana, **O Estado empreendedor: Desmascarando o mito do setor público vs. setor privado**, São Paulo: Portfolio-Penguin, 2014.

prazo, fornecendo uma visão de futuro; e (iii) administrar conflitos.[369] A primeira função de coordenação mostra-se importante, porque em casos como a pesquisa e desenvolvimento de novas infraestruturas digitais, grandes investimentos em atividades de risco e formação de mão de obra especializada são indispensáveis para que o Estado atue garantindo um movimento coordenado de todos os agentes envolvidos, garantindo a estabilidade dos processos que levarão aos produtos finais.[370]

A segunda função, atuar de forma empreendedora, se deve a que somente o Estado pode programar as ações políticas de médio e longo prazo, necessárias para alcançar a soberania digital, projetando uma visão de futuro que formula novas possibilidades de transformação no ecossistema digital[371]. Ademais, o protagonismo em tecnologias digitais frequentemente envolve investimento em novas trajetórias tecnológicas, abertura e consolidação de novos mercados e, enfim, investimentos cercados de incerteza – para os quais o Estado é mais bem equipado, como provedor de investimento paciente e de longo prazo.[372]

Por fim, a terceira função se relaciona com as mudanças estruturais que novos programas podem ocasionar na economia, afetando o valor de ativos específicos e gerando ameaças de perda de demanda a atores que investiram no passado em determinadas atividades e ativos instrumentais para o desenvolvimento da soberania. Esses atores podem criar resistências ao processo de desenvolvimento, pelo que caberia ao Estado administrar esses conflitos da maneira mais consensual possível.[373]

---

369 FIANI, Ronaldo; INSTITUTO DE PESQUISA ECONÔMICA APLICADA (Orgs.), ARRANJOS INSTITUCIONAIS E DESENVOLVIMENTO: O PAPEL DA COORDENAÇÃO EM ESTRUTURAS HÍBRIDAS. In: **CAPACIDADES ESTATAIS E DEMOCRACIA: ARRANJOS INSTITUCIONAIS DE POLÍTICAS PÚBLICAS**, Brasília: Ipea, 2014.

370 CHANG, H. J.; ROWTHORN, R. Entrepreneurship and conflict management. The Role of the State in Economic Change, p. 31-47, 1995; FIANI, Ronaldo. Arranjos institucionais e desenvolvimento: o papel da coordenação em estruturas híbridas. **Texto para Discussão**, 2013, p. 38-44. Disponível em: https://portalantigo.ipea.gov.br/agencia/images/stories/PDFs/TDs/td_1815.pdf.

371 FIANI; INSTITUTO DE PESQUISA ECONÔMICA APLICADA (Orgs.), ARRANJOS INSTITUCIONAIS E DESENVOLVIMENTO: O PAPEL DA COORDENAÇÃO EM ESTRUTURAS HÍBRIDAS.

372 MAZZUCATO, Mariana. **The Entrepreneurial State.** London: Penguin, 2018.

373 FIANI; INSTITUTO DE PESQUISA ECONÔMICA APLICADA (Orgs.), ARRANJOS INSTITUCIONAIS E DESENVOLVIMENTO: O PAPEL DA COORDENAÇÃO EM ESTRUTURAS HÍBRIDAS.

Dessa forma, considerando a necessidade de promover a integração entre instituições públicas, níveis de governo e atores privados, entende-se que seria necessário um arranjo de governança para a Autonomia Tecnológica, cuja função fosse a coordenação de ações, envolvendo um quadro de pessoal, regras e procedimentos próprios; e idealmente vinculado à Presidência da República, que, por sua posição institucional, teria maior capacidade de articulação política e inserção no mais alto nível decisório do governo.

Além das funções listadas acima, esse arranjo também deveria possuir função regulatória, uma vez que o processo inovativo é, inevitavelmente, marcado por incertezas tecnológicas e de mercado, sobretudo nas fases iniciais do negócio. É justamente essa característica que justifica o apoio estatal. A regulação, nesse contexto, não atua apenas como um freio ou como resposta posterior às inovações, mas como elemento constitutivo do próprio ambiente no qual elas florescem.

A regulação pode fornecer segurança jurídica, criar incentivos adequados e abrir espaço para a participação dos setores sociais e atores privados, articulando-os para viabilizar a utilização dos variados instrumentos de política pública, como compras governamentais, incentivos fiscais, subvenções a P&D etc. A título de exemplo, uma inovação importante no direito foi a previsão legal na Lei de Licitações do instituto das encomendas tecnológicas[374], vez que esse instrumento não era utilizado por gestores em razão da insegurança jurídica pela ausência de tipicidade legal.[375] Dessa forma, a criação de regulação ou aperfeiçoamento de instrumentos jurídicos podem incentivar a inovação das empresas.

É importante enfatizar que a regulação, com o seu papel de desenhar as instituições, fornece condições para que o processo da inovação se desenvolva, incentivando o crescimento tecnológico. Conforme observado por Foss, Coutinho e Miterhof[376], "a regulação preexiste à inovação, além de voltar em seguida, para discipliná-la e catalisá-la, ajudando a fomentar as diversas externalidades que esse processo gera para a sociedade". Assim,

374 As encomendas tecnológicas serão abordadas na próxima seção, na parte de compras públicas.

375 FOSS, Maria Carolina; COUTINHO, Diogo; MITERHOF, Marcelo. A regulação para a inovação. **Jota**, 2023.

376 *Ibid*.

é um equívoco afirmar que a regulação compromete a inovação, esse problema dependerá da forma e das estruturas utilizadas para regular.

Nesse ponto, cabe destacar que esse arranjo também deveria inovar no que diz respeito à própria estratégia regulatória, incorporando e alavancando as infraestruturas públicas digitais (*Digital Public Infrastructures* – DPIs) como instrumentos tecno-regulatórios. Trata-se, portanto, de promover o desenvolvimento de protocolos abertos e de arquiteturas baseadas em *software* livre capazes de funcionar como plataformas públicas e interoperáveis, aptas a apoiar a digitalização de setores inteiros da economia.[377]

Além dessas funções, é igualmente necessário que esse arranjo institucional possua capacidade de articular e impulsionar os diversos atores envolvidos no processo de inovação, promovendo a capacitação de gestores públicos, a difusão de conhecimento e o apoio ao uso de instrumentos voltados à gestão inovadora, entre eles, as compras públicas para inovação. Como será discutido adiante, um dos principais obstáculos à utilização estratégica das compras governamentais reside no receio de sanções e na persistência de uma cultura burocrática marcada pela aversão ao risco e pela baixa tolerância à experimentação.

Nesse contexto, uma estrutura de governança capaz de fomentar mudanças culturais internas e externas, especialmente no diálogo com os órgãos de controle, revela-se essencial. Tal estrutura deveria contribuir para a construção de capacidades estatais, bem como para o fortalecimento de competências técnicas e relacionais entre os servidores públicos, de modo a criar um ambiente institucional mais propício ao desenvolvimento da inovação necessária ao avanço da soberania digital.

4.2.1 Agência ou Ministério para Autonomia Tecnológica?

Considerando o conjunto de funções anteriormente descritas, impõe-se a necessidade de definir um arranjo institucional capaz de desempe-

377 BELLI, New Data Architectures in Brazil, China, and India; BELLI, **Building Good Digital Sovereignty through Digital Public Infrastructures and Digital Commons in India and Brazil**; BELLI; MAGALHÃES, **AI Sovereignty and AI Governance: Perspectives from the BRICS and Beyond**; BELLI, Luca; ZINGALES, Nicolo, Interoperability to Foster Open Digital Ecosystems in the BRICS Countries, **SSRN Electronic Journal**, 2023.

nhá-las de maneira eficaz, efetiva e com a maior independência e estabilidade possível. A seção precedente já destacou que essas funções pressupõem uma entidade capaz de atuar de maneira transversal e de induzir comportamentos alinhados ao interesse público. Para que tais atribuições se tornem vinculantes e consistentes em âmbito nacional, esse arranjo precisa ser formalizado por lei, dotando-o de legitimidade e de autoridade para coordenar políticas de Estado.

A soberania digital não é uma noção separada da noção de soberania nacional e, por isso, esse vínculo reforça que as decisões sobre autonomia tecnológica têm natureza tipicamente estatal, pois envolvem escolhas sobre ativos estratégicos para o país. Além disso, a definição dessas diretrizes deveria idealmente permanecer ancorada nos mecanismos de atuação democrática e nos instrumentos clássicos de responsabilização política.

Nessa linha, em termos de arranjo institucional, a escolha adequada poderia ser pela instituição de um novo Ministério para a Autonomia Tecnológica ou conferir as atribuições mencionadas, relacionadas à soberania digital, a um ministério existente. Assim, a proximidade do tema ao Governo permitiria conferir hierarquia e prioridade a políticas de inovação, ciência e tecnologia, coordenando investimentos e alinhando agendas setoriais sob uma mesma orientação estratégica.

Apesar das vantagens desse desenho, a experiência política brasileira mostra que instabilidade institucional e pressões partidárias tendem a comprometer políticas de longo prazo, prejudicando a estabilidade e o sucesso de projetos voltado à pesquisa, desenvolvimento e adoção soluções tecnológicas alternativas, gerando insegurança jurídica para investimentos públicos e privados. Tais fatores explicam, em parte, por que reformas administrativas na década de 1990 resultaram na criação de agências reguladoras independentes, buscando mitigar a interferência política e proporcionar um ambiente regulatório estável.[378]

378 EDITORA, Juruá, **Teoria do Estado Regulador - Volume I - Coleção FGV Direito Rio**, Juruá Editora. Disponível em: <https://www.jurua.com.br/shop_item.asp?id=24100>. Acesso em: 25 nov. 2025.

O modelo de agências reguladoras surgiu no contexto da transição do Estado Intervencionista para o Estado Regulador[379], tanto no Brasil quanto internacionalmente. Ao delegar a regulação a entidades dotadas de autonomia técnica, buscou-se insular as agências das influências políticas, permitindo que os dirigentes atuem de forma técnica e com planejamento de longo prazo.

As agências reguladoras, concebidas como organizações públicas com poderes regulatórios e para as quais não há eleição popular, tampouco direção direta por oficiais eleitos, passaram a representar uma forma de desagregação institucional e "despolitização" ao promover uma separação mais nítida entre decisões técnicas e decisões políticas.[380]

É interessante destacar que a difusão dessas instituições, nos países em desenvolvimento, esteve associada, além disso, à influência de organismos internacionais como Banco Mundial, FMI e OCDE, bem como a processos de isomorfismo institucional.[381] De todo modo, independentemente da forma de incorporação, o modelo de Estado Regulador ganhou relevância por oferecer maior estabilidade decisória, previsibilidade normativa e especialização burocrática, atributos particularmente relevantes em contextos de rápida transformação tecnológica.

Tendo em vista que a soberania digital demanda políticas públicas estáveis, tecnicamente qualificadas e protegidas de oscilações conjunturais, poderia aventar-se a criação de uma agência reguladora como via institucional relevante. No entanto, conforme comentado anteriormente, as características da soberania digital e sua relação próxima e indissociável do conceito de soberania nacional tornam inviável um projeto de "despolitização" via formação de agência reguladora. Alternativamente, alguns arranjos possíveis seriam a atribuição de coordenação de políticas de soberania digital a estruturas já existentes, como um ministério ou uma secretaria especializada, a exemplo da Secretaria de Ciência e Tecnologia para

379 MAJONE, Giandomenico, From the Positive to the Regulatory State: Causes and Consequences of Changes in the Mode of Governance on JSTOR, **Journal of Public Policy**, v. 17, n. 2, p. 139–167.

380 CUNHA, Bruno Queiroz, Os regulocratas: características corporativas e implicações sistêmicas do funcionamento da burocracia das agências reguladoras no Brasil, **http://www.ipea.gov.br**, 2017; BELLI, **De la gouvernance à la régulation de l'internet**.

381 CUNHA, Os regulocratas.

a Transformação Digital do Ministério da Ciência, Tecnologia e Inovação, que já detém competências na formulação e coordenação de políticas públicas na área e poderia ser fortalecida em termos de capacidade técnica, governança e recursos; ou a formação de uma Agência Executiva para Autonomia Tecnológica, dotada de mandato claro, autonomia decisória, mecanismos de participação social e competências transversais como eixo estruturante de uma Política Nacional de Soberania Digital.

4.2.2 Explorar o que já existe: o Comitê Interministerial para a Transformação Digital (CITDigital), o Sistema de Administração dos Recursos de Tecnologia da Informação (SISP) e o Sistema Nacional de Processamento de Alto Desempenho (SINAPAD)

Para finalizar, cabe frisar que algumas instituições e sistemas existentes poderiam – e, na nossa opinião, deveriam – ser explorados de maneira mais proveitosa para construir uma governança da soberania digital no país. É o caso do Comitê Interministerial para a Transformação Digital (CITDigital), do Sistema de Administração dos Recursos de Tecnologia da Informação (SISP), e do Sistema Nacional de Processamento de Alto Desempenho (SINAPAD)

A fim de facilitar a articulação e a coordenação estratégica dos atores mencionados na seção precedente, poderia ser aproveitado o CITDigital, instituído pelo Decreto n.º 12.308/2024. Trata-se de uma instância já existente, que exerce função consultiva de elevada relevância institucional ao assessorar o Presidente da República na elaboração, implementação e monitoramento de políticas públicas voltadas à transformação digital.

Em sua estrutura, o Conselho Consultivo para a Transformação Digital congrega especialistas e representantes da comunidade científica, da sociedade civil e do setor produtivo. Esse órgão multissetorial poderia ser mobilizado como órgão desse novo arranjo institucional, sendo um mecanismo estratégico para articular e coordenar os atores mencionados na seção anterior, de modo a promover uma governança integrada e eficaz da soberania digital.

Ainda, o Conselho Consultivo do CITDigital poderia atuar como plataforma permanente de diálogo e governança multissetorial, contri-

buindo para o alinhamento de interesses, a identificação compartilhada de riscos e oportunidades e a formulação de diretrizes comuns para a agenda digital brasileira. A clara vantagem de se aproveitar um órgão já existente é que a articulação das funções de comunicação, coordenação e cooperação poderia ser implementada imediatamente.

Além do CITDigital, cabe ressaltar que, entre os demais sistemas existentes na Administração Pública brasileira, o Sistema de Administração dos Recursos de Tecnologia da Informação (SISP), instituído pelo Decreto n.º 7.579/2011, desempenha um papel particularmente relevante. Assim, o SISP representa a base organizacional e estratégica para o gerenciamento dos recursos de TI no âmbito do Poder Executivo Federal. Mais do que um instrumento de coordenação, o SISP pode ser compreendido como uma plataforma estruturante que deveria ser alavancada para a construção de um sistema nacional de soberania digital.

A arquitetura do SISP – que é composta por um Órgão Central (Secretaria de Governo Digital do MGI), Órgãos Setoriais, Seccionais e Correlatos – é voltada a criar um ambiente colaborativo entre mais de 250 órgãos e entidades federais. Esse arranjo governamental, já em vigor, possibilita a integração de políticas, infraestruturas, dados e serviços digitais, constituindo uma rede pública coordenada, capaz de produzir soluções tecnológicas próprias, seguras e alinhadas aos interesses nacionais.

Com atribuições que envolvem a padronização, integração e racionalização dos recursos de TI, o SISP oferece as bases necessárias para o desenvolvimento de plataformas governamentais interoperáveis, controle de infraestruturas críticas, gestão de identidades digitais e proteção de dados estratégicos. Essas capacidades são fundamentais para o fortalecimento de uma soberania digital, entendida como a capacidade do país de garantir autonomia sobre suas infraestruturas tecnológicas, seus dados e seus processos de decisão.

O fortalecimento do sistema com a recriação da Comissão de Coordenação do SISP, pelo Decreto n.º 11.736/2023, amplia a governança colaborativa e a participação estratégica dos órgãos na definição de políticas nacionais de Tecnologia da Informação e Comunicação (TIC). Esse ambiente possibilita a construção de diretrizes voltadas ao uso de tecnologias abertas, desenvolvimento de soluções nacionais, promoção da segurança e resiliência digital e redução da dependência de fornecedores estrangeiros.

Por fim, o SISP já inclui o Autodiagnóstico SISP, uma ferramenta que desempenha um papel estratégico na evolução do nível de maturidade digital de cada órgão integrante do sistema, funcionando como instrumento de análise e aprimoramento contínuo da governança de TI. Regulamentado pela Portaria SGD/MGI n.º 4.339/2023, ele possibilita a medição do Índice de Maturidade em Governança de Tecnologia da Informação e Comunicação (iGOVSISP)[382], permitindo identificar pontos fortes, lacunas e oportunidades de melhoria.

Com base nos dados coletados, os órgãos conseguem orientar suas políticas públicas de TIC, priorizar investimentos, definir ações estratégicas e fortalecer suas capacidades institucionais. Ao incorporar critérios relacionados à soberania digital – como será destacado na seção 5.2. –, o autodiagnóstico poderia se tornar também um instrumento fundamental para medir e impulsionar a capacidade do Estado brasileiro de garantir sua autonomia tecnológica.

O SISP poderia, portanto, ser alavancado para atuar como uma instância estratégica complementar ao CITDigital. Enquanto o SISP concentra-se na gestão dos recursos de TI dentro do Poder Executivo Federal, o CITDigital reúne diferentes atores de natureza pública e não pública, capazes de definir diretrizes nacionais amplas e integradas, voltadas a orientar não apenas a administração pública federal, mas também os setores produtivos, educacionais e científicos.

Nesse contexto, o CITDigital pode desempenhar o papel de órgão de governança multissetorial da soberania digital, coordenando políticas que extrapolam a esfera tecnológica e adentram campos como segurança nacional, competitividade econômica, direitos digitais e inclusão social. Enquanto o SISP oferece a base operacional e institucional para a implementação de soluções digitais no Estado, o CITDigital pode definir agendas estratégicas, priorizar investimentos estruturantes, incentivar o desenvolvimento de tecnologias nacionais e promover a cooperação entre governo, academia, sociedade civil e setor produtivo. Dessa forma, a sinergia entre CITDigital e SISP fortaleceria a capacidade do Brasil de planejar, executar e sustentar uma estratégia robusta de soberania digital.

382 **Autodiagnóstico - iGOVSISP**, Governo Digital. Disponível em: <https://www.gov.br/governodigital/pt-br/estrategias-e-governanca-digital/sisp/autodiagnostico-igovsisp/autodiagnostico>. Acesso em: 25 nov. 2025.

Por fim, o Sistema Nacional de Processamento de Alto Desempenho (SINAPAD), instituído pelo Decreto nº 5.156/2004, constitui a mais relevante infraestrutura pública brasileira dedicada ao provimento de recursos computacionais avançados para pesquisa científica, desenvolvimento tecnológico e aplicações estratégicas de interesse nacional.[383] Criado como política pública federal voltada à democratização do acesso à supercomputação, o SINAPAD opera sob a lógica da integração em rede de centros de computação distribuídos em universidades e instituições científicas e tecnológicas, conectados entre si por meio da Rede Nacional de Pesquisa (RNP) e orientados por diretrizes federais de fomento e governança.

A finalidade essencial do SINAPAD consiste em garantir que pesquisadores, órgãos governamentais e agentes econômicos tenham acesso à capacidade computacional de grande porte, necessária para a execução de simulações científicas complexas, análises numéricas avançadas e, mais recentemente, para o treinamento e operação de modelos de IA de grande escala.[384] Trata-se de um instrumento de política pública que busca superar as assimetrias regionais e institucionais no acesso à computação de alto desempenho, assegurando que o conhecimento científico e tecnológico não seja condicionado exclusivamente pela capacidade individual de cada instituição de financiar infraestruturas locais de grande porte.

Os ativos do SINAPAD compreendem supercomputadores instalados em diversos centros nacionais, cada qual dotado de conjuntos heterogêneos de CPU, GPU e arquiteturas híbridas capazes de atender demandas de modelagem matemática, bioinformática, previsão climática, engenharia computacional e inteligência artificial. Essa diversidade de plataformas, quando articulada em rede, permite flexibilidade de uso e alocação otimizada de recursos, além de redundância e resiliência operacional. O SINAPAD conta ainda com equipes técnicas altamente especializadas, responsáveis pela manutenção da infraestrutura, pelo suporte aos usuários e pela promoção de práticas avançadas de computação científica.

383 **Portal da Câmara dos Deputados.** Disponível em: <https://www2.camara.leg.br/legin/fed/decret/2004/decreto-5156-26-julho-2004-533126-publicacaooriginal-16208-pe.html>. Acesso em: 2 dez. 2025. **SINAPAD - Sistema Nacional de Processamento de Alto Desempenho**. Disponível em: <https://www.lncc.br/sinapad/>. Acesso em: 2 dez. 2025.

384 Relatório Seminário Pilha IA Soberana.

A modernização do SINAPAD torna o sistema apto a operar como infraestrutura de IA como serviço, ofertando ambientes seguros e padronizados, plataformas de MLOps, bibliotecas pré-instaladas e suporte especializado para pesquisadores e empresas nacionais. Dessa forma, o sistema deixa de ser apenas um provedor de capacidade bruta de processamento e passa a desempenhar um papel de indução tecnológica, reduzindo barreiras de entrada para agentes que não dispõem de capacidade computacional própria.[385]

O SINAPAD possui potencial singular para atuar como nó central do ecossistema nacional de inteligência artificial, ao permitir que modelos sensíveis, estratégicos ou de interesse público sejam treinados e executados em infraestrutura estatal, sujeita a controles jurídicos nacionais e a salvaguardas de segurança cibernética. Isso reduz dependências tecnológicas externas e fortalece a autonomia do país na produção de conhecimento científico e no desenvolvimento de tecnologias críticas.

A integração com o CITDigital e o SISP, no âmbito de um sistema brasileiro de soberania digital, pode permitir a articulação entre infraestrutura, governança de dados, formação de competências e políticas industriais, criando um arranjo institucional capaz de sustentar a construção da autonomia tecnológica em IA.

Ademais, a conformação federada do SINAPAD permite sua complementaridade com políticas regionais de inovação, promovendo a internalização de capacidades tecnológicas em diferentes regiões do país. A articulação com parques tecnológicos, polos de desenvolvimento e laboratórios avançados amplia o alcance do sistema e potencializa seu papel como instrumento de desenvolvimento territorial.

Assim, o SINAPAD apresenta-se como ativo estratégico, não apenas pelo que representa em termos de capacidade de processamento, mas pela função estruturante que desempenha na arquitetura nacional de soberania tecnológica, constituindo-se como elemento nuclear para a construção de soluções de IA capazes de responder aos desafios econômicos, sociais e ambientais do Brasil contemporâneo.

O capítulo 4 identifica os elementos centrais de um futuro Sistema Nacional de Soberania Digital, entre os quais acreditamos que o CITDigital, o SISP e o SINAPAD deveriam desempenhar um papel fundamental. Antes

385 BELLI, **Building Good Digital Sovereignty through Digital Public Infrastructures and Digital Commons in India and Brazil**.

de ingressar nos detalhes de tal sistema, porém, a próxima seção explora os diversos instrumentos públicos que podem ser utilizados para a política pública de soberania digital.

4.3 Instrumentos públicos existentes para implementação da política de soberania digital

Para implementar políticas públicas voltadas ao fortalecimento da soberania digital, diversos instrumentos podem ser utilizados, tais como (i) gestão direta, particularmente interessante quando o Estado precisa manter capacidade governamental, (ii) corporações governamentais; (iii) regulação econômica ou social; (iv) contratação; (v) assistência financeira; (vi) renúncia fiscal; (vii) impostos corretivos ou taxas etc.[386] Como será destacado no próximo capítulo, tais instrumentos poderiam ser complementados com o uso da uma Avaliação de Autonomia Tecnológica[387] (AAT), voltada a permitir a análise prévia de qualquer produto e serviço digital utilizado pela administração pública.

É interessante pontuar que cada política pública, programa ou ação pode utilizar mais de um instrumento para sua implementação, sendo essa escolha um ponto de atenção, pois o instrumento utilizado influencia o próprio processo de implementação da política[388], levando à aproximação ou distanciamento dos objetivos originais guiados pela soberania digital. Desenhados pelos formuladores de políticas públicas como meio de alcançar os objetivos inicialmente traçados, esses instrumentos configuram-se como uma ação estratégica do Estado.

Um amplo espectro das políticas públicas de soberania digital está conectado às políticas públicas para promover a inovação[389], que se com-

386 Essa tipologia é apresentada por Salamon.SALAMON, Lester M., **The Tools of Government: A Guide to the New Governance**, Oxford: Oxford University Press, USA, 2002.

387 A Avaliação de Autonomia Tecnológica e os critérios necessários para efetuar tal analise serão analisados na seção 5.4.

388 OLLAIK, Leila Giandoni; MEDEIROS, Janann Joslin, Instrumentos governamentais: reflexões para uma agenda de pesquisas sobre implementação de políticas públicas no Brasil, **Revista de Administração Pública**, v. 45, n. 6, p. 1943–1967, 2011.

389 Segundo Edler e Fagerberg, a inovação é compreendida como a introdução de novas soluções para responder a problemas ou desafios originados da sociedade. EDLER, Jakob; FAGERBERG, Jan, Innovation Policy: What, Why & How, **Working Papers on Innovation Studies**, 2016.

plementam e se relacionam às políticas de ciência e tecnologia e as políticas industriais *lato sensu*[390]. E, por isso, ela será o foco desta seção.

A política pública voltada para inovação pressupõe a atuação estatal por meio de determinados instrumentos. Esses instrumentos podem atuar na oferta, sendo voltados à construção de capacidades tecnológicas, e na demanda, sendo destinados a estimular a adoção e a difusão de inovações, ampliando a demanda por novos produtos e serviços e criando condições favoráveis à sua absorção.

Entre os mecanismos disponíveis ligados à oferta estão subvenções, incentivos fiscais à pesquisa e desenvolvimento (P&D) e apoio de atividades de pesquisa em universidades, enquanto entre os instrumentos ligados à demanda estão as compras públicas, capital de risco, instrumentos de apropriação regulação e estímulos para o setor privado inovar. Aplicados de modo seletivo ou genérico, esses instrumentos permitem ao Estado não apenas mitigar riscos, mas também orientar trajetórias tecnológicas estratégicas. É interessante pontuar que a classificação dos mecanismos de política nos eixos da oferta e da demanda não é mandatória, sendo cada vez mais evidenciado, pela literatura, que os instrumentos de política são complementares e devem interagir.[391]

Nesse contexto, a racionalidade que sustenta tal interação encontra respaldo na concepção da inovação como um processo sistêmico, interativo e não linear. A crítica ao modelo linear de inovação, predominante nas políticas voltadas exclusivamente ao lado da oferta, impulsionou a adoção do referencial dos Sistemas Nacionais de Inovação (SNI), segundo o qual a geração, a difusão e a absorção de inovações dependem da articulação entre múltiplos atores e da dinâmica de aprendizado coletivo.[392]

---

390 Conforme pontuado por Rauen, a P&D não é a única fonte para a inovação. RAUEN, André Tortato, COMPRAS PÚBLICAS PARA INOVAÇÃO NO BRASIL: O PODER DA DEMANDA PÚBLICA, *in*: **Compras públicas para inovação no Brasil : novas possibilidades legais**, Brasília: IPEA, 2022, p. 15–38.

391 CUNNINGHAM, Paul *et al*, The innovation policy mix, *in*: EDLER, Jakob *et al* (Orgs.), **Handbook of Innovation Policy Impact**, [s.l.]: Edward Elgar Publishing, 2016; FOSS, Maria Carolina, **COMPRAS PÚBLICAS COMO INSTRUMENTO DE POLÍTICA DE INOVAÇÃO ORIENTADA À DEMANDA: EXPERIÊNCIAS NO BRASIL, NOS ESTADOS UNIDOS E NA UNIÃO EUROPEIA**, Unicamp, 2019.

392 EDQUIST, Charles, Striving Towards a Holistic Innovation Policy in European Countries -But Linearity Still Prevails!, **STI Policy Review**, v. 5, n. 2, p. 1–19, 2014; LUNDVALL, Bengt-Åke, National Systems of Innovation: Towards a Theory of Innovation and Interactive Learning, *in*: **The Learning Economy and the Economics of Hope**, [s.l.]: Anthem Press, 2016, p. 85–106.

Sob essa perspectiva, políticas de inovação efetivas não podem restringir-se ao fortalecimento da base científica e tecnológica ou ao estímulo à pesquisa e desenvolvimento, mas devem igualmente considerar instrumentos que ampliem a demanda por inovações, promovam a participação dos usuários no processo de desenvolvimento e criem condições institucionais para sua absorção. Essa abordagem holística permite superar a fragmentação típica das políticas centradas em um único eixo e contribui para alinhar os incentivos governamentais às necessidades dos diversos atores envolvidos no sistema de inovação.

Cumpre destacar que Foss, analisando os caminhos trilhados por governos europeus nos incentivos à ciência, tecnologia e inovação (CT&I), alertou para um paradoxo da inovação. Segundo a autora, uma interpretação restritiva dos sistemas de inovação levou a programas e políticas que investiram em P&D e investimentos em setores de tecnologia que não trouxeram os retornos esperados.[393]

Nesse sentido, Mazzucato[394] afirma que há um mito de que o acúmulo de P&D conduz à inovação, o que se alinha à posição de Lundvall[395]. Segundo os referidos autores, países europeus centraram esforços nas políticas de inovação orientadas à oferta e os resultados econômicos ficaram aquém das expectativas. Esse fato poderia ser considerado como uma das possíveis explicações para os resultados desanimadores em termos de soberania digital no velho continente.[396]

Foss defende o uso de mecanismos e instrumentos de política do "eixo" da demanda, em vez de apenas concentrar as estratégias de incentivo à inovação do lado da oferta. Para exemplificar a variedade das possibilidades de

---

393 FOSS, Maria Carolina, **Compras públicas como instrumento de política de inovação orientada à demanda: experiências no Brasil, nos Estados Unidos e na União Europeia.**, tese de doutorado, Universidade Estadual de Campinas, Campinas, 2019, p. 14. *Ibid*.

394 MAZZUCATO, Mariana, **O estado empreendedor: desmascarando o mito do setor público vs. privado**, [s.l.]: Penguin-Companhia das Letras, 2021.

395 LUNDVALL, Bengt-Åke, **Innovation System Research and Policy: Where it came from and where it might go**, [s.l.: s.n.], 2007.

396 FOSS, Maria Carolina, **Compras públicas como instrumento de política de inovação orientada à demanda: experiências no Brasil, nos Estados Unidos e na União Europeia**, tese de doutorado, Universidade Estadual de Campinas, Campinas, 2019.

instrumentos públicos a serem utilizados em políticas públicas de inovação, segue abaixo um infográfico desenhado por Maria Carolina Foss.[397]

Ademais, o Estado pode aplicar políticas horizontais, que abrangem a totalidade da economia (ex.: incentivos fiscais, crédito, infraestrutura, propriedade intelectual) e políticas verticais, voltadas a setores ou cadeias produtivas específicas. Um exemplo eloquente destas últimas foram as Parcerias para o Desenvolvimento Produtivo (PDPs) desenvolvidas pelo Ministério da Saúde, que se baseavam simultaneamente na demanda observada no SUS e na necessidade de reforço da capacidade tecnológica da base produtiva nacional.

Entende-se que tais parcerias deveriam ser expandidas e alavancadas na perspectiva da construção da soberania digital nacional, especialmente considerando o potencial para desenvolvimento de sistemas de IA de ponta com base nos enormes ativos nacionais existentes no setor da saúde pública, em termos de dados, de tecnologias, de capital humano e de governança. Tais ativos poderiam ser aproveitados para o desenvolvimento de sistemas de IA voltados à resolução de problemas e prioridades nacionais.

Nesse sentido, é interessante notar, ainda, a criação recente do Programa de Desenvolvimento e Inovação Local (PDIL) no âmbito da Estratégia Nacional para o Desenvolvimento do Complexo Econômico-Industrial da Saúde, modalidade que "visa promover o desenvolvimento da produção e inovação locais voltados aos desafios em saúde, a sustentabilidade e resiliência do Sistema Único de Saúde (SUS) e a ampliação do acesso à saúde, a fim de reduzir a vulnerabilidade produtiva e tecnológica do SUS"[398].

A expansão de tal programa na perspectiva de um investimento estratégico para transformação digital soberana do país, com o intuito de resolver problemas prioritários e de interesse público, parece mais que desejável.

Essa perspectiva desloca o Estado de uma função meramente garantidora das condições de mercado para a de agente promotor e direcionador de inovações e transformações sociotécnicas, conforme mencionado na seção anterior. Borrás e Edler[399] identificam múltiplos papéis estatais nesse pro-

397 *Ibid*.

398 BRASIL [MS], **Programa de Desenvolvimento e Inovação Local**, Ministério da Saúde. Disponível em: <https://www.gov.br/saude/pt-br/composicao/sectics/pdil/programa-de-desenvolvimento-e-inovacao-local>. Acesso em: 28 ago. 2025.

399 BORRÁS, Susana; EDLER, Jakob, The roles of the state in the governance of socio-technical systems' transformation.

cesso, que vão do observador ao facilitador, promotor, garantidor e iniciador – papéis associados a intervenções transformadoras. Em linha semelhante, a abordagem do "Estado empreendedor"[400] enfatiza políticas de inovação diretas capazes de gerar inovações radicais e difundi-las na economia.

A despeito da variedade de instrumentos relacionados nesta seção, as próximas subseções focam no aprofundamento de um dos instrumentos públicos disponíveis no "eixo da demanda": as compras públicas. A escolha desse instrumento se baseou na revisão teórica realizada por Foss[401], em que a referida autora expressou que as compras públicas correspondiam ao principal instrumento voltado para a demanda.

As compras públicas são instrumentos legais que permeiam diferentes setores e programas distintos do governo, já que podem ser aplicadas tanto às políticas industriais, como as de ciência e tecnologia e de inovação. Segundo Rauen[402], as compras públicas para inovação são voltadas ao problema do esforço inicial para aquisição, e, com isso, permitem usar o poder de compra do Estado "tanto para tentar desenvolver uma inovação, quanto para introduzir e difundir inovações já desenvolvidas". Essa combinação de desenvolvimento, indução e difusão de tecnologia autóctone é essencial no que diz respeito à promoção da soberania digital.

Antes de tratar do tema, porém, é relevante destacar que a análise dos instrumentos relacionados às compras públicas, apresentada na próxima subseção, não é realizada considerando todos os entes federativos, mas concentra-se, de forma geral, em órgãos da esfera federal. Cada instrumento de compra pública abordado possui peculiaridades que podem, ou não, restringir sua utilização por determinados entes federativos, de acordo com a regulamentação estadual ou municipal, bem como por entidades integrantes da administração indireta, como sociedades de economia mista e empresas públicas[403].

---

400 MAZZUCATO, **O estado empreendedor**.

401 FOSS, Maria Carolina, **Compras públicas como instrumento de política de inovação orientada à demanda: experiências no Brasil, nos Estados Unidos e na União Europeia**, tese de doutorado, Universidade Estadual de Campinas, Campinas, 2019; MAZZUCATO, O estado empreendedor.

402 RAUEN, COMPRAS PÚBLICAS PARA INOVAÇÃO NO BRASIL: O PODER DA DEMANDA PÚBLICA, p. 14.

403 É interessante notar, por exemplo, que a nova Lei de Licitações não se aplica para empresas públicas, sociedades de economia mista e suas subsidiárias, que são regidas por outras legislações (artigo 1º, § 1º da Lei 14.133/2021).

4.3.1 Compras públicas

As compras públicas correspondem ao processo pelo qual o Estado adquire produtos, serviços e contrata obras que atendam a seus interesses e necessidades, podendo envolver tanto produtos padronizados, já disponíveis no mercado, como soluções personalizadas ou inovadoras, inclusive estimulando o desenvolvimento de tais soluções por atores domésticos. São indispensáveis ao gerenciamento do setor público, uma vez que nem sempre este dispõe de capacidades para produzir o bem de que necessita ou, mesmo quando dispõe, é economicamente mais racional adquirir e contratar terceiros do que o Estado internalizar a produção e prestação de todos os bens e serviços que demandar.[404]

O aspecto relevante para esse trabalho é que, conforme colocado por Uyarra e Flanagan[405], esse instrumento pode ser utilizado para atingir objetivos de caráter social, econômico ou ambiental, bem como para criar e difundir inovações, utilizando o mercado consumidor como forma de apoio. As compras públicas para inovação distinguem-se das compras tradicionais ao incorporarem o risco tecnológico ao mecanismo de política pública, podendo alavancar um determinado negócio.

É importante, no entanto, alertar que a função principal da compra pública é resolver uma demanda concreta[406]. E, por isso, conforme afirmado por Rauen[407], a "tecnologia e a inovação são meios e não fins" em si mesmas.

Tradicionalmente, o regime jurídico de contratações públicas no Brasil foi estruturado, principalmente, pela Lei de Licitações e Contratos Administrativos (Lei 8.666/1993), posteriormente complementada por outras legislações, como a Lei do Pregão (Lei n.º 10.250/2002), a Lei da Inovação

404 FOSS, Maria Carolina, **Compras públicas como instrumento de política de inovação orientada à demanda: experiências no Brasil, nos Estados Unidos e na União Europeia**, tese de doutorado, Universidade Estadual de Campinas, Campinas, 2019,

405 UYARRA, Elvira; FLANAGAN, Kieron, Understanding the Innovation Impacts of Public Procurement, **European Planning Studies**, v. 18, n. 1, p. 123–143, 2010.

406 WEISS, Linda; THURBON, Elizabeth. The Business of Buying American: Public Procurement as Trade Strategy in the USA. Review of International Political Economy, v. 13, n. 5, p. 701-724, 2006. FOSS, Maria Carolina. **Compras públicas como instrumento de política de inovação orientada à demanda: experiências no Brasil, nos Estados Unidos e na União Europeia**. Tese. Universidade Estadual de Campinas, Campinas, 2019.

407 RAUEN, COMPRAS PÚBLICAS PARA INOVAÇÃO NO BRASIL: O PODER DA DEMANDA PÚBLICA.

(Lei n.º 10.973/2004), o Marco Legal de Ciência, Tecnologia e Inovação (Lei n.º 13.243/2016) e Lei Complementar das Startups (Lei Complementar n.º 182/2021). Em abril de 2021, foi promulgada uma nova Lei de Licitações e Contratos Administrativos, que incorporou muitos dos instrumentos de inovação previstos nessas normas esparsas (Lei n.º 14.133/2021).

O meio tradicional para se realizar uma compra pública é a licitação. Para realizá-la, existe um conjunto de regras destinadas a regular os contratos celebrados entre entes públicos e privados, cuja lógica central é assegurar a seleção da proposta mais vantajosa à administração, resguardar o princípio constitucional da isonomia entre competidores e atender a princípios de direito administrativo, como da legalidade, da impessoalidade, da moralidade, da publicidade, da probidade administrativa, da vinculação ao instrumento convocatório e do julgamento objetivo[408].

As modalidades previstas na Lei n.º 14.133/2021 são: (i) pregão; (ii) concorrência; (iii) concurso; (iv) leilão; e (v) diagnóstico competitivo (artigo 28 da Lei n.º 14.133/2021)[409]. Essas modalidades, entretanto, nem sempre são as mais adequadas para se promover a inovação. Para ilustrar o ponto, considere o pregão, modalidade mais utilizada pela Administração Pública Federal. É considerado como isonômico, impessoal e eficiente, mas nem sempre pode ser considerado como adequado para situações em que não há assimetria perfeita de informações e para aquisição de produtos complexos.

Rauen[410] destaca sete instrumentos de compras públicas previstos na legislação acima mencionada e que são comumente considerados mais adequados. São eles: i) diálogos competitivos; ii) concursos para inovação, com a possibilidade de negociação da propriedade intelectual; iii) encomendas tecnológicas; iv) contrato público de soluções inovadoras; v) margens de preferências adicionais; vi) compensação tecnológica em defesa; e, vii) parcerias para o desenvolvimento produtivo. Para uma melhor compreensão, cada um desses instrumentos será analisado nas próximas subseções.

---

408 BRASIL, Presidência da República, Lei de Licitações e Contratos Administrativos.

409 *Ibid*.

410 RAUEN, COMPRAS PÚBLICAS PARA INOVAÇÃO NO BRASIL: O PODER DA DEMANDA PÚBLICA.

4.3.1.1 Diálogo competitivo

O diálogo competitivo foi introduzido no ordenamento jurídico brasileiro (artigo 32 da Lei n.º 14.133/2021) como uma modalidade que busca maior flexibilidade e interação entre o poder público e potenciais contratados, especialmente em contratações complexas ou inovadoras.

Esse instrumento permite que a administração pública dialogue com possíveis contratantes previamente selecionados para identificar e desenvolver soluções que atendam a necessidades de interesse público. Essa modalidade se diferencia das licitações tradicionais por viabilizar a construção conjunta da solução durante o próprio processo licitatório, algo essencial em contextos de inovação tecnológica ou técnica[411].

Foss e Monteiro[412] destacam, entretanto, que esse instrumento é restrito a contratações que envolvam inovação tecnológica ou técnica, conforme art. 32 da Lei n.º 14.133/2021. Essa delimitação legal reflete o caráter excepcional e estratégico dessa modalidade, que deve ser utilizada quando não há solução pronta disponível no mercado ou quando as especificações do objeto demandam desenvolvimento conjunto entre Estado e fornecedores. É importante registrar que esse instrumento não serve para financiar atividades com risco tecnológico, como aquelas que envolvem P&D. Desse modo, pode-se concluir que essa modalidade de licitação pode ser utilizada para fomentar a introdução ou difusão da inovação, mas não o seu desenvolvimento[413].

Os autores destacam que a essência do instrumento está no próprio diálogo, o que o torna especialmente adequado para contratações voltadas à ciência, tecnologia e inovação (CT&I), onde o problema público exige soluções ainda não consolidadas[414]. Apesar do potencial, o uso do diálogo competitivo ainda é incipiente no Brasil e enfrenta desafios interpretativos, especialmente quanto à abrangência e cumulatividade dos requisi-

411 FOSS, Maria Carolina; MONTEIRO, Vítor, Diálogos competitivos motivados pela inovação, *in*: RAUEN, André Tortato (Org.), **Compras públicas para inovação no Brasil : novas possibilidades legais**, Brasília: IPEA, 2022, p. 239–270.

412 *Ibid*.

413 RAUEN, COMPRAS PÚBLICAS PARA INOVAÇÃO NO BRASIL: O PODER DA DEMANDA PÚBLICA.

414 FOSS; MONTEIRO, Diálogos competitivos motivados pela inovação.

tos legais. Foss e Monteiro[415] observam que a modalidade possui caráter inovador, mas exige amadurecimento institucional e normativo para que cumpra plenamente seu papel de instrumento de política pública de inovação. Inspirado em experiências da União Europeia e do Banco Mundial, o diálogo competitivo tende a ser mais eficaz quando aplicado a contratações complexas, nas quais a definição do objeto demanda colaboração técnica e aprendizado mútuo entre Estado e mercado.

4.3.1.2 Margens de preferências adicionais para bens e serviços nacionais

As Margens de Preferência Adicionais (MPAs) constituem um recurso que pode ser utilizado na licitação voltada à promoção da produção e da inovação nacionais por meio das compras públicas. Trata-se de um mecanismo que confere prioridade à aquisição de bens e serviços nacionais nas licitações realizadas pela administração pública.

Essa possibilidade de licitação está prevista no art. 26 da Lei n.º 14.133/2021, segundo o qual, no processo licitatório, poderá ser definida margem de preferência para bens manufaturados e serviços nacionais que atendam às normas técnicas brasileiras e para bens reciclados, recicláveis ou biodegradáveis. De forma específica, o § 2º do artigo 26 prevê a aplicação das MPAs aos bens e serviços de conteúdo inovador podendo a margem de preferência a que se refere o caput do artigo ser de até 20% (vinte por cento)[416].

As MPAs configuram-se como uma extensão das Margens de Preferência (MPRs), previstas originalmente na legislação brasileira, que permitem a preferência de bens e serviços produzidos no país, ainda que apresentem preço superior aos equivalentes importados, desde que dentro de um limite percentual previamente estabelecido. A peculiaridade das MPAs reside no fato de que o bem ou serviço beneficiado deve resultar de atividades de desenvolvimento e inovação tecnológica realizadas em território nacional.

Nesse sentido, as MPAs configuram-se como um instrumento de política de inovação pelo lado da demanda, ao permitirem que produtos ou

415 *Ibid*.

416 BRASIL, Lei de Licitações e Contratos Administrativos.

serviços produzidos com o desenvolvimento tecnológico ou inovação nacional possam ter preferência a produtos estrangeiros. Vale, por fim, registrar uma diferença das MPAs para outros instrumentos de uso de poder de compra do Estado: conforme apontado por Arcuri e Gonçalves[417], as MPAs têm o objetivo de ampliar ou facilitar o acesso a inovações que foram anteriormente desenvolvidas.

4.3.1.3 Compensação tecnológica em defesa

A compensação tecnológica constitui um elemento central do instrumento internacionalmente conhecido como *offset*, ou acordo de compensação, amplamente utilizado no comércio internacional de defesa. Esse mecanismo consiste na exigência, por parte de um país importador, de contrapartidas econômicas, industriais ou tecnológicas do fornecedor estrangeiro como condição para a aquisição de determinados bens ou serviços estratégicos. Tais contrapartidas são formalizadas por meio de contratos específicos, nos quais se estabelecem obrigações de transferência de benefícios, conhecimentos ou capacidades produtivas ao país comprador, caracterizando, assim, uma forma de contra comércio estratégico[418].

Segundo Rauen[419], essa é uma estratégia similar àquelas empregadas pelas PDPs. Isso significa que se vincula à aquisição de produtos ou serviços com tecnologia estrangeira à transferência dessa mesma tecnologia já incorporada.

No contexto brasileiro, a política nacional de *offsets* tem conferido especial ênfase à compensação tecnológica, direcionando esforços para promover a transferência de tecnologia (TT) e a capacitação técnica de instituições públicas das Forças Armadas e de empresas nacionais do setor industrial de defesa.

---

417 ARCURI, Marcos; GONÇALVES, João Emílio, Margens de preferência adicionais: recomendações para sua efetiva aplicação no Brasil, *in*: RAUEN, André Tortato (Org.), **Compras públicas para inovação no Brasil: novas possibilidades legais**, Brasília: IPEA, 2022, p. 271–308.

418 GIESTEIRA, Luís Felipe; MATOS, Patrícia de Oliveira, Compras públicas em defesa, *in*: RAUEN, André Tortato (Org.). **Compras públicas para inovação no Brasil : novas possibilidades legais**, Brasília: IPEA, 2022, p. 309–380.

419 RAUEN, COMPRAS PÚBLICAS PARA INOVAÇÃO NO BRASIL: O PODER DA DEMANDA PÚBLICA.

Segundo Giesteira e Matos[420], essa orientação estratégica visa reduzir a dependência tecnológica externa e fortalecer a base industrial de defesa (BID), promovendo o desenvolvimento tecnológico autônomo. Ademais, a política brasileira de *offsets* está alinhada às experiências internacionais de países que utilizaram esse instrumento como meio de realizar o "catch up" tecnológico, notadamente Índia e Coreia do Sul, cujas trajetórias evidenciam o potencial do *offset* como vetor de internalização de capacidades científicas e tecnológicas.

Um exemplo emblemático da aplicação desse tipo de compensação no Brasil é o Projeto Satélite Geoestacionário de Defesa e Comunicações Estratégicas (SGDC), iniciado em 2012, no âmbito do Ministério da Ciência, Tecnologia e Inovações (MCTI) e do Ministério da Defesa (MD). Para viabilizar o projeto e assegurar a transferência de tecnologia espacial, foi criada a Visiona Tecnologia Espacial, uma *joint venture* entre a Embraer e a Telebras, responsável pela aquisição do satélite junto à empresa estrangeira Thales Alenia Space.

O acordo firmado, denominado Acordo de Transferência de Tecnologia Espacial, estabeleceu as bases para a capacitação técnica nacional, sendo executado em duas etapas: a primeira, realizada na França, envolveu o treinamento de técnicos e engenheiros da Agência Espacial Brasileira (AEB), do Instituto Nacional de Pesquisas Espaciais (Inpe), do MD, da Visiona e do MCTI; a segunda, conduzida no Brasil, contemplou a participação de empresas nacionais receptoras da tecnologia, entre as quais se destacam AEL Sistemas S/A, Cenic Engenharia, Equatorial Sistemas S/A, Fibraforte Engenharia e Orbital Engenharia S/A. O projeto representou, portanto, um caso paradigmático de utilização bem-sucedida de *offset* como instrumento de política tecnológica, ao promover a internalização de conhecimento técnico e industrial no setor espacial brasileiro[421].

420 GIESTEIRA; MATOS, Compras públicas em defesa; RAUEN, COMPRAS PÚBLICAS PARA INOVAÇÃO NO BRASIL: O PODER DA DEMANDA PÚBLICA.

421 GIESTEIRA; MATOS, Compras públicas em defesa.

4.3.1.4 Parcerias de desenvolvimento produtivo de saúde

O setor de saúde é particularmente estratégico, devido, não somente às consideráveis capacidades em termos de pesquisa, desenvolvimento e governança, mas também à unicidade e abundância de ativos de altíssimo valor, como dados médicos de alta qualidade que podem ser alavancados para desenvolvimento de sistemas de IA soberanos de alta utilidade. Além disso, o setor é caracterizado por uma forma particular de Parcerias para o Desenvolvimento Produtivo (PDPs).

As PDPs configuram uma importante estratégia de utilização do poder de compra do Estado para reduzir as fragilidades tecnológicas do Sistema Único de Saúde (SUS) e diminuir a dependência internacional na área da saúde[422]. Trata-se de uma forma de contratação direta e está prevista na Lei 14.133, artigo 75, incisos XII e XVI.

Seu princípio econômico fundamental baseia-se na vinculação de contratos de aquisição pública à exigência de transferência de tecnologia do objeto adquirido. Em outras palavras, o Estado aceita a exclusividade temporária no fornecimento de determinado bem ou serviço, desde que a tecnologia necessária à sua produção seja integralmente transferida a uma instituição pública brasileira. Por essa razão, Rauen[423] afirma que as PDPs são especialmente adequadas para a introdução e difusão de inovações já consolidadas internacionalmente, em estágio de maturidade tecnológica, mas ainda não internalizadas no mercado nacional. Dessa forma, não há assunção de risco tecnológico por parte da Administração Pública.

Conforme explicam Pimentel, Paranhos e Chiarini[424], a estrutura de uma PDP envolve, tipicamente, três atores principais: o Ministério da Saúde (MS), responsável pela aquisição de medicamentos, vacinas, hemoderivados, equipamentos e materiais médico-hospitalares destinados ao SUS; a empresa privada parceira, encarregada de transferir a tecnologia de produção para o setor público; e o laboratório público receptor, que recebe

422 RAUEN, COMPRAS PÚBLICAS PARA INOVAÇÃO NO BRASIL: O PODER DA DEMANDA PÚBLICA.

423 *Ibid*.

424 PIMENTEL, Vitor Paiva; PARANHOS, Julia; CHIARINI, Tulio, Desdobramentos da nova lei de licitações nas parcerias para o desenvolvimento produtivo de saúde, *in*: RAUEN, André Tortato (Org.), **Compras públicas para inovação no Brasil: novas possibilidades legais**, Brasília: IPEA, 2022.

e internaliza essa tecnologia. O contrato entre as partes, de natureza jurídico-administrativa, é firmado sob a forma de convênio ou parceria público-privada, e prevê um prazo máximo de dez anos para a plena transferência tecnológica. Ao término desse período, espera-se que o laboratório público esteja capacitado para produzir o bem de forma autônoma e, potencialmente, replicar a tecnologia em outras instituições estatais, promovendo a chamada portabilidade tecnológica.

4.3.1.5 Concursos para inovação

Os concursos para inovação são modalidades de licitação, cujo objeto é a própria descrição do problema enfrentado pela Administração, com o propósito de premiar invenções ou inovações (tecnológicas ou não), avaliadas conforme critérios específicos e transparentes. A previsão normativa está nos artigos 30 e 93, § 2º, da Lei n.º 14.133/2021.

Um aspecto distintivo é que as regras de premiação – inclusive quanto à propriedade intelectual (PI) – são estabelecidas antes do início da competição, o que os caracteriza como prêmios *ex ante*. Essa modelagem diferencia os CIs de outros instrumentos de inovação, como o Contrato Público para Solução Inovadora (CPSI), pois dispensa a pré-seleção de candidatos e não exige o compartilhamento de riscos tecnológicos entre Estado e participantes[425].

Os concursos públicos para inovação são especialmente úteis em contextos em que há alta incerteza tecnológica ou assimetria de informações entre governo e potenciais inovadores. Nesses casos, o concurso permite mobilizar talentos diversos e chamar a atenção da sociedade para um problema existente, desde pesquisadores e startups até grupos independentes, ampliando a base de soluções possíveis. Além disso, os CIs são adequados para desafios sociais complexos, nos quais o Estado busca estimular a cria-

425 RAUEN, André Tortato, Concursos para inovação: como a licitação na modalidade concurso pode estimular o desenvolvimento e a introdução de soluções no mercado brasileiro, *in*: RAUEN, André Tortato (Org.), **Compras públicas para inovação no Brasil: novas possibilidades legais**, Brasília: IPEA, 2022, p. 431–466.

tividade coletiva sem comprometer-se, de imediato, com a aquisição de produtos ou serviços específicos[426].

Por seu baixo custo de implementação, transparência procedimental e capacidade de mobilização social, os CIs se mostram ferramentas valiosas para estimular a inovação aberta (*open innovation*) e *crowdsourcing*, integrando o poder público como catalisador da inovação e indutor da cooperação entre Estado, academia e setor privado[427].

4.3.1.6 Contrato público de solução inovadora

O Contrato público de solução inovadora (CPSI) consiste em um contrato firmado entre a administração pública e um ou mais parceiros privados com o objetivo de desenvolver, testar e, eventualmente, adquirir soluções inovadoras para desafios de interesse público. Trata-se de um instrumento que permite ao Estado assumir parte dos riscos tecnológicos inerentes ao processo de inovação, criando condições seguras para o desenvolvimento de soluções ainda em fase experimental[428]. Além disso, o CPSI pode ser considerado como um dos instrumentos mais inovadores estabelecidos pelo Marco Legal das Startups e caracteriza-se como uma modalidade de licitação na qual a seleção ocorre por meio de testes remunerados, conforme pode ser observado no capítulo VI da LC n.º182/2021.

A finalidade central do CPSI é estimular o desenvolvimento tecnológico nacional, fortalecer a capacidade inovadora das empresas e resolver problemas públicos complexos por meio de soluções inéditas. O contrato é estruturado em fases sucessivas, que incluem pesquisa, desenvolvimento, prototipagem, validação e eventual fornecimento. Caso a solução se mostre viável e atenda aos critérios técnicos definidos, a administração pública pode adquirir o produto ou serviço desenvolvido, dispensando nova licitação[429].

426 *Ibid*.

427 *Ibid*.

428 MENDONÇA, Hudson; PORTELA, Bruno Monteiro; NETO, Adalberto do Rego Maciel, Contrato público de soluções inovadoras: racionalidade fundamental e posicionamento no mix de políticas de inovação que atuam pelo lado da demanda, *in*: **Compras públicas para inovação no Brasil: novas possibilidades legais**, Brasília: IPEA, 2022, p. 467–492.

429 *Ibid*.

Embora tenha sido desenhado para startups, não se trata de uma aplicação exclusiva, o que permite que pequenas e médias empresas possam competir com grandes fornecedores globais, como *big techs*, já que essas podem ser remuneradas durante os testes.

Por suas características e pela possibilidade de remuneração de atividades que envolvem risco tecnológico, especialmente nas fases finais de pesquisa e desenvolvimento (P&D), os Contratos Públicos para Solução Inovadora (CPSIs) configuram-se como instrumentos adequados tanto para apoiar o desenvolvimento de tecnologias em estágios avançados de maturidade, quanto para favorecer a introdução e a difusão de inovações já consolidadas[430].

4.3.1.7 Encomenda tecnológica

A encomenda tecnológica é um mecanismo de fomento e contratação de pesquisa e desenvolvimento que viabiliza a aquisição de resultados de pesquisa ou o desenvolvimento de tecnologia sob encomenda, mediante contrato entre o poder público e entidades públicas ou privadas. Trata-se de um instrumento híbrido, que combina características de fomento (por apoiar atividades de pesquisa) e de contratação pública (por exigir a entrega de um resultado ou protótipo)[431].

Dessa forma, a solução demandada pelo poder público, voltada para o desenvolvimento de produtos, processos ou serviços inovadores, ainda não está disponível no mercado ou, embora já exista, não se encontra disponível por meio de uma relação comercial comum. Essa modalidade está prevista no artigo 20 da Lei n.º 10.973/2004, regulamentado pelo Decreto n.º 9.283/2018, e artigo 75, inciso V, da Lei n.º 14.133/2021.

As encomendas tecnológicas são especialmente relevantes por permitirem a remuneração de atividades de P&D com risco tecnológico, ou seja, em fases nas quais não há garantia de êxito técnico ou comercial. Essa

430 RAUEN, COMPRAS PÚBLICAS PARA INOVAÇÃO NO BRASIL: O PODER DA DEMANDA PÚBLICA.

431 NASCIMENTO, Henrique Fernandes *et al*, Desafios e aprendizados na execução de encomenda tecnológica: o registro da experiência no setor espacial brasileiro, *in*: RAUEN, André Tortato (Org.), **Compras públicas para inovação no Brasil: novas possibilidades legais**, Brasília: IPEA, 2022, p. 493–531.

característica as torna adequadas para projetos em níveis intermediários e avançados de maturidade tecnológica[432].

Outro aspecto fundamental é sua flexibilidade procedimental, que possibilita ajustes contratuais ao longo da execução, adaptando o escopo do projeto conforme os resultados obtidos. Isso contrasta com a rigidez típica das licitações tradicionais e favorece a experimentação e a colaboração tecnológica. Ademais, por prever a participação de universidades, institutos de pesquisa e empresas, a encomenda tecnológica promove a integração entre os setores público, acadêmico e produtivo, fortalecendo o ecossistema nacional de inovação[433].

Apesar dos avanços institucionais e normativos alcançados nas últimas décadas, persistem obstáculos significativos à sua plena operacionalização. A implementação efetiva desses mecanismos ainda enfrenta entraves de natureza jurídica, administrativa e cultural, que limitam o potencial transformador das políticas de inovação orientadas pela demanda estatal.

Nesse contexto, um relatório conjunto do Banco Interamericano de Desenvolvimento (BID) e do Tribunal de Contas da União (TCU)[434] evidencia que, embora o Brasil disponha de um sistema legal avançado em comparação internacional, há desafios concretos relacionados à governança, à capacidade técnica e à gestão de riscos que precisam ser superados para que as compras públicas cumpram plenamente seu papel como indutoras da inovação. É o que será abordado na próxima seção.

4.3.2 Desafios e soluções para a implementação das compras públicas para inovação

Embora o arcabouço normativo brasileiro tenha avançado de forma expressiva na criação de instrumentos voltados à promoção da inovação por meio das compras públicas, a efetividade prática desses mecanismos ainda enfrenta limitações significativas. Um relatório conjunto do Banco Interamericano de Desenvolvimento (BID) e do Tribunal de Contas da

432 *Ibid*.

433 *Ibid*.

434 BANCO INTERAMERICANO DE DESENVOLVIMENTO; TRIBUNAL DE CONTAS DA UNIÃO, **Modelo de Apoio a Compras Públicas de Inovação**, 2021: [s.n., s.d.].

União (TCU)[435] evidencia que, apesar do potencial transformador e da solidez jurídica do sistema, a utilização das compras públicas como instrumento de política de inovação é comprometida por obstáculos estruturais, institucionais e culturais.

O primeiro obstáculo refere-se à cultura institucional da administração pública, que não favorece a mudança nem a inovação. O segundo é a falta de competências técnicas. A ausência de gestão do conhecimento e de capacitação é considerada um dos maiores gargalos para o avanço das compras públicas para inovação. Essa lacuna envolve desde a compreensão de conceitos básicos à legislação aplicável. Soma-se a isso a ausência de uma visão estratégica sobre a área de compras, que muitas vezes é tratada como um meio burocrático e não como um setor central para a implementação de políticas públicas.

A falta de alinhamento entre os diversos atores também constitui barreira significativa. O sistema federativo gera incompatibilidades entre legislações e também entre decisões dos próprios tribunais para a resoluções de conflitos. Há, ainda, a insegurança jurídica provocada pelos órgãos de controle.

O medo do controle é outro fator limitante. O chamado "apagão das canetas" reflete o receio de gestores e servidores em adotar iniciativas inovadoras diante da possibilidade de serem responsabilizados pessoalmente. Dessa forma, o sistema de controle externo impõe ao gestor público a opção por contratos menos arriscados. Por outro lado, não se está defendendo que a solução seja a ausência de controle, uma vez que esse é importante para lidar com os gastos da Administração Pública. O problema envolve desafios de coordenação e aprendizado entre gestores e órgãos de controle, conforme exposto na seção anterior sobre governança.

Por último, há a escassez de recursos. A falta de tempo e orçamento limita fortemente a adoção de práticas inovadoras. No entanto, cabe frisar que o investimento em política industrial não deve ser enxergado como um gasto adicional. Ao contrário, tem o potencial de poupar os cofres públicos, considerando que parte desses recursos poderia ser redirecionada a partir dos valores já gastos pelo Estado, porém atualmente direcionados a serviços fornecidos por provedores de computação em nuvem estrangeiros.

435 *Ibid*.

Rauen[436] destaca que, no período de 2010 até 2016, de forma geral, no Brasil houve um gasto de R$ 710 bilhões em compras públicas, o que representou 9,2% do PIB. Esse valor, segundo o autor, corresponde à média praticada dos países da OCDE. Por outro lado, o orçamento do Fundo Nacional de Desenvolvimento Científico e Tecnológico (FNDCT) previsto para 2022 foi de apenas R$ 8,6 bilhões[437]. Ainda, um recente levantamento realizado por Silva *et al.*[438] indicou gastos em 23 bilhões do setor público com licenças de software, soluções de cloud, aplicações de segurança e serviços similares oriundos de corporações estrangeiras no período de 2014 a 2025.

Pode-se acrescentar, ainda, dois principais vetores de problemas, destacados por Foss[439], sobre o desenho, a implementação e o controle das compras públicas como instrumento de política de inovação no Brasil:

(i) Fraca articulação entre os objetivos das políticas públicas de inovação e o uso do poder de compra do Estado; e

(ii) Dificuldades de coordenação e cooperação entre órgãos e entes da administração pública responsáveis pelo desenho/implementação e o controle das compras públicas com risco tecnológico[440].

Cabe ressaltar que o destaque concedido para as compras públicas nesta subseção não significa que esse deve ser um instrumento utilizado de forma isolada. O que se buscou chamar atenção é que, considerando o volume de investimentos em compras públicas relacionadas à tecnologia,

436 RAUEN, André Tortato, MAPEAMENTO DAS COMPRAS FEDERAIS DE P&D SEGUNDO USO DA LEI DE INOVAÇÃO NO PERÍODO 2010-2015, *in*: RAUEN, André Tortato (Org.), **Políticas de inovação pelo lado da demanda no Brasil**, Brasília: IPEA, 2022, p. 481.

437 *Ibid*.

438 SILVA, Ergon Cugler de Moraes *et al*, **Contratos, Códigos e Controle A Influência das Big Techs no Estado Brasileiro**, São Paulo: [s.n.], 2025.

439 FOSS, **COMPRAS PÚBLICAS COMO INSTRUMENTO DE POLÍTICA DE INOVAÇÃO ORIENTADA À DEMANDA: EXPERIÊNCIAS NO BRASIL, NOS ESTADOS UNIDOS E NA UNIÃO EUROPEIA**; RAUEN, Concursos para inovação: como a licitação na modalidade concurso pode estimular o desenvolvimento e a introdução de soluções no mercado brasileiro.

440 FOSS, **Compras públicas como instrumento de política de inovação orientada à demanda: experiências no Brasil, nos Estados Unidos e na União Europeia.**

seu potencial de indução da inovação é maior quando comparado a outros mecanismos tradicionais de fomento[441].

Dessa forma, é importante registrar que o processo de implementação de eventual política pública de soberania digital não deve ser estanque e, ao contrário, o sucesso de qualquer estratégia ou plano de soberania digital dependerá da interação com as demais políticas industriais e de inovação já existentes, devendo sempre considerar para eleição dos instrumentos as necessidades políticas e sociais. Ademais, a adoção de uma racionalidade sistêmica voltada para inovação implica na elaboração de desenhos que permitam maior interação entre os instrumentos públicos voltados à oferta e os instrumentos públicos voltados à demanda.

4.3.3 Compras Públicas como Estratégia de Política Industrial Digital: Lições Internacionais e Aplicações no Brasil

Como destacado na seção precedente, compras públicas representam, em muitos países, um dos instrumentos mais poderosos de política industrial e tecnológica. Ao direcionar o poder de compra do Estado para produtos e serviços inovadores, governos podem criar demanda inicial, reduzir riscos de mercado e acelerar a maturação de tecnologias estratégicas. No âmbito de tecnologias digitais, essa abordagem tem se mostrado especialmente eficaz para fomentar ecossistemas nacionais de software, hardware, conectividade e cibersegurança, setores nos quais a escala e o domínio tecnológico são cruciais.

Nessa seção, concentra-se em uma seleção de exemplos específicos que ilustram, de formas distintas, como o gasto público pode ser utilizado não apenas para atender a necessidades imediatas do Estado, mas também para estruturar cadeias produtivas e tecnológicas. Primeiramente, analisaremos os casos paradigmáticos de Estados Unidos e China, que exploram compras públicas como alavanca da política industrial orientada às tecnologias digitais há décadas.

Cabe ressaltar que, nesses países, políticas públicas moldaram ecossistemas inteiros a partir de programas de compras estratégicas, não apenas

441 *Ibid*.

adquirindo tecnologias, mas também definiram requisitos, padrões e escalas que estimularam o surgimento e a consolidação de indústrias locais.

Em vez de atuar apenas como regulador ou financiador, o Estado assume o papel de "cliente-âncora", criando demanda inicial para tecnologias emergentes e garantindo condições de escala e aprendizado para fornecedores nacionais. Essa lógica se estende desde os supercomputadores e softwares de código aberto até serviços de nuvem soberana e soluções de cibersegurança.

Em seguida, mencionará a recente experiência da Áustria que, por sua vez, oferece um raro exemplo de iniciativa concreta voltada a fortalecer a autonomia tecnológica na União Europeia por meio de aquisição pública. Por fim, essa seção destaca que, no Brasil, o debate sobre inovação e compras públicas tem ganhado novo fôlego à luz de experiências como a da Petrobras, que ao encomendar supercomputadores de alta performance produzidos em parceria com a Positivo Tecnologia, demonstra que é possível alinhar demanda pública, capacidade produtiva nacional e avanço tecnológico. Assim esta seção analisa esses casos e distila diretrizes para o Brasil estruturar uma política de inovação digital sustentada por compras públicas.

É importante admitir, porém, que nem a política industrial nem as compras públicas são uma solução milagrosa e múltiplos exemplos demonstram que, como qualquer outra estratégia, podem falhar especialmente quando o Estado não tem uma relação realista com a economia global ou, ainda mais frequentemente, quando a política industrial é utilizada como desculpa para o clientelismo e o nepotismo.[442] Assim, as experiências internacionais devem ser estudadas como fonte de inspiração, entendendo, porém, que frequentemente não será possível replicar as mesmas soluções em contextos diferentes.

4.3.3.1 Estados Unidos: a tradição norte-americana de compras públicas para inovação

Os Estados Unidos possuem uma longa tradição de utilizar o poder de compra do Estado como ferramenta de desenvolvimento tecnológico, tendo adotado um arcabouço normativo e institucional dedicado ao longo

442 **Embedded Autonomy | Princeton University Press**. Disponível em: <https://press.princeton.edu/books/paperback/9780691037363/embedded-autonomy>. Acesso em: 6 nov. 2025.

das últimas sete décadas. Desde 1958, a *Defense Advanced Research Projects Agency* (DARPA) é o principal laboratório dessa lógica.[443] Por meio de contratos públicos, a DARPA impulsionou tecnologias que se tornariam pilares da economia digital: os protocolos da Internet (ARPANET), interfaces gráficas, semicondutores avançados e sistemas de GPS. O Estado, portanto, não apenas financiou pesquisa, mas atuou como demanda estruturante, conectando inovação científica e aplicação comercial.

Nos anos 2000, políticas como a Cloud First Policy[444] (2011) e os programas de procurement tecnológico do Departamento de Defesa e da General Services Administration (GSA) ampliaram o escopo do uso de compras públicas para estimular setores estratégicos, como computação em nuvem, segurança digital e inteligência artificial. Essas políticas criaram mercados previsíveis e de grande escala que favoreceram o surgimento de gigantes como Amazon Web Services (AWS), Microsoft Azure e Google Cloud, hoje líderes mundiais em serviços digitais.

Além disso, o marco regulatório estadunidense viabiliza e até incentiva a comercialização dos resultados da pesquisa e desenvolvimento financiados publicamente. O Bayh-Dole Act (1980) permitiu que universidades e pequenas empresas mantivessem a propriedade intelectual de inovações financiadas com recursos públicos, incentivando sua comercialização. O Small Business Innovation Research (SBIR) Act (1982), por sua vez, criou um mecanismo formal para que agências federais contratassem pequenas empresas em projetos de pesquisa aplicada e desenvolvimento tecnológico.

Um exemplo mais recente dessa abordagem é o Cybersecurity Collaboration Center[445] (CCC), criado pela National Security Agency (NSA) em 2020. O programa foi concebido para fortalecer o ecossistema nacional de cibersegurança, especialmente entre pequenas e médias empresas (PMEs) que integram a Defense Industrial Base (DIB), o conjunto de fornecedores da base industrial de defesa dos EUA.

---

443 PIIE Briefing 21-5: Scoring 50 years of US industrial policy, 1970-2020; CHENEY, David W.; VAN ATTA, Richard, 8. DARPA's Process for Creating New Programs, p. 229–288, 2020.

444 MULHOLLAND, Jessica, **What Obama Did for Tech: Cloud by Default**, GovTech. Disponível em: <https://www.govtech.com/computing/What-Obama-Did-for-Tech-Cloud-by-Default.html>. Acesso em: 6 nov. 2025.

445 **Cybersecurity Collaboration Center**. Disponível em: <https://www.nsa.gov/About/Cybersecurity-Collaboration-Center/>. Acesso em: 6 nov. 2025.

Mais de 70% do DIB é composto por PMEs que frequentemente não possuem recursos para implementar soluções de segurança de ponta. O CCC atua como um mecanismo de compra coletiva e assistência tecnológica, financiado com recursos públicos e operado em parceria com empresas privadas norte-americanas de cibersegurança. Assim, o CCC atua simultaneamente como centro de coordenação técnica e instrumento de política industrial. Ao financiar e contratar soluções nacionais[446] para oferecer serviços a outras companhias do setor, a NSA cria mercado interno, aumenta a escala produtiva e incentiva o investimento em P&D no setor de cibersegurança.

Essa abordagem reforça a autonomia tecnológica dos EUA, reduzindo a dependência de fornecedores estrangeiros e consolidando um ecossistema doméstico resiliente. O programa ilustra como compras públicas podem operar não apenas como gasto, mas como investimento estratégico, estimulando inovação e fortalecendo cadeias críticas.

Assim, o caso americano demonstra que o sucesso de uma política industrial digital depende da capacidade do Estado de atuar como cliente-âncora, oferecendo previsibilidade de demanda a empresas inovadoras; de fomentar a colaboração público-privada, integrando universidades, agências e empresas em programas de P&D aplicados; direcionar recursos públicos a setores estratégicos (como IA, semicondutores e cibersegurança), com foco em capacitação nacional; tratar compras públicas como instrumento de soberania tecnológica, e não apenas de eficiência administrativa.

4.3.3.2 China: planejamento estatal para construção de ecossistemas digitais

A China utiliza o poder do Estado de forma ainda mais explícita como ferramenta de política industrial. A Government Procurement Law (2002) estabelece que compras públicas devem priorizar produtos e serviços desenvolvidos domesticamente, especialmente em áreas consideradas estratégicas.[447] Essa abordagem foi reforçada por uma série de políticas industriais extremamente bem articuladas, lançadas a partir de 2014.

---

446 Ver BELLI *et al*, **Cibersegurança**; BELLI *et al*, **Governança e regulação da cibersegurança no Brasil**.

447 LI, Yanchao; GEORGHIOU, Luke, Signaling and accrediting new technology: Use of procurement for innovation in China, **Science and Public Policy**, v. 43, n. 3, p. 338–351, 2016.

Cabe ressaltar que o fortalecimento da indústria de semicondutores é considerado pilar da soberania tecnológica há mais de uma década e os avanços atuais são o resultado de tal visão estratégica. A China criou em 2014 o *National Integrated Circuit Industry Investment Fund* (o "Big Fund"), que financia empresas locais de design e fabricação de chips, e redefiniu o curso da indústria de circuitos integrados e a inovação tecnológica nesta área ao longo da década seguinte[448]. Paralelamente, compras públicas e contratos governamentais priorizam o uso de semicondutores desenvolvidos internamente.

Mesmo sob sanções internacionais, essa política combinada de financiamento público e preferência nas compras permitiu avanços notáveis em empresas como SMIC (fabricante de chips), Yangtze Memory Technologies (memórias flash) e diversos fornecedores de equipamentos e materiais semicondutores. O Estado chinês, portanto, atua não apenas como financiador, mas como consumidor estratégico, capaz de orientar a direção tecnológica de longo prazo.

A política "Internet Plus", lançada em 2015, organizou a transformação digital dos serviços públicos e das cadeias tradicionais de manufatura, agricultura, transporte e serviços.[449] Ela incentivou o uso de compras públicas e parcerias estatais para digitalizar setores produtivos e expandir a conectividade nacional. O governo central e as províncias passaram a adquirir plataformas digitais, softwares de gestão e soluções de computação em nuvem desenvolvidas por fornecedores chineses, estimulando o crescimento de empresas locais como Alibaba Cloud, Tencent Cloud e Baidu AI Cloud.

O Made in China 2025, também lançado em 2015, definiu metas concretas para aumentar a autossuficiência tecnológica e elevar a participação de produtos nacionais em setores de alta tecnologia.[450] As compras públicas, nesse contexto, funcionam como instrumento de internalização da demanda, garantindo mercado para empresas emergentes e reduzindo a

448 TONG, Xin; WAN, Xiaomeng, National industrial investment fund and China's integrated circuit industry technology innovation, **Journal of Innovation & Knowledge**, v. 8, n. 1, p. 100319, 2023.

449 WANG, China's digital transformation.

450 MADE IN CHINA 2025 The making of a high-tech superpower and consequences for industrial countries.

vulnerabilidade às oscilações do mercado global. Empresas como Huawei, ZTE, Lenovo, Inspur e Hikvision cresceram sob esse modelo. As demandas do Estado chinês em infraestrutura digital, 5G, vigilância e computação em nuvem forneceram escala e previsibilidade para o amadurecimento tecnológico dessas empresas que, em muitos casos, depois se tornaram líderes globais.

Por fim, o Plano de Desenvolvimento de Inteligência Artificial da China (2017) reforçou essa dinâmica, apesar de ter sido frequentemente criticado por ser excessivamente dispendioso.[451] Estabeleceu metas para tornar o país líder mundial em IA até 2030, com investimentos públicos maciços em infraestrutura digital, big data e supercomputação. Compras públicas de plataformas de IA para serviços públicos – em setores críticos, desde vigilância urbana até diagnósticos médicos – criaram um vasto mercado interno para empresas nacionais, impulsionando inovações que posteriormente se expandiram globalmente.

Assim, o modelo chinês mostra como compras públicas podem ser parte central de um planejamento industrial coerente, articulando P&D, financiamento e demanda. Ao mesmo tempo, reforça a importância de tratar a digitalização não apenas como mercado, mas como infraestrutura crítica de soberania nacional.

4.3.3.3 Áustria: conjugando compras públicas e código aberto para incrementar a soberania digital

Como já mencionado, embora a União Europeia e seus Estados-membros tenham liderado debates globais sobre regulação digital, eles avançaram pouco na produção de resultados práticos e transformadores. Ainda assim, apesar do limite geográfico, a iniciativa da Áustria merece destaque, tanto por sua simplicidade e capacidade de replicação quanto pelo papel central desempenhado por tecnologias de código aberto em sua implementação.

Em 2024, o Ministério da Economia da Áustria anunciou a adoção da plataforma Nextcloud – um provedor alemão de computação em nuvem com presença em vários países europeus – como alternativa a soluções

451 CHAN, Kyle *et al*, **Full Stack: China's Evolving Industrial Policy for AI**, [s.l.: s.n.], 2025.

proprietárias de grandes empresas dos EUA.[452] Essa decisão se insere em um movimento mais amplo que tenta construir concretamente a soberania digital europeia.

Cabe frisar que a solução austríaca é particularmente interessante porque alavanca as compras públicas para estimular a adoção de tecnologias que se alinham à normativa em matéria de proteção de dados pessoais, particularmente o Regulamento Geral de Proteção de Dados ou "GDPR", e da Diretiva NIS2, que exigem maior controle sobre a segurança de informação.

Cabe também ressaltar que as soluções de escritório como o Microsoft Office não são sistemas de IA altamente complexos e alternativas de código aberto estão prontamente disponíveis para a maioria das ferramentas. Nesse sentido, a mudança austríaca foi implementada em apenas quatro meses e priorizou a hospedagem em infraestrutura nacional, garantida pela infraestrutura da Nextcloud, com interoperabilidade entre sistemas já utilizados. Além de promover maior segurança e conformidade regulatória, a compra pública fortaleceu o ecossistema europeu de software de código aberto e serviços de nuvem locais.

Esse caso demonstra como mesmo países de menor escala econômica podem usar compras públicas para reposicionar o papel do Estado como articulador tecnológico, estimulando alternativas domésticas e regionais em setores dominados por grandes multinacionais.

4.3.3.4 O potencial das compras públicas para inovação digital no Brasil

No Brasil, várias empresas públicas e estatais, como Petrobras, Serpro, Dataprev e Embraer, têm capacidade orçamentária e técnica para atuar como clientes-âncora de tecnologias digitais nacionais. Por exemplo, o projeto do supercomputador Pégaso, desenvolvido pela Petrobras em parceria com a Positivo Tecnologia, é um caso emblemático de política industrial baseada na demanda pública.[453] A Petrobras contratou a Positivo Servers & Solutions

452 POHLMANN, Kim, Austria's Ministry of Economy takes decisive steps toward digital sovereignty.

453 **Positivo Servers industrializa servidores para supercomputador Pégaso**, Exame. Disponível em: <https://exame.com/bussola/positivo-servers-industrializa-servidores-para-supercomputador-pegaso/>. Acesso em: 6 nov. 2025.

para produzir, em território nacional, os servidores que compõem um dos supercomputadores mais potentes da América Latina.

Cabe ressaltar que essa parceria foi possível somente graças à colaboração com fornecedores estrangeiros (como Supermicro e NVIDIA). Assim, o exemplo ilustra que, ao pensar em autonomia tecnológica, não devemos pensar em autarquia, considerando que o caminho rumo à autonomia tecnológica passa necessariamente pela parceria internacional com atores estabelecidos, pelo menos no curto e médio prazo. No caso concreto, o resultado de tal parceria foi duplo: a estatal obteve infraestrutura tecnológica de ponta para suas operações de exploração e IA, enquanto a Positivo consolidou capacidade industrial e tecnológica em um segmento de alta complexidade.

O caso evidencia como uma compra pública estratégica pode estimular a produção nacional de infraestrutura computacional avançada, fomentar capacitação técnica e empregos qualificados; e conseguir também criar efeitos de demonstração para outras empresas públicas e privadas.

O caso da Petrobras com a Positivo mostra que, quando o Estado atua como comprador estratégico, é possível alinhar inovação, produção local e desenvolvimento tecnológico. Cabe frisar que, como destacamos acima, o Brasil já possui instituições, base legal e capacidade industrial suficientes para aplicar e replicar esse modelo.

O desafio é transformar essas experiências pontuais em política estruturada, com planejamento de longo prazo, metas claras de soberania digital e integração entre ministérios, estatais e agências de fomento. Nesse sentido, o próximo capítulo fornece uma série de pistas para que o Brasil possa, não apenas reduzir sua dependência tecnológica, mas também tornar-se produtor de soluções digitais críticas, inserindo-se de forma mais competitiva na economia digital global.

4.4 Empreendedorismo inovador, retenção e repatriação de talentos

A consolidação dos Facilitadores Essenciais da Soberania em Inteligência Artificial (FESIAs), em particular aquele relativo ao *humanware* (promoção e retenção de talentos), depende, não apenas da formação de

pessoas altamente qualificadas, mas também da criação de condições efetivas para que essas pessoas possam empreender e permanecer no país. Nesse contexto, torna-se estratégico estruturar um sistema nacional que facilite a criação e o crescimento de startups e empresas de base tecnológica, com ênfase em jovens empreendedores, tanto para mitigar a fuga de cérebros quanto para incentivar a repatriação de talentos.

Considerando as assimetrias salariais em relação a mercados como Estados Unidos ou União Europeia, é improvável que o Brasil consiga competir apenas por meio de remunerações diretas mais altas. Entretanto, o país pode atrair e reter talentos ao oferecer um ambiente especialmente favorável à criação de novos negócios intensivos em conhecimento, com trajetórias claras de crescimento, participação societária relevante e maior autonomia profissional. Em outras palavras, a política de soberania em IA deve combinar instrumentos de formação e pesquisa com um ecossistema de empreendedorismo inovador que reduza o custo de oportunidade de permanecer – ou retornar – ao Brasil.

Do ponto de vista de desenho institucional, esse sistema poderia articular, de forma coerente, diferentes instrumentos: (i) subsídios diretos e bolsas de empreendedorismo tecnológico para a fase de ideação e validação de produtos e serviços baseados em IA; (ii) regimes de baixa tributação ou mesmo tributação nula por período determinado para startups intensivas em FESIAs, condicionados a critérios de reinvestimento em P&D, qualificação profissional e geração de empregos qualificados; (iii) processos administrativos simplificados para abertura, alteração e fechamento de empresas de base tecnológica, idealmente por meio de uma plataforma pública integrada que conecte juntas comerciais, administração tributária, registros de propriedade intelectual e mecanismos de fomento; e (iv) apoio infraestrutural sob a forma de aluguel subsidiado em parques tecnológicos, laboratórios compartilhados (*labs*) e espaços de coworking associados a universidades e centros de pesquisa.

Esse arranjo deveria priorizar jovens empreendedores e pesquisadores, inclusive com a possibilidade de conversão parcial de bolsas acadêmicas e de pesquisa em capital semente para constituição de startups, bem como prever linhas específicas para brasileiras e brasileiros no exterior que desejem retornar ao país. A articulação entre políticas de repatriação de cientistas, programas de apoio ao empreendedorismo inovador e o marco regulatório

de startups permitiria transformar o retorno de talentos em oportunidades concretas de criação de empresas orientadas aos diferentes FESIAs.

Como frisamos, a agenda de soberania em inteligência artificial exige a construção de um sistema robusto de *humanware*, o que pressupõe formação, retenção e repatriação de talentos, mas também condições concretas para que pesquisadoras e pesquisadores construam empresas de base tecnológica. Antes de propor novos mecanismos, é útil observar que o Brasil já dispõe de bases legais e programas de fomento – ainda que fragmentados – voltados ao empreendedorismo inovador e à repatriação de cientistas.

A Lei Complementar nº 182/2021, conhecida como Marco Legal das Startups (MLS), constitui o principal instrumento jurídico para startups no país. Ela enquadra como startup a empresa com até dez anos de inscrição no CNPJ e faturamento anual até R$ 16 milhões, estabelecendo regras especiais para investidores-anjo e ambientes regulatórios experimentais (*sandboxes*)[454]. Pesquisas acadêmicas mostram que o MLS simplificou a abertura e a operação de empresas de tecnologia, ampliou a segurança jurídica para investidores e introduziu mecanismos de participação societária mais flexíveis[455]. Há, contudo, críticas significativas.

O MLS recebeu vetos importantes durante a sanção presidencial, como a retirada da possibilidade de que o investidor-anjo compensasse perdas com ganhos em outras startups. Essa mudança suprimiu incentivos tributários que muitos consideravam necessários para dinamizar o mercado de capital de risco. Outro veto impediu a flexibilização do acesso de startups ao mercado de capitais, limitando a captação de recursos via bolsa. Juristas também apontam inconsistências na definição de "investidor-anjo", o que pode gerar insegurança jurídica[456]. Trabalhos recentes

---

454 GOES, Severino, **Estímulo ao setor tecnológico é o principal objetivo da lei das startups**, Consultor Jurídico. Disponível em: <https://www.conjur.com.br/2021-jun-04/estimulo-setor-tecnologico-principal-objetivo-lei-startups/>. Acesso em: 19 nov. 2025.

455 GARBE, Hugo de Souza, **Os impactos do Marco Legal das Startups no ecossistema empreendedor nacional: uma análise dos efeitos do Marco Legal das Startups no desenvolvimento tecnológico e empresarial no Brasil**, Escola de Direito da FGV SP, São Paulo, 2025.

456 QUINELATO, João, **Marco Legal das Startups: avanços e retrocessos**, JOTA Jornalismo. Disponível em: <https://www.jota.info/coberturas-especiais/inova-e-acao/marco-legal-das-startups-avancos-e-retrocessos>. Acesso em: 19 nov. 2025; GERSTENBERER, Fatima Cristina Santoro; GERSTENBERER, Guilherme Santoro, Controvérsias acerca do Marco Legal das Startups no Brasil, 2021.

observam que, embora o MLS represente um avanço, ele não enfrentou a complexidade tributária nem o volume de burocracia que continuam a dificultar o crescimento das empresas emergentes[457].

As próximas seções oferecerão uma breve análise de alguns dos instrumentos, programas e iniciativas em vigor, voltados a promover o empreendedorismo inovador, a retenção e a repatriação de talentos, bem como do impacto que eles tiveram.

4.4.1 Programas de aceleração e inovação

O governo federal e instituições parceiras operam diversos programas de aceleração e inovação, mas eles funcionam de forma desconectada. Entre os maiores, está o InovAtiva Brasil, programa de aceleração gratuito que realiza um ciclo ao ano e seleciona até noventa startups alinhadas à política pública da Nova Indústria Brasil. O programa oferece conexão com investidores, mentorias individuais e coletivas, visibilidade em canais de comunicação e uma rede nacional de empreendedores e mentores. Além disso, os startups têm acesso a capacitação de alto nível, conexões estratégicas e mentorias especializadas, com foco na transformação digital da indústria[458].

Outra iniciativa recente é a plataforma Sebrae Startups, lançada em 2023. Em dois anos, ela se consolidou como a maior rede de apoio ao empreendedorismo inovador na América Latina, com 18 mil startups cadastradas e mais de 107 mil atendimentos em eventos, mentorias, consultorias e programas de internacionalização. A plataforma coordena 205 programas nacionais e sete metodologias próprias e tem direcionado mais de R$ 40 milhões para inovação em bioeconomia, transformação digital e saúde. Destaca-se também o Prêmio Sebrae Startups, que, em 2024, distribuiu R$ 950 mil em premiações e destinou 40% das vagas a startups lideradas por grupos minorizados[459].

---

457 GARBE, **Os impactos do Marco Legal das Startups no ecossistema empreendedor nacional**.

458 **InovAtiva Brasil**, InovAtiva. Disponível em: <https://www.inovativa.online/inovativa-brasil/>. Acesso em: 18 nov. 2025.

459 PAULINO, Isabela, **Sebrae Startups completa dois anos com 18 mil startups cadastradas e mais de 100 mil atendimentos realizados**, Anprotec. Disponível em: <https://anprotec.org.br/site/2025/06/sebrae-startups-completa-dois-anos-com-18-mil-startups-cadastradas-e-mais-de-100-mil-atendimentos-realizados/>. Acesso em: 18 nov. 2025.

O Conecta Startup Brasil é outro programa de inovação aberta que conecta startups em estágio inicial a grandes empresas e investidores. Com financiamento de até R$ 90 mil por startup, a iniciativa oferece capacitação, aporte financeiro, mentoria com mais de 400 profissionais e acompanhamento sistemático. Em sua segunda edição, mais de 250 mil pessoas foram impactadas, e o programa já registra mais de 2.500 inscrições de empreendedores e 800 mentores e embaixadores envolvidos[460].

Além desses, o país mantém programas específicos de aceleração regional, como Inova Amazônia, Catalisa ICT e Inova Startups, que canalizaram mais de R$ 40 milhões para áreas prioritárias[461]. Contudo, esses programas carecem de integração com uma estratégia nacional de soberania em IA; falta um mecanismo de coordenação que os oriente para os Facilitadores Essenciais da Soberania em IA (FESIAs).

4.4.2 Políticas de repatriação e retenção de talentos

No campo da *humanware*, o Brasil vem desenvolvendo iniciativas para mitigar a fuga de cérebros. O principal programa é o Conhecimento Brasil, lançado pelo CNPq em 2024. A iniciativa prevê investimento de R$ 604 milhões para contratar 599 projetos de pesquisadores brasileiros que residem em 34 países ou que concluíram doutorado ou pós-doutorado no exterior[462]. As bolsas, com valores de R$ 13 mil mensais para doutores e R$ 10 mil para mestres, incluem auxílio-instalação, deslocamento e seguro, além de investimento em equipamentos até R$ 400 mil por projeto[463]. O programa também destinou recursos para redes de cooperação internacional, com 640 projetos aprovados e mais de R$ 228 milhões em investimen-

460 **Home**, Conecta Startup Brasil. Disponível em: <https://conectastartupbrasil.org.br/>. Acesso em: 18 nov. 2025.

461 PAULINO, **Sebrae Startups completa dois anos com 18 mil startups cadastradas e mais de 100 mil atendimentos realizados**.

462 BRASIL [MCTI], **Conhecimento Brasil trará de volta cientistas que atuam em 34 países; veja o resultado final**, Conselho Nacional de Desenvolvimento Científico e Tecnológico. Disponível em: <https://www.gov.br/cnpq/pt-br/assuntos/noticias/cnpq-em-acao/conhecimento-brasil-trara-de-volta-ao-brasil-cientistas-que-atuam-em-34-paises-veja-o-resultado-final>. Acesso em: 18 nov. 2025.

463 *Ibid*.

tos[464]. Essa política demonstra que o governo pretende repatriar cientistas, evitar novas saídas e fortalecer redes de pesquisa.

Apesar do alcance, a iniciativa enfrenta críticas substanciais. Reportagem da *Folha de São Paulo* (reproduzida pelo *Jornal de Brasília*) destaca que pesquisadores brasileiros consideram a repatriação desejável, mas apontam que os R$ 1 bilhão previstos para o programa não resolvem problemas estruturais da ciência nacional, como salários defasados, sucateamento de laboratórios e carência de recursos para quem já trabalha no país[465].

Cientistas como Carlos Hotta argumentam que o programa peca no "momento e forma"; a verba, distribuída ao longo de quatro a cinco anos, deveria ser acompanhada de investimentos muito maiores nas instituições existentes[466]. Outros especialistas observam que as bolsas e condições oferecidas aos repatriados podem superar a remuneração de docentes permanentes das universidades federais, evidenciando uma má alocação de recursos e a ausência de políticas robustas de financiamento de pesquisa[467]. Essas críticas mostram que, embora o Conhecimento Brasil seja positivo, ele é insuficiente se não houver uma política que enfrente a precarização das instituições de ensino e pesquisa.

A retenção da fuga de talentos exige um avanço que vá além de programas de repatriação pontual e seja capaz de construir uma conexão entre ecossistema científico, inovação e empreendedorismo, capaz de oferecer previsibilidade, carreira e infraestrutura. É necessário considerar que a retenção de talentos passa também pela possibilidade de atração e manutenção de especialistas dentro do próprio Estado brasileiro. Nesse sentido, parece essencial proporcionar condições de trabalho que não sejam completamente desconectadas das condições ofertadas pelo mercado. No campo de tecnologias digitais, destaca-se o caso dos Analistas de Tecnologia da Informação (ATI), carreira de Estado vinculada ao Ministério da Gestão

464 *Ibid*.

465 WATANABE, Phillippe; BOTTALLO, Ana, **Programa de R$ 1 bilhão para repatriar cientistas é criticado por pesquisadores**, Jornal de Brasília. Disponível em: <https://jornaldebrasilia.com.br/noticias/politica-e-poder/programa-de-r-1-bilhao-para-repatriar-cientistas-e-criticado-por-pesquisadores/>. Acesso em: 18 nov. 2025.

466 *Ibid*.

467 *Ibid*.

e da Inovação. Apesar de serem responsáveis por serviços considerados críticos, como gestão de infraestruturas digitais federais, arquiteturas de interoperabilidade, governança de dados e segurança cibernética, os ATIs recebem uma remuneração significativamente inferior àquela oferecida pelo mercado privado de tecnologia[468].

A Associação Nacional dos Analistas de TI demonstrou em pesquisa recente que mais da metade dos aprovados no concurso de 2024 não chegaram a tomar posse no cargo devido à grande diferença salarial em relação ao mercado privado.[469] A definição de um plano robusto de valorização e progressão funcional deveria ser uma condição essencial para garantir a capacidade do Estado de implementar políticas de transformação digital, proteger infraestruturas críticas e manter a autonomia tecnológica em áreas sensíveis.

Por fim, cabe ressaltar que a competição salarial internacional tem se tornado um vetor central da fuga de talentos em tecnologia em países em desenvolvimento, incluindo o Brasil. Estudos sobre dinâmicas globais de trabalho remoto mostram que empresas estrangeiras tendem a recrutar profissionais altamente qualificados em países de renda média oferecendo salários indexados a moedas fortes, criando uma assimetria crescente entre remunerações locais e internacionais.[470] O mercado global de trabalho remoto é profundamente polarizado, com trabalhadores do Sul Global competindo por remunerações significativamente menores do que seus pares em países desenvolvidos, pressionando salários domésticos e incentivando a migração digital.[471] No caso brasileiro, trabalhos recentes analisando teletrabalho e remuneração sugerem que o país possui grande oferta de profissionais qualificados em áreas digitalizáveis, mas enfrenta um mercado doméstico incapaz de competir com ofertas internacionais, favorecendo a migração digital de talentos.

---

468 ANATI, **NOTA OFICIAL DA ANATI - Evasão recorde de futuros Analistas em TI aprovados no Concurso Público Nacional Unificado (CPNU)**, Associação Nacional dos Analistas em TI - ANATI. Disponível em: <https://anati.org.br/noticias/nota-oficial-da-anati-evasao-recorde-atis-cpnu>. Acesso em: 25 nov. 2025.

469 *Ibid*.

470 BRAESEMANN, Fabian *et al*, The global polarisation of remote work, **PLOS ONE**, v. 17, n. 10, p. e0274630, 2022.

471 *Ibid*.

Somado a isso, estudos do Banco Mundial indicam que a expansão da digitalização durante a pandemia reorganizou cadeias globais de valor, criando um ambiente no qual empresas estrangeiras extraem mão de obra especializada em países emergentes sem necessidade de migração física e intensificando a drenagem de talentos.[472] Em conjunto, essas evidências sugerem que o Brasil enfrenta uma concorrência estrutural: salários internacionais em moeda forte capturam seus profissionais mais preparados, pressionando empresas locais e reduzindo a capacidade de retenção de talentos, o que dificulta ainda mais o desenvolvimento de indústrias digitais nacionais.[473]

4.4.3 Avaliação geral

O panorama revela que o Brasil já dispõe de pilares importantes para um subsistema de inovação baseada em empreendedorismo e startups: um marco jurídico (MLS), programas de aceleração consolidados (InovAtiva Brasil, Sebrae Startups, Conecta Startup Brasil) e iniciativas de repatriação de talentos (Conhecimento Brasil). Entretanto, esses instrumentos atuam de modo fragmentado e carecem de coordenação com os FESIAs.

As críticas ao MLS e ao Conhecimento Brasil indicam que as medidas existentes não enfrentam a pesada carga tributária, a burocracia excessiva, as restrições de acesso ao mercado de capitais nem as condições estruturais da pesquisa científica[474]. É, portanto, necessário redirecionar e integrar esses instrumentos dentro de um sistema de governança e de incentivos que oriente os esforços de fomento, aceleração e repatriação para a consolidação do *humanware* e dos demais FESIAs.

Ademais, o componente de startups e empreendedorismo configura, tão somente, um dos elementos de uma mirada sistêmica sobre a inovação, com o potencial de fixar profissionais de alta qualificação, mas com al-

472 World Bank Document.

473 COSTA, João Erick Alexandre Barbosa *et al*, Wage returns from telework in Brazil: an analysis based on the concept of potential telework, **Revista Brasileira de Economia de Empresas**, v. 24, n. 2, 2024.

474 GERSTENBERER; GERSTENBERER, Controvérsias acerca do Marco Legal das Startups no Brasil; WATANABE; BOTTALLO, **Programa de R$ 1 bilhão para repatriar cientistas é criticado por pesquisadores**.

cance limitado. As medidas indicadas nesta seção podem contribuir para o fortalecimento do ambiente empreendedor no país e, em consequência, reforçar a fixação e repatriação de profissionais de alta qualificação. No entanto, é importante notar que o problema da "fuga de cérebros" é complexo e multifacetado e não há um único pacote de políticas públicas que se possa prescrever com total garantia de sucesso. O desenvolvimento socioeconômico pela via da inovação envolve, conforme já explicitado anteriormente, a interação de uma complexa rede de instituições e atores, incluindo políticas horizontais e verticais, diretas e indiretas.

5 Caminhos e oportunidades para um Sistema Nacional de Soberania Digital

A consolidação de uma estratégia nacional de soberania digital requer mais do que diagnósticos precisos e boas intenções políticas: exige coordenação, coerência institucional e compromisso de longo prazo. Assim, parece importante pontuar que a soberania digital não é um ponto de chegada, mas um processo contínuo de construção de capacidades estatais, regulatórias, tecnológicas, humanas e econômicas, orientadas à autonomia e à proteção do interesse público em um ambiente global profundamente assimétrico.

Nesse contexto, propõe-se que seja estabelecido um Sistema Nacional de Soberania Digital (SNSD), que deve ser compreendido como um projeto político-jurídico de Estado, e não apenas de governo, que articula instrumentos regulatórios, capacidades técnicas e mecanismos econômicos em torno de uma estratégia voltada a alcançar o objetivo constitucional da autonomia tecnológica, idealmente numa política de Estado e não numa política sazonal de governos que mudam a cada quatro ou oito anos.

Como destacado na seção 4.2, o Brasil já detém vários ativos cruciais, não somente em termos de recursos naturais, informacionais e humanos, mas também em termos de capacidade institucional e regulatória que pode ser explorada de maneira mais eficiente e efetiva para se alcançar a soberania digital.

Portanto, a construção de um Sistema Nacional de Soberania Digital não exige começar do zero, mas pode fortalecer e articular estruturas já existentes no Estado brasileiro, como o SISP e o CITDigital. O SISP oferece uma base operacional e institucional consolidada para a gestão, integração e padronização de recursos de tecnologia da informação no governo federal, enquanto o CITDigital atua como instância estratégica e multissetorial, capaz de formular políticas amplas que envolvem segurança, inovação, economia digital e governança de dados.

O aproveitamento do SINAPAD e sua articulação com um futuro SNSD permitiria traçar um caminho institucional para o desenvolvimento de sistemas de IA autônomos. Ao permitir que modelos sejam treinados e operados em infraestrutura nacional, em pleno respeito da legislação

pátria e com garantias de segurança, o país daria um passo importante para reduzir sua dependência de tecnologias estrangeiras, desenvolver capacidades internas e criar estímulos para que sua indústria de software, hardware e semicondutores possa avançar na direção de maior autonomia. A integração entre governança estratégica e infraestrutura operacional revela-se, portanto, como elemento indispensável para viabilizar um projeto nacional de soberania digital que responda às demandas científicas, econômicas e geopolíticas do Brasil.

Alavancando a combinação das capacidades operacionais, estratégicas e infraestruturais, podem ser criadas as condições propícias para que o Brasil avance rumo a uma soberania digital efetiva.

Como ressaltado na introdução e no primeiro capítulo deste livro, a soberania digital deve ser entendida como a capacidade de entender, desenvolver e regular sistemas digitais para alcançar a autonomia, a autodeterminação e o controle sobre tais sistemas. Essa soberania, contudo, não se realiza pela construção de uma autarquia digital, mesmo supondo que tal opção fosse possível, mas pela criação de um ecossistema institucional, tecnológico e econômico capaz de regular, induzir e coordenar ações públicas e privadas orientadas à preservação da autonomia tecnológica. Nesse sentido, o SNSD deveria operar em três frentes complementares.

A primeira frente consiste no fortalecimento das capacidades digitais soberanas do Estado brasileiro, com ênfase no aprimoramento de sua infraestrutura tecnológica e no fortalecimento dos elementos que definimos como Facilitadores Essenciais da Soberania em Inteligência Artificial (FESIA). A segunda diz respeito à coordenação entre as instituições reguladoras que exercem controle sobre cada um desses elementos, buscando evitar sobreposições, lacunas e assimetrias de atuação.

Por fim, a terceira frente refere-se à criação de uma percepção situacional (*situational awareness*) voltada ao monitoramento contínuo de riscos e oportunidades, tanto no plano nacional quanto internacional. A integração dessas três dimensões deve permitir a consolidação de um espaço digital brasileiro robusto, seguro e interoperável, sustentado por capacidades estatais e mecanismos de governança aptos a garantir a efetividade dos direitos fundamentais, a competitividade econômica e a autonomia tecnológica do país. A seguir, propõe-se um conjunto de medidas institucionais

destinadas a estruturar e operacionalizar o Sistema Nacional de Soberania Digital (SNSD).

5.1 O Conselho Nacional de Soberania Digital

Para viabilizar uma proposta abrangente e duradoura na forma do SNSD, é imperativo um arcabouço político-institucional capaz de alicerçar, desenvolver e conduzir suas iniciativas. Nesse sentido, o primeiro eixo institucional da proposta é o Conselho Nacional de Soberania Digital (CNSD), órgão de alto nível político e técnico, concebido como espaço de coordenação e deliberação estratégica. Sua presidência pela Casa Civil ou pela Presidência da República poderia refletir a natureza transversal da agenda digital e a necessidade de articulação interministerial. O CNSD reuniria representantes da administração pública, além de membros da comunidade científica, da sociedade civil e do setor produtivo. Essa composição plural não se justifica apenas pela diversidade de interesses envolvidos, mas pela própria natureza policêntrica da governança digital contemporânea.

O CNSD poderia ser estabelecido de forma relativamente simples, aproveitando a estrutura já existente do Comitê Interministerial sobre Transformação Digital (CITDigital) e seu Comitê Consultivo. Entre suas atribuições centrais, o "Conselho" deveria definir prioridades estratégicas, planos plurianuais de soberania digital, alocar recursos do Fundo Nacional de Soberania Digital (FNSD) e elaborar, junto ao Itamaraty, notas necessárias para informar a tomada de decisões estratégicas sobre assuntos nacionais e internacionais, particularmente relacionados com os FESIA.

Além disso, caberia ao CNSD arbitrar conflitos federativos ou interministeriais, garantindo coerência e previsibilidade regulatória. Na medida em que amadurecesse, o Conselho poderia evoluir para integrar um Ministério de Assuntos Digitais, com competência transversal, consolidando a governança de temas digitais hoje dispersos entre diferentes órgãos. Essa trajetória institucional reproduz, em alguma medida, o modelo de maturação observado em políticas industriais e científicas de sucesso[475].

475 **Embedded Autonomy | Princeton University Press**.

5.2 A Secretaria Executiva Técnica de Soberania Digital

A SET-SoberaniaDigital configuraria o braço operacional e técnico do sistema, incumbida da execução das diretrizes emanadas pelo CNSD. Sua missão seria reduzir a fragmentação institucional hoje observada entre órgãos que tratam de segurança cibernética, compras públicas, inovação e regulação de dados. Com corpo técnico multidisciplinar, composto por especialistas em planejamento, direito regulatório, P&D e segurança digital, a Secretaria teria poder normativo secundário, apto a editar portarias, guias técnicos e protocolos de interoperabilidade, em consonância com o artigo 84, inciso VI, da Constituição Federal.

A SET-Soberania atuaria também como um centro de expertise, produzindo indicadores, avaliando políticas e coordenando planos de ação interinstitucionais. Sua estrutura deve ser concebida para garantir flexibilidade administrativa e capacidade de resposta rápida às transformações tecnológicas. Essa centralidade técnica é condição para a efetividade da política, pois a soberania digital não é apenas um problema normativo, mas um problema de capacidade estatal de implementação e continuidade.

A SET-SoberaniaDigital deveria também evoluir para ser integrada a um Ministério ou a uma Agência para Autonomia Tecnológica, que poderia ser criada *ex novo* ou, preferencialmente, com o aproveitamento de entidade da administração pública já porventura existente. Por exemplo, a Secretaria de Ciência e Tecnologia para a Transformação Digital do Ministério da Ciência, Tecnologia e Inovação já possui responsabilidade pela formulação e coordenação de políticas públicas voltadas à transformação digital, bem como pela promoção da pesquisa e do desenvolvimento de tecnologias digitais emergentes, conforme estabelecido no Decreto nº 11.493/2023.

5.3 O Fundo Nacional de Soberania Digital e o Mecanismo de Compras Públicas Estratégicas

Nenhum projeto de soberania digital é viável sem sustentação financeira estável e de longo prazo. O Fundo Nacional de Soberania Digital (FNSD) deve, portanto, funcionar como instrumento central de financiamento, articulando recursos públicos, privados e multilaterais. Inspi-

rado no Fundo Nacional de Desenvolvimento Científico e Tecnológico (FNDCT), o FNSD poderia integrar receitas oriundas do FUST, de linhas de crédito do BNDES e de aportes orçamentários diretos. A previsibilidade orçamentária mostra-se indispensável para a construção de capacidades estatais e empresariais em tecnologias críticas, como extração e o processamento de terras raras, desenvolvimento de semicondutores, criação e treinamento de modelos de linguagem, e computação em nuvem.

O FNSD deveria financiar tanto projetos estratégicos de infraestrutura soberana (como redes federadas de dados públicos e plataformas nacionais de acesso a dados públicos) quanto programas de inovação e formação de competências digitais. Nesse ponto, o Estado deve exercer papel ativo na orientação de investimentos, estimulando a inovação por meio de políticas públicas orientadas por missões[476]. Assim, o FNSD deve ser concebido como motor de uma política industrial digital brasileira que simultaneamente possibilita autonomia estratégica e capacidade de projeção nacional e regional.

Para complementar o FNSD, deveria ser instituído um mecanismo de Compras Públicas Estratégicas para a Soberania Digital (MCP-SD) como vetor econômico essencial. O Estado é o maior comprador de tecnologia do país, e seu poder de compra deve ser utilizado como instrumento de política tecnológica e de desenvolvimento. Ao estabelecer critérios de soberania digital nos editais, priorizando soluções interoperáveis, auditáveis e desenvolvidas no país, o MCP-SD pode criar incentivos econômicos diretos para a produção tecnológica nacional. Como ressaltado, a literatura econômica e as experiências estrangeiras demonstram que o *procurement* público estratégico é um dos instrumentos mais eficazes de desenvolvimento tecnológico, especialmente em setores de alto risco e alta complexidade.

A centralização e padronização das compras públicas digitais também permitem ganhos de escala e de segurança jurídica. A SET-Soberania poderia emitir diretrizes estabelecendo critérios mínimos de soberania, segurança e conformidade com os padrões de interoperabilidade de dados, idealmente definidos pela ANPD e pelo MGI. Tais mecanismos devem ser entendidos como expressão concreta do princípio da eficiência administrativa (art. 37, *caput*, CF) e do dever de promoção do desenvolvimento nacional (art. 3º, II, CF).

476 MAZZUCATO, Mariana, **The Value of Everything**, [s.l.: s.n.], 2019.

5.4 A Avaliação de Autonomia Tecnológica

Por fim, recomenda-se também a criação de uma Avaliação de Autonomia Tecnológica (AAT), concebida como instrumento de certificação de *compliance* com regulamentação dos FESIA, que poderia ser integrado imediatamente no Autodiagnóstico do SISP. Inspirando-se na experiência europeia com o *Cloud Sovereignty Framework (CSF) e com o sistema SEAL – Sovereignty Effectiveness Assurance Level*, a Avaliação de Autonomia Tecnológica deverá adotar lógica semelhante àquela implementada pela Comissão Europeia, que define níveis graduais de aderência às várias dimensões da soberania digital, particularmente no que diz respeito à cumprimento da regulamentação em vigor.

Assim como o CSF permite demonstrar *compliance* com obrigações em áreas particularmente relevantes para soberania digital, a AAT serviria como instrumento nacional de mensuração e transparência sobre o cumprimento de obrigações legislativas, tornando-se um complemento valioso para as estratégias e políticas industriais voltadas à promoção da autonomia tecnológica. Como consequência, o objetivo da ATS seria permitir que provedores tecnológicos possam participar de licitações públicas, demonstrando, de forma objetiva, seu grau de conformidade com as obrigações definidas pelo Estado brasileiro.

Propõe-se, portanto, a criação de um *framework* destinado a orientar a participação de fornecedores tecnológicos em processos de contratação pública, com o objetivo de assegurar que a administração pública disponha de serviços tecnologicamente autônomos, capazes e garantir controle operacional, proteção de dados e segurança da informação, por meio dos seguintes critérios:[477]

(i) Independência Jurídica e Estrutural: o critério da independência jurídica e estrutural diz respeito ao grau em que um fornecedor está livre de coerção ou interferência por parte de ordenamentos estrangeiros capazes de impor obrigações de acesso, vigilância ou interrupção de serviços. Ela avalia não apenas a nacionalidade

477 Os critérios são destilados a partir do valioso trabalho desenvolvido pelos membros da EuroStack Industry Initiative. A Proposed Framework for a "Buy European" Regulation of Strategic Digital Procurement.

formal da empresa, mas a profundidade da sua cadeia societária, o local de incorporação e as legislações às quais seus controladores se submetem. O fornecedor deverá comprovar, mediante documentação abrangente sobre sua cadeia societária e manifestação jurídica formal, que não se encontra subordinado à incidência coercitiva de ordenamentos estrangeiros capazes de exigir acesso a informações governamentais ou influenciar a continuidade do serviço. A aferição desse requisito ocorre como etapa inicial e excludente, de modo que qualquer empresa sujeita a tais interferências externas será automaticamente afastada da disputa, antes mesmo da análise técnica ou econômica.

(ii) Robustez da Cadeia de Suprimentos: a robustez da cadeia de suprimentos analisa o nível de dependência do fornecedor em relação a componentes críticos – de hardware ou software – provenientes de jurisdições sujeitas a instabilidade regulatória, geopolítica ou econômica. Trata-se de avaliar a capacidade da empresa de manter continuidade operacional diante de interrupções externas, sanções, falhas de fornecimento ou conflitos internacionais. O fornecedor deverá apresentar plano formal e auditável destinado a reduzir a dependência de componentes críticos, tanto de hardware quanto de software. O documento deve contemplar medidas de contingência voltadas a assegurar a continuidade operacional diante de sanções, interrupções de fornecimento ou outros eventos geopolíticos adversos.

(iii) Localização de Categorias Específicas de Dados: a localização de dados sensíveis mede a extensão em que informações estratégicas, criticamente relevantes ou classificadas permanecem armazenadas, tratadas e administradas dentro das fronteiras nacionais. Essa dimensão considera tanto a infraestrutura física quanto a lógica de gestão e os mecanismos de acesso, incluindo metadados e a camada de comando dos sistemas. Trata-se de medir quão completa é a proteção territorial e quão reduzida é a exposição às jurisdições estrangeiras.

(iv) Autonomia Operacional da Equipe Técnica: o critério avalia até que ponto os profissionais que administram sistemas críticos possuem acessos privilegiados ou operam infraestruturas sensíveis estão juridicamente, fisicamente e funcionalmente vinculados ao território nacional. Ela envolve residência, contratação por pessoa jurídica nacional e exercício das funções a partir do país. É fundamental que haja exigência de que os profissionais com prerrogativas de administração de sistemas, acesso privilegiado a dados ou atuação direta na operação da infraestrutura de dados devam residir em território nacional e ser contratados por empresa estabelecida e com operação a partir do território nacional.

(v) Interoperabilidade e Portabilidade: a interoperabilidade e a portabilidade analisam a capacidade de a solução tecnológica dialogar com outros sistemas, migrar para diferentes fornecedores e evitar dependências rígidas ou aprisionamento tecnológico. Essa dimensão observa o uso de padrões abertos, APIs documentadas e componentes de código aberto nas partes essenciais da solução. Em essência, mede-se o quanto o sistema preserva liberdade de escolha e reduz assimetrias de poder entre contratante e fornecedor. No entanto, soluções que adotem padrões abertos devem ser priorizadas e o *framework* deve restringir a participação de soluções de padrões fechados.

(vi) Arquiteturas Abertas, Transparentes e Auditáveis: esse critério avalia a transparência técnica da solução e a possibilidade de realizar auditorias independentes para verificar segurança, integridade, ausência de portas traseiras e alinhamento com o interesse público. Ela contempla mecanismos como acesso controlado ao código-fonte, inspeções conduzidas por entidades nacionais ou disponibilização de documentação detalhada sobre a lógica interna dos sistemas. Fornecedores que não ofereçam espaços para auditorias e exames de códigos devem ser também impedidos de acessar os mecanismos propostos.

(vii) Reversibilidade e Continuidade: o critério de reversibilidade e continuidade mede a capacidade de a administração pública as-

> sumir ou transferir a operação da solução para outro fornecedor em caso de falha, interrupção ou encerramento contratual. Ela se baseia na existência de documentação completa, automação de processos, mecanismos de reinstalação e práticas que permitam a independência operacional. Assim, trata-se de medir o quanto o Estado mantém capacidade real de continuidade sem dependências insuperáveis.

Para assegurar plena compatibilidade com o Acordo sobre Compras Governamentais da Organização Mundial do Comércio – acordo cuja adesão o Brasil atualmente negocia –, a implementação da AAT deve amparar-se no artigo 3 desse tratado, que autoriza medidas indispensáveis à proteção de interesses essenciais de segurança. Essa base jurídica permite exigir requisitos rigorosos de autonomia tecnológica sem violar o princípio de não discriminação, garantindo que a proteção de infraestruturas e dados sensíveis permaneça dentro dos limites legítimos previstos pelo regime comercial internacional. O modelo proposto permite avaliar neutralmente empresas nacionais e estrangeiras, penalizando a exposição ou dependência que coloquem em risco a soberania nacional, em termos técnicos e jurídicos mensuráveis.

Em virtude disso, a avaliação funcionaria como um indicador público de conformidade, com critérios instrumentais para se alcançar a soberania tecnológica, como segurança da informação, proteção de dados e interoperabilidade com infraestruturas digitais nacionais, a serem definidos pela SET-Soberania, juntamente com as autoridades reguladoras competentes. Sua adoção permitirá classificar fornecedores e soluções tecnológicas segundo níveis graduais de aderência aos princípios de soberania digital, estimulando a competição por qualidade e segurança sendo, portanto, extremamente útil também para informar e orientar as escolhas dos consumidores.

Além de se tornar requisito a ser utilizado em editais de licitações, o selo também poderia ser elegível para benefícios fiscais, como créditos tributários e deduções em programas de inovação, dialogando com outros elementos de soberania digital. Dessa forma, a AAT não apenas reforçaria a compra do Estado como vetor de desenvolvimento tecnológico, mas criaria um arcabouço de incentivos positivos capaz de colaborar com o alinhamento de objetivos industriais, regulatórios e de segurança nacional em torno da construção de uma economia digital soberana.

5.5 A utilização estratégica das capacidades regulatórias já existentes

Cabe pontuar que, para alcançar a soberania digital, o Brasil não precisa necessariamente reinventar todo o aparato institucional: é necessário começar por usar estrategicamente o que já possui. As instituições e instrumentos legais existentes já oferecem base normativa suficiente para impulsionar a transição rumo à autonomia digital, desde que haja coordenação e vontade política.

Em primeiro lugar, o Conselho Administrativo de Defesa Econômica (CADE) deveria revisitar sua jurisprudência a fim de efetivamente implementar o artigo 9º do Marco Civil da Internet (Lei n.º 12.965/2014) e o artigo 9º do Decreto n.º 8.771/2016, que proíbem práticas de *zero rating* que, além de ter consequências nefastas pela inovação e concorrência, prejudicam seriamente a execução de qualquer plano de IA, como destacado anteriormente. A proibição das práticas de *zero rating*, portanto, nos parece essencial para evitar a concentração de poder de mercado e de dados em poucas empresas estrangeiras de IA. O princípio da neutralidade de rede, nesse contexto, deve ser reafirmado como princípio instrumental para alcançar a concorrência, a inovação e a diversidade na IA.

Em segundo lugar, o CADE deveria utilizar o arcabouço jurídico existente, especialmente após as eventuais alterações que podem ser introduzidas pelo Projeto de Lei nº 4675/2025, para facilitar o acesso ao mercado e isonomia de tratamento entre os agentes econômicos que atuam em cima da infraestrutura de orquestradores de ecossistemas digitais.[478] De forma complementar, o CADE deveria editar e fiscalizar exigências comuns de transparência para facilitar escolhas livres e informadas nos ecossistemas digitais, e analisar de forma sistemática e aprofundada as concentrações econômicas que envolvem os orquestradores desses ecossistemas.[479]

Em terceiro lugar, a Agência Nacional de Proteção de Dados (ANPD) deve exercer plenamente sua competência prevista no artigo 40 da LGPD (Lei nº 13.709/2018), definindo padrões de interoperabilidade e portabilida-

478 BELLI; ZINGALES. **Interoperability to Foster Open Digital Ecosystems in the BRICS Countries.**

479 ZINGALES, Nicolo; RENZETTI, Bruno, Digital Platform Ecosystems and Conglomerate Mergers: A Review of the Brazilian Experience, **World Competition**, v. 45, n. 4, 2022.

de de dados. Tais padrões são condições estruturantes para a livre circulação de dados entre plataformas, prevenindo o chamado *lock-in* tecnológico e permitindo a efetivação do direito fundamental à autodeterminação informativa. A interoperabilidade, além de ser instrumento de proteção de direitos, é elemento essencial de uma economia de dados aberta e soberana.

Por seu turno, o Ministério da Gestão e da Inovação em Serviços Públicos (MGI) deve definir padrões de interoperabilidade e segurança para os dados públicos, articulando-se à ANPD para assegurar coesão normativa e técnica. O SERPRO e a DATAPREV e os PRODE, por sua vez, devem ser reposicionados como plataformas públicas de intercâmbio de dados, nos modelos dos *data exchanges* chineses, operando sob as condições de acesso e segurança definidas por ANPD e MGI. A reorientação dessas empresas públicas para funções de infraestrutura de dados soberana representa passo fundamental na construção de um espaço digital estatal interoperável e confiável. Neste contexto, nos parece que o Tribunal de Contas da União (TCU) tenha um papel particularmente relevante, devendo atuar como instância de controle e monitoramento da implementação das medidas propostas, definindo prazos, avaliando indicadores e verificando a eficiência na utilização dos recursos do FNSD e na execução das diretrizes do CNSD.

Por fim, cabe frisar a necessidade de reinterpretar de forma integrada instrumentos jurídicos e econômicos tradicionalmente tratados de forma isolada. Nesse sentido, nossa pesquisa demonstra que a reforma tributária abre espaço para que a tributação seja compreendida como eixo regulatório central na promoção da soberania digital, capaz de enfrentar assimetrias de poder informacional e de corrigir desequilíbrios estruturais produzidos pela economia de dados.[480] A tributação deve deixar de ocupar posição meramente arrecadatória e assumir papel ativo na regulação de modelos de negócio que se baseiam na exploração intensiva de dados pessoais e não pessoais. Assim, instrumentos fiscais podem ser mobilizados para desencorajar práticas extrativistas, reduzir externalidades negativas associadas à concentração de dados e valorizar modelos que promovam transparência, segurança da informação e respeito à autodeterminação informativa em suas dimensões individual e coletiva.

480 BELLI *et al*, Proteção de dados, tributação de dados e equidade de dados: equilíbrio entre valores, riscos e obrigações.

Como evidenciado em pesquisas específicas sobre tributação e equidade de dados, o Brasil não dispõe de políticas tributárias que atuem como indutoras de boas práticas de governança informacional.[481] O atual desenho tributário não alcança dados brutos, tampouco os direitos de exploração econômica desses dados; concentra-se, de forma limitada, na tributação de serviços digitais prestados ao usuário final. Essa estrutura contradiz princípios consolidados do direito tributário internacional, especialmente os critérios de nexo e criação de valor, além de facilitar a erosão da base tributária e o deslocamento artificial de lucros para jurisdições mais favoráveis. Ao ignorar o papel central dos dados como ativos econômicos, o sistema tributário brasileiro acaba por reforçar a lógica de exploração unilateral por plataformas que se apropriam de externalidades positivas geradas pela sociedade brasileira, ao mesmo tempo que socializam os custos associados à perda de privacidade, insegurança informacional, opacidade algorítmica e concentração de poder econômico.

Reformular o papel da tributação implica reconhecer que ela pode e deve funcionar como mecanismo regulatório orientado à proteção de direitos fundamentais e à promoção de soberania digital. A recente reforma tributária pode ser alavancada para estruturar uma tributação destinada a desincentivar práticas de coleta excessiva, e tratamento opaco e inseguro de dados, e incentivar modelos de negócio que adotem governança responsável, privacidade por padrão, segurança robusta e demonstrem o compromisso na redução de externalidades negativas.[482]

Ao utilizar a tributação como forma de alinhar incentivos econômicos ao interesse público, o Estado brasileiro pode fortalecer sua autonomia tecnológica, aumentar a resiliência institucional e reequilibrar as relações entre cidadãos, empresas e plataformas globais. Dessa forma, a política tributária deixa de ser instrumento neutro e passa a integrar uma estratégia mais ampla de proteção da autodeterminação informativa e de consolidação da soberania digital do país.

Além disso, é importante ressaltar também que, dada a dinâmica global da internet, é indispensável fortalecer mecanismos de coordenação institucional que articulem as dimensões geopolíticas da soberania digital.

481 *Ibid.*

482 *Ibid.*

Para isso, o Brasil poderia fomentar maior cooperação entre o Itamaraty, MCTI, MGI e MME (nas frentes de energia e minerais críticos), tanto para equacionar tensões geopolíticas quanto para coordenar a internacionalização de cadeias produtivas e parcerias tecnológicas. Essa integração reforçaria a capacidade do país de projetar influência internacional sem renunciar à busca por autonomia estratégica, criando condições para que políticas internas de regulação, concorrência, proteção de dados e desenvolvimento tecnológico possam operar de forma mais eficaz e convergente.

6 Conclusão: autonomia tecnológica como projeto de Estado

A soberania digital é, em última instância, um projeto de autonomia tecnológica e democracia informacional. Trata-se, assim, de garantir que o Brasil tenha condições de definir suas próprias regras, proteger seus dados e desenvolver suas tecnologias, sem subordinação estrutural a interesses externos. Como demonstrado, tal desiderato não se alcança pela via da autarquia digital, mas pela construção de capacidade de escolha: pela possibilidade de decidir, de forma soberana e informada, quais tecnologias adotar, como utilizá-las e em que condições compartilhar dados e conhecimento.

O Sistema Nacional de Soberania Digital, ao articular instituições, normas e instrumentos financeiros, oferece um caminho concreto para a realização desse ideal. Ele materializa, em linguagem institucional, o princípio da soberania previsto no artigo 1º, inciso I, da Constituição, e o dever de promoção do desenvolvimento nacional (art. 3º, II). Mais do que um programa de governo, o SNSD representa a institucionalização de um novo paradigma de ação estatal, em que a tecnologia é compreendida não apenas como infraestrutura, mas como expressão do poder público e instrumento de emancipação nacional.

Um elemento essencial para o sucesso de tal sistema é a coordenação do Estado. Nenhum sistema nacional de soberania digital pode prosperar em meio à fragmentação institucional. Para tanto, o Estado deve recuperar sua capacidade de planejar, coordenar e induzir, superando o modelo de regulação reativa e setorial. Isso implica reconhecer que a soberania digital é, simultaneamente, uma questão de direito, política econômica e, também, de ciência de dados. Nesse sentido, as fronteiras tradicionais entre regulação, inovação e segurança precisam ser redesenhadas em torno de uma governança multissetorial e multinível.

Nesse contexto, a necessidade de formulação de uma nova Estratégia Brasileira para a Transformação Digital (E-Digital), cujo ciclo atual expira em 2026, deve ser compreendida como oportunidade estratégica para reposicionar a autonomia tecnológica como elemento central da visão de fu-

turo do país. A transformação digital não pode ser limitada à digitalização de serviços públicos ou ao incentivo à adoção de tecnologias emergentes; esta deve incorporar, de forma explícita, objetivos de soberania digital, desenvolvimento de capacidades nacionais, redução de dependências estruturais e fortalecimento da resiliência de infraestruturas críticas.

Assim, a atualização da E-Digital pode se revelar uma oportunidade extremamente valiosa para redefinir o papel orientador e estruturante da política tecnológica brasileira, de modo a consolidar a autonomia informacional, infraestrutural e lógica como princípios fundamentais da atuação estatal no ambiente digital. Nesse sentido, a nova estratégia deve funcionar como um eixo central articulador, concebida como uma estratégia guarda-chuva, que não apenas integre políticas e planos já existentes, mas que desempenhe função de coordenação e convergência entre atores, setores e agendas.

O objetivo não é, pois, a simples harmonização técnica de iniciativas dispersas, mas a construção de uma visão unificada que conecte efetivamente os múltiplos agentes envolvidos na transformação digital do país. Como detectado pelo presente estudo, isso implica criar mecanismos institucionais que fomentem comunicação, coordenação e colaboração entre órgãos governamentais, setor privado, academia e sociedade civil, assegurando participação ampla e governança efetiva.

A coordenação interinstitucional e intersetorial permite não apenas reduzir redundâncias e conflitos normativos, mas também alinhar incentivos entre políticas públicas, conectando proteção de dados, política industrial, educação e defesa nacional. Para o sucesso dessa abordagem, portanto, é essencial a presença de burocracias profissionais capazes de formular e implementar políticas complexas. Dessa forma, a nova E-Digital poderá servir como plataforma comum de ação, capaz de orientar investimentos, regular práticas, promover interoperabilidade e impulsionar a inovação nacional em alinhamento com os interesses estratégicos do Brasil.

Nesse sentido, entende-se que o SNSD não deva ser considerado apenas um arranjo formal, mas um mecanismo efetivo de governança, com poder decisório, capacidade técnica e estabilidade política. Isso exige arcabouço jurídico claro, recursos garantidos e mecanismos de *accountability* permanentes. A criação de instrumentos de planejamento plurianual, como os Planos Nacionais de Soberania Digital, é indispensável para alinhar as políticas setoriais em um horizonte de longo prazo.

A consolidação da soberania digital brasileira também depende de sua inserção estratégica no cenário internacional. Num mundo em que a infraestrutura informacional é globalmente interdependente, nenhuma soberania pode ser exercida de forma isolada.

O Brasil precisa afirmar sua autonomia não contra o sistema internacional, mas, dentro dele, ampliando sua voz nos espaços de governança digital e fortalecendo alianças políticas e tecnológicas com países do Sul Global. A cooperação Sul-Sul, a participação ativa em fóruns multilaterais e o desenvolvimento de padrões técnicos abertos, de base pública e interoperável, são caminhos para ampliar a margem de escolha e reduzir dependências críticas.

Assim, uma concepção cooperativa e desenvolvimentista de soberania digital se torna também um poderoso instrumento de política externa, capaz de reposicionar o país como protagonista de uma governança digital global participativa e colaborativa. O Brasil tem a oportunidade de reconquistar sua posição de liderança global, ao promover uma visão positiva de soberania digital, fundamentada no desenvolvimento sustentável, na inovação descentralizada, na livre concorrência, no uso da tecnologia para o empoderamento dos cidadãos e na criação de sistemas tecnológicos autônomos, porém interoperáveis.

É igualmente necessário compreender a soberania digital como um processo contínuo de construção institucional, e não como um estado permanente. A autonomia tecnológica se conquista e se renova a cada ciclo de inovação, regulação e aprendizado social. Isso requer *situational awareness* e capacidade adaptativa, caracterizada por instituições que devem aprender, se adaptar e evoluir constantemente. Assim sendo, o Brasil precisa cultivar um ecossistema público, científico e industrial capaz de experimentar, avaliar e corrigir rumos, combinando a estabilidade das políticas de Estado com a flexibilidade necessária à inovação. A soberania digital, nesse sentido, é também um projeto de país: traduz a capacidade de uma sociedade de compreender, governar e se beneficiar das tecnologias que a moldam.

O Brasil já dispõe da maior parte dos instrumentos legais e institucionais necessários para iniciar essa trajetória. Falta-lhe, contudo, a capacidade de coordenação que transforme normas dispersas em políticas integradas e coerentes, e diagnósticos reiterados em ações efetivas voltadas à construção de sistemas digitais autônomos. O primeiro passo rumo à soberania digital

brasileira, portanto, não é tecnológico, mas político: utilizar, com efetividade e propósito, os instrumentos já existentes e alavancar nossos ativos para desenvolver aquilo que ainda não possuímos, tornando-nos tecnologicamente autônomos sem deixar de permanecer abertos e interconectados.

Referências

ADA LOVELACE INSTITUTE. **Friends for sale: the rise and risks of AI companions**. Disponível em: https://www.adalovelaceinstitute.org/blog/ai-companions/. Acesso em: 6 dez. 2025.ADNER, Ron. Ecosystem as Structure: An Actionable Construct for Strategy. **Journal of Management**, v. 43, n. 1, p. 39–58, 2017.

AGÊNCIA ESTADO. **Comunicações obtém aval para investir R$ 58 mi em infraestrutura**. CNN Brasil. Disponível em: <https://www.cnnbrasil.com.br/economia/macroeconomia/ministerio-das-comunicacoes-obtem-aval-para-investir-r-58-mi-do-funttel-em-infraestrutura>. Acesso em: 6 nov. 2025.

ALONSO-GUINEA, Fernando; ALAÑÓN-PARDO, Ángel. On support from National Development Banks for the internationalisation of public Brazilian companies: it's hard to say goodbye (to good companies). **Journal of Economic Policy Reform**, v. 27, n. 4, p. 389–412, 2024.

ALVIM, Mariana; GALLAS, Daniel. **Pix investigado por EUA: como Brasil defende sistema de pagamentos**. BBC News Brasil. Disponível em: <https://www.bbc.com/portuguese/articles/cm2vrnq17vdo>. Acesso em: 27 ago. 2025.

AMARANTE, Jose Carlos Albano; FRANKO, Patrice. Defense Transformation in Latin America: Will It Transform the Technological Base? **Democracy and Security**, v. 13, n. 3, p. 173–195, 2017.

AMOORE, Louise. Cloud geographies: Computing, data, sovereignty. **Progress in Human Geography**, v. 42, n. 1, p. 4–24, 2018.

ANATI. **NOTA OFICIAL DA ANATI - Evasão recorde de futuros Analistas em TI aprovados no Concurso Público Nacional Unificado (CPNU)**. Associação Nacional dos Analistas em TI - ANATI. Disponível em: <https://anati.org.br/noticias/nota-oficial-da-anati-evasao-recorde-atis-cpnu>. Acesso em: 25 nov. 2025.

AQUINO, Miriam. **Redes de telecom voltam a ter prioridade na construção de obras de infraestrutura**. Tele.síntese. Portal de Telecom, internet e TIC. Disponível em: <https://telesintese.com.br/redes-de-telecom-voltam-a-ter-prioridade-na-construcao-de-obras-de-infraestrutura>. Acesso em: 6 nov. 2025.

ARAUJO, Misael Sousa de; MACHADO, Bruna Aparecida Souza; PASSOS, Francisco Uchoa. Resilience in the Context of Cyber Security: A Review of the Fundamental Concepts and Relevance. **Applied Sciences**, v. 14, n. 5, p. 2116, 2024.

ARCURI, Marcos; GONÇALVES, João Emílio. Margens de preferência adicionais: recomendações para sua efetiva aplicação no brasil. *In*: RAUEN, André Tortato (Org.). **Compras públicas para inovação no Brasil : novas possibilidades legais**. Brasília: IPEA, 2022, p. 271–308. Disponível em: <https://repositorio.ipea.gov.br/server/api/core/bitstreams/c5f52657-edb2-40ae-85aa-5c5f4d2196f4/content>. Acesso em: 5 nov. 2025.

BANCO INTERAMERICANO DE DESENVOLVIMENTO; TRIBUNAL DE CONTAS DA UNIÃO. **Modelo de Apoio a Compras Públicas de Inovação**. 2021: [s.n., s.d.].

BANSAL, Radhika. Net Neutrality in the Indian Context. 2021. Disponível em: <https://www.researchgate.net/doi/10.13140/RG.2.2.17647.56488>. Acesso em: 4 dez. 2025.

BARIFOUSE, Rafael. **Por que 5G da Huawei põe Brasil em saia-justa com China e EUA**. BBC News Brasil. Disponível em: <https://www.bbc.com/portuguese/brasil-50468237>. Acesso em: 12 nov. 2025.

BARRIOS, Lucas de Góis. Soberania, Planejamento Estatal e Transformação Digital: análise comparada dos instrumentos jurídicos da União Europeia e do Brasil. v. 2, n. 1, 2023. Disponível em: <http://resede.com.br/index.php/revista/article/view/69>.

BARROS, Mateus. Justiça dá 30 dias para Telegram e Signal se adequarem às leis brasileiras. Disponível em: <https://olhardigital.com.br/2022/04/01/internet-e-redes-sociais/justica-da-30-dias-para-telegram-e-signal-se-adequarem-as-leis-brasileiras/>. Acesso em: 4 jan. 2025.

BARTOLOMÉ, Mariano. Redes sociales, desinformación, cibersoberanía y vigilancia digital: una visión desde la ciberseguridad. **Revista de Estudios en Seguridad Internacional**, v. 7, nº.2, n. Revista de Estudios en Seguridad Internacional, p. 167–185, 2021.

BELLI, Luca. **Brasil precisa reconstruir sua soberania digital**. Estadão. Disponível em: <https://www.estadao.com.br/politica/blog-do-fausto-macedo/brasil-precisa-reconstruir-sua-soberania-digital/>. Acesso em: 13 nov. 2025.

BELLI, Luca. BRICS countries and AI sovereignty: Introduction to Thematic Section. **The African Journal of Information and Communication (AJIC)**, n. 34, p. 1–6, 2024.

BELLI, Luca. BRICS Countries to Build Digital Sovereignty. *In*: BELLI, Luca (Org.). **CyberBRICS: Cybersecurity Regulations in the BRICS Countries**. Cham: Springer International Publishing, 2021, p. 271–280. Disponível em: <https://doi.org/10.1007/978-3-030-56405-6_7>. Acesso em: 1 mar. 2023.

BELLI, Luca. **Building Good Digital Sovereignty through Digital Public Infrastructures and Digital Commons in India and Brazil**. ThinkTwenty (T20) India 2023 - Official Engagement Group of G20. Disponível em: <https://t20ind.org/research/building-good-digital-sovereignty-through-digital-public-infrastructures/>. Acesso em: 24 set. 2025.

BELLI, Luca. Cibersegurança: uma visão sistêmica rumo a uma Proposta de Marco Regulatório para um Brasil Digitalmente soberano. Disponível em: <https://cyberbrics.info/ciberseguranca-uma-visao-sistemica-rumo-a-uma-proposta-de-marco-regulatorio-para-um-brasil-digitalmente-soberano/>. Acesso em: 22 ago. 2023.

BELLI, Luca. **Community Networks: Building Digital Sovereignty and Environmental Sustainability**. Rio de Janeiro, RJ: Publicações Direito Rio, 2023.

BELLI, Luca (Org.). **CyberBRICS: Cybersecurity Regulations in the BRICS Countries**. Cham: Springer International Publishing, 2021. Disponível em: <https://link.springer.com/10.1007/978-3-030-56405-6>. Acesso em: 6 jun. 2024.

BELLI, Luca. **Da soberania digital à soberania em IA**. JOTA Jornalismo. Disponível em: <https://www.jota.info/opiniao-e-analise/colunas/ia-regulacao-democracia/da-soberania-digital-a-soberania-em-ia>. Acesso em: 11 mar. 2025.

BELLI, Luca. **De la gouvernance à la régulation de l'internet**. Paris: Berger Levrault, 2015. Disponível em: <https://hdl.handle.net/10438/33380>. Acesso em: 10 nov. 2025.

BELLI, Luca. **De la gouvernance à la régulation de l'internet**. Berger-Levrault, Boulogne-Billancourt, 2016. (Au fil des études). Disponível em: <https://univ-droit.fr/recherche/actualites-de-la-recherche/parutions/9385-de-la-gouvernance-a-la-regulation-de-l-internet>. Acesso em: 12 jun. 2024.

BELLI, Luca. Exploring the Key AI Sovereignty Enablers (KASE) of Brazil, towards an AI Sovereignty Stack. **SSRN Electronic Journal**, 2023. Disponível em: <https://www.ssrn.com/abstract=4465501>. Acesso em: 22 ago. 2023.

BELLI, Luca. **Glossary of Platform Law and Policy Terms**. Rio de Janeiro, RJ: Publicações Direito Rio, 2021.

BELLI, Luca. Neutralidade da rede, zero-rating e o Marco Civil da Internet. *In*: **Governança e regulações da internet na América Latina**. Rio de Janeiro: FGV Direito Rio, 2018, p. 175–204. Disponível em: <http://hdl.handle.net/10438/27164>. Acesso em: 3 mar. 2023.

BELLI, Luca. **Neutralidade de rede e ordem econômica**. Omci.gov.br. Disponível em: <https://www.omci.org.br/jurisprudencia/207/neutralidade-de-rede-e-ordem-economica/>. Acesso em: 13 nov. 2025.

BELLI, Luca. 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, p. 145, 2022.

BELLI, Luca. **Por que o ChatGPT descumpre a LGPD e por que peticionei à ANPD**. JOTA Jornalismo. Disponível em: <https://www.jota.info/artigos/por-que-o-chatgpt-descumpre-a-lgpd-e-por-que-peticionei-a-anpd>. Acesso em: 28 mar. 2025.

BELLI, Luca. IA generativa "grátis" é a nova fronteira da colonização digital. **Folha de S.Paulo,** São Paulo, 2025. Disponível em: https://www1.folha.uol.com.br/tec/2025/09/ia-generativa-gratis-e-a-nova-fronteira-da-colonizacao-digital.shtml. Acesso em: 5 mar. 2026.

BELLI, Luca. **Regulação da inteligência artificial para inglês ver?** Jota. Disponível em: <https://www.jota.info/opiniao-e-analise/colunas/ia-regulacao-democracia/regulacao-da-inteligencia-artificial-para-ingles-ver>. Acesso em: 10 nov. 2025.

BELLI, Luca. Soberania em Inteligência Artificial: O que é e quais facilitadores essenciais podem tornar o Brasil um país soberano em IA? *In*: VILLAS BÔAS CUEVA, Ricardo; SCHERTEL MENDES, Laura; BIONI, Bruno; *et al* (Orgs.). **Inteligência Artificial e Regulação**. Rio de Janeiro: Gen Jurídico, 2024. Disponível em: <https://cyberbrics.info/soberania-em-inteligencia-artificial-o-que-e-e-o-quais-facilitadores-essenciais-podem-tornar-o-brasil-um-pais-soberano-em-ia/>.

BELLI, Luca. Soberania em Inteligência Artificial: O que é e quais facilitadores essenciais podem tornar o Brasil um país soberano em IA?; (Sovereignty in Artificial Intelligence: What Is It and What Key Enablers Can Make Brazil a Sovereign Country in AI?). 2024. Disponível em: <https://www.ssrn.com/abstract=4961537>. Acesso em: 20 ago. 2025.

BELLI, Luca. Structural Power as a Critical Element of Social Media Platforms' Private Sovereignty. 2022. Disponível em: <https://papers.ssrn.com/abstract=4569863>. Acesso em: 23 set. 2025.

BELLI, Luca. **The scramble for data and the need for network self-determination**. openDemocracy. Disponível em: <https://www.opendemocracy.net/en/scramble-for-data-and-need-for-network-self-determination/>. Acesso em: 10 nov. 2025.

BELLI, Luca. To Get Its AI Foothold, Brazil Needs to Apply the Key AI Sovereignty Enablers (KASE). 2023. Disponível em: <https://papers.ssrn.com/abstract=4465501>. Acesso em: 23 set. 2025.

BELLI, Luca. **Views: On AI sovereignty and how Brazil can redefine it**. Medianama. Disponível em: <https://www.medianama.com/2024/06/223-views-ai-sovereignty-brazil-global-debate/>. Acesso em: 13 nov. 2025.

BELLI, Luca; BRIAN, Ana; MENDOZA, Jonathan; *et al*. **Transferência internacional de dados pessoais na América Latina: rumo à harmonização de normas**. 1a edição. Rio de Janeiro, RJ: Lumen Juris, 2024. Disponível em: <https://hdl.handle.net/10438/36141>. Acesso em: 28 jan. 2025.

BELLI, Luca; CELESTE, Edoardo; HELDT, Amélie; *et al*. Structural Power as a Critical Element of Digital Platforms Private Sovereignty. *In*: **Constitutionalising Social Media**. London: Hart, 2022.

BELLI, Luca; CHANG, Sofia. Governança de dados na China: Soberania, cibersegurança e proteção de dados rumo ao "Efeito Pequim". **Revista Brasileira de Direitos Fundamentais & Justiça**, v. 24, n. 53, 2025. Disponível em: <https://dfj.emnuvens.com.br/dfj/article/view/1730>. Acesso em: 5 mar. 2026.

BELLI, Luca; FOSSATI, Gustavo; MCCLASKEY, Layla; *et al*. Proteção de dados, tributação de dados e equidade de dados: equilíbrio entre valores, riscos e obrigações. **CPDP LatAm Discussion Papers**, 2025. Disponível em: <https://cpdp.lat/wp-content/uploads/2025/07/discussion-paper-cpdp-latam-2025.pdf>.

BELLI, Luca; FRANQUEIRA, Bruna Diniz; BAKONYI, Erica; *et al*. **Cibersegurança: uma visão sistêmica rumo a uma Proposta de Marco Regulatório para um Brasil Digitalmente soberano**. Rio de Janeiro, RJ: FGV Direito Rio, 2023. Disponível em: <https://hdl.handle.net/10438/33784>.

BELLI, Luca; GALDINO DE MAGALHÃES SANTOS, Larissa. Editorial: Toward a BRICS stack? Leveraging digital transformation to construct digital sovereignty in the BRICS countries. **Computer Law & Security Review**, v. 55, p. 106064, 2024.

BELLI, Luca; GASPAR, Walter B.; JASWANT, Shilpa Singh. Data sovereignty and data transfers as fundamental elements of digital transformation: Lessons from the BRICS countries. **Computer Law & Security Review**, v. 54, p. 106017, 2024.

BELLI, Luca; GASPAR, Walter Britto (Orgs.). **AI from the Global Majority: Official outcome of the UN IGF Data and Artificial Intelligence Governance Coalition**. Rio de Janeiro: FGV Direito Rio, 2024. (DC-DAIG, 2). Disponível em: <https://www.intgovforum.org/en/filedepot_download/279/28447>. Acesso em: 13 dez. 2024.

BELLI, Luca; GASPAR, Walter Britto (Orgs.). **The Quest for AI Sovereignty, Transparency and Accountability**. Rio de Janeiro: FGV Direito Rio, 2023. Disponível em: <https://hdl.handle.net/10438/34295>.

BELLI, Luca; GUGLIELMI, Gilles J.; BORDÈRE, Camille; *et al*. **L' État digital : numérisation de l'administration publique et administration publique du numérique / sous la direction de Luca Belli et Gilles J. Guglielmi**. [s.l.]: Berger-Levrault, 2022. (Au fil du débat. Etudes). Disponível em: <https://documentation.insp.gouv.fr/insp/doc/SYRACUSE/402376/l-etat-digital-numerisation-de-l-administration-publique-et-administration-publique-du-numerique-sou>. Acesso em: 23 set. 2025.

BELLI, Luca; JIANG, Min. Conclusion: Digital Sovereignty in the BRICS: Structuring Self-Determination, Cybersecurity, and Control. *In*: JIANG, Min; BELLI, Luca (Orgs.). **Digital Sovereignty in the BRICS Countries**. 1. ed. Cambridge: Cambridge University Press, 2025, p. 214–238. Disponível em: <https://www.cambridge.org/core/product/identifier/9781009531085%23CN-bp-10/type/book_part>. Acesso em: 23 set. 2025.

BELLI, Luca; MAGALHÃES, Larissa. **AI Sovereignty and AI Governance: Perspectives from the BRICS and Beyond**. [s.l.: s.n.], 2026.

BELLI, Luca; MAGALHÃES, Larissa. Computer Law & Security Review. **Digital Transformation in the BRICS Countries**, v. 54, . Disponível em: <https://www.sciencedirect.com/journal/computer-law-and-security-review>. Acesso em: 25 ago. 2025.

BELLI, Luca; MEDEIROS, Breno Pauli; COUTO, Natália; *et al*. **Governança e regulação da cibersegurança no Brasil: proteção da infraestrutura crítica, segurança da informação e construção da soberania digital**. [s.l.]: Lumen Juris, 2025. Disponível em: <https://cyberbrics.info/governanca-e-regulacao-da-ciberseguranca-no-brasil-protecao-da-infraestrutura-critica-

seguranca-da-informacao-e-construcao-da-soberania-digital/>. Acesso em: 14 out. 2025.

BELLI, Luca; MEDEIROS, Breno Pauli; COUTO, Natalia de Macedo; *et al*. **Governança e regulação da cibersegurança no Brasil**. [s.l.: s.n.], 2025. Disponível em: <https://hdl.handle.net/10438/37991>. Acesso em: 4 dez. 2025.

BELLI, Luca; NOUGRÈRES, Ana Brian; ISERTE, Jonathan Mendoza; *et al*. **Hacia un modelo latinoamericano de adecuación para la transferencia internacional de datos personales**. Rio de Janeiro: CPDP LatAm, 2023. (Discussion paper).

BELLI, Luca; ZINGALES, Nicolo. Interoperability to Foster Open Digital Ecosystems in the BRICS Countries. **SSRN Electronic Journal**, 2023. Disponível em: <https://www.ssrn.com/abstract=4641496>. Acesso em: 17 nov. 2025.

BIDARE, Pranav Majesh; DREYER, Stephan; KELLER, Clara Iglesias. **Between evidence and policy: bridging the gap in disinformation regulation**. Internet Policy Review. Disponível em: <https://policyreview.info/articles/news/between-evidence-and-policy-bridging-gap-disinformation-regulation/1667>. Acesso em: 4 dez. 2025.

BINGJIE LI. Export Effect of Trade Facilitation in Asian "Belt and Road" Coastal Countries on China's Cross-border E-commerce. **Journal of Coastal Research**, v. 104, p. 628–632, 2020.

BOBBIO, Norberto. **Dalla struttura alla funzione: nuovi studi di teoria del diritto**. Milano: Edizioni di Comunità, 1976. (Diritto e cultura moderna, 18). Disponível em: <https://lawcat.berkeley.edu/record/37023>. Acesso em: 22 out. 2025.

BORDEN, Col Andrew. What is Information Warfare?

BORRÁS, Susana; EDLER, Jakob. The roles of the state in the governance of socio-technical systems' transformation. Disponível em: <https://www.scopus.com/inward/record.uri?eid=2-s2.0-85083087971&doi=10.1016%2fj.respol.2020.103971&partnerID=40&md5=ef781c4b05337ff4e9436982451ffd5d>.

BORTOLASO, Ingridi Vargas; BALESTRIN, Alsones; TEIXEIRA, Rafael; *et al*. Trajectory of the Brazilian Semiconductor Industry and Supply Chain: Economic, Governmental, and Technological Perspectives. **Journal of Operations and Supply Chain Management**, v. 6, n. 2, p. 20–39, 2013.

BR, Núcleo de Informação e Coordenação do Ponto; EVANGELISTA, Rafael de Almeida; RABELLO, Maricy. **Educação em um cenário de plataformização e economia de dados: soberania e infraestrutura**. São Paulo, SP: Núcleo de Informação e Coordenação do Ponto BR, 2023.

BRAESEMANN, Fabian; STEPHANY, Fabian; TEUTLOFF, Ole; *et al*. The global polarisation of remote work. **PLOS ONE**, v. 17, n. 10, p. e0274630, 2022.

BRASIL. **Decreto 11.456**. Disponível em: <https://www.in.gov.br/en/web/dou/-/decreto-n-11.456-de-28-de-marco-de-2023-473390191>. Acesso em: 28 jan. 2025.

BRASIL. **Lei n. 14.533**. Disponível em: <https://www.planalto.gov.br/ccivil_03/_ato2023-2026/2023/lei/L14533.htm>. Acesso em: 10 nov. 2025.

BRASIL. **Plano brasileiro de IA terá supercomputador e investimento de R$ 23 bilhões em quatro anos**. Ministério da Ciência, Tecnologia e Inovação. Disponível em: <https://www.gov.br/mcti/pt-br/acompanhe-o-mcti/noticias/2024/07/plano-brasileiro-de-ia-tera-supercomputador-e-investimento-de-r-23-bilhoes-em-quatro-anos>. Acesso em: 13 nov. 2025.

BRASIL [GSI]. PNCiber – Apresentação do Projeto. Disponível em: <https://www.gov.br/gsi/pt-br/seguranca-da-informacao-e-cibernetica/audiencia-publica/PNCiberAudienciaPublicaProjetoBase.pdf>. Acesso em: 10 nov. 2025.

BRASIL [MCTI]. **Conhecimento Brasil trará de volta cientistas que atuam em 34 países; veja o resultado final**. Conselho Nacional de Desenvolvimento Científico e Tecnológico. Disponível em: <https://www.gov.br/cnpq/pt-br/assuntos/noticias/cnpq-em-acao/conhecimento-brasil-trara-de-volta-ao-brasil-cientistas-que-atuam-em-34-paises-veja-o-resultado-final>. Acesso em: 18 nov. 2025.

BRASIL [MDIC]. **Brasil ganha nova política industrial com metas e ações para o desenvolvimento até 2033**. Ministério do Desenvolvimento, Indústria,

Comércio e Serviços. Disponível em: <https://www.gov.br/mdic/pt-br/assuntos/noticias/2024/janeiro/brasil-ganha-nova-politica-industrial-com-metas-e-acoes-para-o-desenvolvimento-ate-2033>. Acesso em: 13 nov. 2025.

BRASIL [MME]. **Brasil registra maior produção de energia limpa dos últimos 12 anos**. Ministério de Minas e Energia. Disponível em: <https://www.gov.br/mme/pt-br/assuntos/noticias/brasil-registra-maior-producao-de-energia-limpa-dos-ultimos-12-anos>. Acesso em: 10 nov. 2025.

BRASIL [MS]. **Programa de Desenvolvimento e Inovação Local**. Ministério da Saúde. Disponível em: <https://www.gov.br/saude/pt-br/composicao/sectics/pdil/programa-de-desenvolvimento-e-inovacao-local>. Acesso em: 28 ago. 2025.

BRASIL, Presidência da República. Lei de Licitações e Contratos Administrativos. Disponível em: <https://www.planalto.gov.br/ccivil_03/_ato2019-2022/2021/lei/l14133.htm>. Acesso em: 23 set. 2025.

BRATTON, Benjamin H. **The stack: on software and sovereignty**. Cambridge, Mass. London: MIT press, 2015. (Software studies).

BREMMER, Ian. The Technopolar Moment: How Digital Powers Will Reshape the Global Order. **Foreign Affairs**, v. 100, n. 6, p. 112–128, 2021.

BRIA, Francesca; TIMMERS, Paul; GERNONE, Fausto. EuroStack – A European Alternative for Digital Sovereignty. p. 127 p., 2025.

BRUNER, Christopher. States, Markets, and Gatekeepers: Public-Private Regulatory Regimes in an Era of Economic Globalization. **Michigan Journal of International Law**, v. 30, n. 1, p. 125–176, 2008.

CARAMANCION, Kevin Matthe; LI, Yueqi; DUBOIS, Elisabeth; *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, 2022.

CARR, E. H. **The Twenty Years' Crisis, 1919-1939: Reissued with a new preface from Michael Cox**. [s.l.]: Springer, 2016.

CASAGRANDE, Dieison; MALLMANN, Conrado; FEISTEL, Paulo Ricardo. US-China Trade War: The Effects of Trade Conflict on Brazilian Exports. **SSRN Electronic Journal**, 2023. Disponível em: <https://www.ssrn.com/abstract=4577170>. Acesso em: 29 out. 2025.

CASSIOLATO, José Eduardo; LASTRES, Helena; SOARES, Maria Clara. The Brazilian national system of innovation: challenges to sustainability and inclusive development. *In*: DUTRÉNIT, Gabriela; SUTZ, Judith (Orgs.). **National Innovation Systems, Social Inclusion and Development**. [s.l.]: Edward Elgar Publishing, 2014. Disponível em: <https://china.elgaronline.com/view/edcoll/9781782548676/9781782548676.00008.xml>. Acesso em: 26 set. 2025.

CATH, Corinne. **Clouds Over the Netherlands: Preserving Public Interest Internet Governance in the Era of Hyperscaler Clouds**. Amsterdam: Zenodo, 2025. Disponível em: <https://zenodo.org/doi/10.5281/zenodo.15230914>. Acesso em: 10 nov. 2025.

CENTER FOR STRATEGIC AND INTERNATIONAL STUDIES (CSIS). **What to Know About the Signed U.S.-Ukraine Minerals Deal**. Disponível em: <https://www.csis.org/analysis/what-know-about-signed-us-ukraine-minerals-deal>. Acesso em: 6 nov. 2025.

CETIC.BR. **TIC Domicílios**. Centro Regional para o Desenvolvimento da Sociedade da Informação. Disponível em: <https://cetic.br/pt/pesquisa/domicilios/publicacoes/>. Acesso em: 10 nov. 2025.

CHACON, Guilherme; BAWDEN SILVERIO DE CASTRO, Henrique; XAVIER MORALES, Luiza; *et al.* **Análise: Termos De Uso e Políticas De Privacidade do Google Workspace for Education e Microsoft 365 (Office 365 Educação)**. [s.l.]: Zenodo, 2022. Disponível em: <https://zenodo.org/record/7718863>. Acesso em: 10 nov. 2025.

CHAGNON, C. W.; DURANTE, F.; GILLS, B. K.; *et al.* From extractivism to global extractivism: the evolution of an organizing concept. n. 49(4), p. 760–792, . (The Journal of Peasant Studies).

CHALLAPALLY, Aditya; PEASE, Chris; RASKAR, Ramesh; *et al*. STATE OF AI IN BUSINESS 2025.

CHAN, Kyle; SMITH, Gregory; GOODRICH, Jimmy; *et al*. **Full Stack: China's Evolving Industrial Policy for AI**. [s.l.: s.n.], 2025. Disponível em: <https://www.rand.org/pubs/perspectives/PEA4012-1.html>. Acesso em: 6 nov. 2025.

CHENEY, David W.; VAN ATTA, Richard. 8. DARPA's Process for Creating New Programs. p. 229–288, 2020.

CHINA. Proposta do Comitê Central do PCC sobre a formulação do 15º Plano Quinquenal para o Desenvolvimento Econômico e Social Nacional (中共中央关于制定国民经济和社会发展第十五个五年规划的建议). 2025. Disponível em: <https://www.gov.cn/zhengce/202510/content_7046052.htm>. Acesso em: 19 nov. 2025.

CHOUDHURY, S. P.; SHARMA, S.; JAIN, S. Three Waves: Tracking the Evolution of India's Startups. Disponível em: <https://knowledge.wharton.upenn.edu/article/three-waves-tracking-evolution-indias-startups/>. Acesso em: 13 nov. 2025.

CHRISTL, Wolfie. How Companies Use Personal Data Against People. Automated Disadvantage, Personalized Persuasion, and the Societal Ramifications of the Commercial Use of Personal Information. **Working paper by Cracked Labs**, 2017. Disponível em: <https://crackedlabs.org/dl/CrackedLabs_Christl_DataAgainstPeople.pdf>. Acesso em: 25 ago. 2025.

CMA. **CMA AI strategic update**. GOV.UK. Disponível em: <https://www.gov.uk/government/publications/cma-ai-strategic-update/cma-ai-strategic-update>. Acesso em: 10 nov. 2025.

CNDI. **Nova Indústria Brasil: Plano de ação para a Neoindustrialização**. Brasília: Conselho Nacional de Desenvolvimento Industrial, MDIC, 2024. Disponível em: <https://www.gov.br/mdic/pt-br/composicao/se/cndi/plano-de-acao/nova-industria-brasil-plano-de-acao.pdf>. Acesso em: 20 fev. 2024.

COBBE, Jennifer; SINGH, Jatinder. Regulating Recommending: Motivations, Considerations, and Principles. **European Journal of Law and Technology**, v.

10, n. 3, 2019. Disponível em: <https://ejlt.org/index.php/ejlt/article/view/686>. Acesso em: 4 dez. 2025.

COCHRANE, Daniel. **Big Tech's Power to Shape Public Discourse**. The Heritage Foundation. Disponível em: <https://www.heritage.org/big-tech/report/big-techs-power-shape-public-discourse>. Acesso em: 13 nov. 2025.

COELHO, Cido. **Huawei abre código de modelos de IA enquanto busca adoção no mercado global**. Times Brasil – Licenciado Exclusivo CNBC. Disponível em: <https://timesbrasil.com.br/empresas-e-negocios/tecnologia-e-inovacao/huawei-abre-codigo-de-modelos-de-ia-enquanto-busca-adocao-no-mercado-global/>. Acesso em: 12 nov. 2025.

CORIAT, Benjamin; WEINSTEIN, Olivier. Intellectual Property Right Regimes, Firms and the Commodification of Knowledge. **SSRN Electronic Journal**, 2009. Disponível em: <http://www.ssrn.com/abstract=1440866>. Acesso em: 9 fev. 2023.

COSTA, Viviane da; GASPAR, Walter Britto; JOHANSSON, Germano. Brazilian AI Sovereignty: an agenda evaluation. *In*: BELLI, Luca; MAGALHÃES, Larissa (Orgs.). **AI Sovereignty and AI Governance: Perspectives from the BRICS and Beyond**. [s.l.: s.n.], 2026.

COSTA, João Erick Alexandre Barbosa; FREGUGLIA, Ricardo da Silva; SILVA, Thamyres Firmino Gomes da; *et al*. Wage returns from telework in Brazil: an analysis based on the concept of potential telework. **Revista Brasileira de Economia de Empresas**, v. 24, n. 2, 2024. Disponível em: <https://portalrevistas.ucb.br/index.php/rbee/article/view/15487>. Acesso em: 25 nov. 2025.

COULDRY, Nick; MEJIAS, Ulises A. Data Colonialism: Rethinking Big Data's Relation to the Contemporary Subject. **Television & New Media**, v. 20, n. 4, p. 336–349, 2019.

COULDRY, Nick; MEJIAS, Ulises A. The Costs of Connection: How Data Are Colonizing Human Life and Appropriating It for Capitalism. **ResearchGate**, 2024. Disponível em: <https://www.researchgate.net/publication/344629010_The_Costs_of_Connection_How_Data_Are_Colonizing_Human_Life_and_Appropriating_It_for_Capitalism>. Acesso em: 11 mar. 2025.

COUTO, Natália. Regulação de redes sociais no Brasil: grupos de interesse e o caso do PL 2630/2020. *In*: **Os caminhos da internacionalização e o futuro do Direito**. São Paulo: Conpedi (prelo), 2025.

COUTO, Natalia de Macedo. O papel regulatório do Estado na moderação de conteúdo exercida pelas plataformas de redes sociais. 2022. Disponível em: <https://hdl.handle.net/10438/33008>. Acesso em: 13 jun. 2024.

CPDP LATAM. **Publications**. Publications. Disponível em: <https://cpdp.lat/en/publications/>. Acesso em: 13 nov. 2025.

CSERNATONI, Raluca; MAVRONA, Katerina. The Artificial Intelligence and Cybersecurity Nexus: Taking Stock of the European Union's Approach. 2022. Disponível em: <https://www.vectra.ai/news/as-the-war-in-ukraine-spirals-vectra-ai-announces-free-cybersecurity-services.>.

CTS-FGV. **Centro de Tecnologia e Sociedade**. Centro de Tecnologia e Sociedade. Disponível em: <https://direitorio.fgv.br/pesquisa/centro-de-tecnologia-e-sociedade>. Acesso em: 20 out. 2025.

CULPEPPER, Pepper D.; THELEN, Kathleen. Are We All Amazon Primed? Consumers and the Politics of Platform Power. **Comparative Political Studies**, v. 53, n. 2, p. 288–318, 2020.

CUNHA, Bruno Queiroz. Os regulocratas : características corporativas e implicações sistêmicas do funcionamento da burocracia das agências reguladoras no Brasil. **http://www.ipea.gov.br**, 2017. Disponível em: <https://repositorio.ipea.gov.br/handle/11058/7931>. Acesso em: 14 set. 2024.

CUNNINGHAM, Paul; EDLER, Jakob; FLANAGAN, Kieron; *et al*. The innovation policy mix. *In*: EDLER, Jakob; CUNNINGHAM, Paul; GÖK, Abdullah; *et al* (Orgs.). **Handbook of Innovation Policy Impact**. [s.l.]: Edward Elgar Publishing, 2016. Disponível em: <https://elgaronline.com/view/edcoll/9781784711849/9781784711849.00024.xml>. Acesso em: 6 mar. 2026.

CYBERBRICS. Cybersecurity and Digital Sovereignty: A New Path for Brazil. Disponível em: <https://cyberbrics.info/cybersecurity-and-digital-sovereignty-a-new-path-for-brazil/>. Acesso em: 10 nov. 2025.

DAVE, Paresh. This Website Shows How Much Google's AI Can Glean From Your Photos. **Wired**, 2024. Disponível em: <https://www.wired.com/story/website-google-ai-photos-ente/>. Acesso em: 10 nov. 2025.

DE SAILLE, Stevienna; MEDVECKY, Fabien. Innovation for a steady state: a case for responsible stagnation. **Economy and Society**, v. 45, n. 1, p. 1–23, 2016.

DESMARAIS, Anna. Is overreliance on US Big Tech a threat to Europe? The Netherlands may soon find out. Euronews. 2025. Disponível em: <https://www.euronews.com/next/2025/02/27/is-overreliance-on-us-big-tech-a-threat-to-europe-the-netherlands-may-soon-find-out>. Acesso em: 15 set. 2025.

DEVANNY, Joe. Artificial Intelligence and Cyber Power. **Research Publications**, 2024. Disponível em: <https://digitalcommons.fiu.edu/jgi_research/63>.

DOHNÁNY, Sebastian; KURTH-NELSON, Zeb; SPENS, Eleanor; *et al*. Technological folie à deux: Feedback Loops Between AI Chatbots and Mental Illness. 2025. Disponível em: <http://arxiv.org/abs/2507.19218>. Acesso em: 6 dez. 2025.

DOWSE, Andrew; BACHMANN, Sascha Dov. Information warfare: methods to counter disinformation. **Defense & Security Analysis**, v. 38, n. 4, p. 453–469, 2022.

DRAPER, Hannah; BELLI, Luca; MEIRA, Marina; *et al*. **A Consumer-centric Approach to DPIs for sustainable financial inclusion**. Brasil: T20 Brasil 2024, 2024. (Inclusive Digital Transformation).

DYSA, Yuliia. Ukraine, US launch fund for critical minerals projects with $150 million investment. **Reuters**, 2025. Disponível em: <https://www.reuters.com/business/finance/ukraine-us-launch-fund-critical-minerals-projects-with-150-million-investment-2025-09-17/>. Acesso em: 6 nov. 2025.

EDITORA, Juruá. **Teoria do Estado Regulador - Volume I - Coleção FGV Direito Rio**. Juruá Editora. Disponível em: <https://www.jurua.com.br/shop_item.asp?id=24100>. Acesso em: 25 nov. 2025.

EDLER, Jakob; FAGERBERG, Jan. Innovation Policy: What, Why & How. **Working Papers on Innovation Studies**, 2016. (Working Papers on Innovation

Studies). Disponível em: <https://ideas.repec.org//p/tik/inowpp/20161111.html>. Acesso em: 22 set. 2025.

EDQUIST, Charles. Striving Towards a Holistic Innovation Policy in European Countries -But Linearity Still Prevails! **STI Policy Review**, v. 5, n. 2, p. 1–19, 2014.

EUROPEAN COMMISSION (Org.). **The future of European competitiveness: Part A: A competitiveness strategy for Europe**. Luxembourg: Publications Office, 2025. Disponível em: <https://commission.europa.eu/document/download/97e481fd-2dc3-412d-be4c-f152a8232961_en>.

EUROPEAN WORKING TEAM ON DIGITAL COMMONS. **Towards a Sovereign Digital Infrastructure of Commons**. Paris, France: [s.n.], 2022. Disponível em: <https://labo.societenumerique.gouv.fr/en/articles/european-initiative-of-19-member-states-around-the-digital-commons-what-are-the-key-proposals/>. Acesso em: 4 dez. 2025.

EYAL, Nir; HOOVER, Ryan. **Hooked: Como construir produtos e serviços formadores de hábitos**. São Paulo: AlfaCon, 2020. Disponível em: <https://www.amazon.com.br/HOOKED-ENGAJADO-construir-produtos-formadores/dp/8583394768>.

FARIS, Robert; ASHAR, Amar; GASSER, Urs; *et al*. Understanding Harmful Speech Online | Berkman Klein Center. **Berkman Klein Center for Internet & Society Publication**, 2016. Disponível em: <https://dash.harvard.edu/handle/1/38022941>. Acesso em: 4 dez. 2025.

FARRELL, Henry; NEWMAN, Abraham L. Weaponized Interdependence: How Global Economic Networks Shape State Coercion. **International Security**, v. 44, n. 1, p. 42–79, 2019.

FARRELL, Henry; NEWMAN, Abraham L. Weaponized Interdependence: How Global Economic Networks Shape State Coercion. **International Security**, v. 44, n. 1, p. 42–79, 2019.

FIANI, Ronaldo; INSTITUTO DE PESQUISA ECONÔMICA APLICADA (Orgs.). ARRANJOS INSTITUCIONAIS E DESENVOLVIMENTO: O PAPEL DA COORDENAÇÃO EM ESTRUTURAS HÍBRIDAS.

In: **CAPACIDADES ESTATAIS E DEMOCRACIA: ARRANJOS INSTITUCIONAIS DE POLÍTICAS PÚBLICAS**. Brasília: Ipea, 2014. Disponível em: <https://repositorio.ipea.gov.br/server/api/core/bitstreams/f3c0af80-8a54-40f3-a2ad-7c01f1491bab/content>.

FONSECA, Bruno. **Google pagou R$ 670 mil em anúncios contra o PL 2630**. Agência Pública. Disponível em: <https://apublica.org/2023/05/google-pagou-mais-de-meio-milhao-de-reais-em-anuncios-no-facebook-contra-pl-das-fake-news/>. Acesso em: 10 nov. 2025.

FOSS, Maria Carolina. **Compras públicas como instrumento de política de inovação orientada à demanda: experiências no Brasil, nos Estados Unidos e na União Europeia.** tese de doutorado, Universidade Estadual de Campinas, Campinas, 2019. Disponível em: <file:///C:/Users/natalia.couto/Downloads/Foss_MariaCarolina_D.pdf>.

FOSS, Maria Carolina. **COMPRAS PÚBLICAS COMO INSTRUMENTO DE POLÍTICA DE INOVAÇÃO ORIENTADA À DEMANDA: EXPERIÊNCIAS NO BRASIL, NOS ESTADOS UNIDOS E NA UNIÃO EUROPEIA**. Unicamp, 2019.

FOSS, Maria Carolina; COUTINHO, Diogo; MITERHOF, Marcelo. Jota. **A regulação para a inovação**, 2023. Disponível em: <https://www.jota.info/opiniao-e-analise/artigos/a-regulacao-para-a-inovacao>. Acesso em: 23 set. 2025.

FOSS, Maria Carolina; MONTEIRO, Vítor. Diálogos competitivos motivados pela inovação. *In*: RAUEN, André Tortato (Org.). **Compras públicas para inovação no Brasil : novas possibilidades legais**. Brasília: IPEA, 2022, p. 239–270. Disponível em: <http://repositorio.ipea.gov.br/handle/11058/11623>. Acesso em: 5 nov. 2025.

FRANÇA. **LaSuite : l'espace de travail collaboratif**. LaSuite: l'espace de travail collaboratif. Disponível em: <https://www.numerique.gouv.fr/offre-accompagnement/expertise-suite-num%C3%A9rique/>. Acesso em: 4 dez. 2025.

FRANCO, Sebastián Fernández; GRAÑA, Juan M.; RIKAP, Cecilia. Dependency in the Digital Age? The Experience of Mercado Libre in Latin America. **Development and Change**, v. 55, n. 3, p. 429–464, 2024.

FRANKE, Ulrike. Artificial Intelligence diplomacy | Artificial Intelligence governance as a new external policy tool. 2021.

G1 REDAÇÃO. **WhatsApp já foi bloqueado por decisão judicial em 2015 e 2016 no Brasil**. G1. Disponível em: <https://g1.globo.com/tecnologia/noticia/2022/03/18/whatsapp-ja-foi-bloqueado-por-decisao-judicial-em-2015-e-2016-no-brasil.ghtml>. Acesso em: 29 out. 2025.

GARBE, Hugo de Souza. **Os impactos do Marco Legal das Startups no ecossistema empreendedor nacional: uma análise dos efeitos do Marco Legal das Startups no desenvolvimento tecnológico e empresarial no Brasil**. Escola de Direito da FGV SP, São Paulo, 2025. Disponível em: <https://hdl.handle.net/10438/36582>. Acesso em: 18 nov. 2025.

GARCIA, Renato; ROSELINO, José Eduardo. Uma avaliação da Lei de Informática e de seus resultados como instrumento indutor de desenvolvimento tecnológico e industrial. **Gestão & Produção**, v. 11, p. 177–185, 2004.

GASPAR, Walter; BELLI, Luca; JASWANT, Smriti. Data Sovereignty and Data Transfers as Fundamental Elements of Digital Transformation. *In*: **AI Sovereignty and AI Governance: Perspectives from the BRICS and Beyond.** [s.l.: s.n.], 2026.

GELUVARAJ, B.; SATWIK, P. M.; KUMAR, T. A. Ashok. The future of cybersecurity: Major role of artificial intelligence, machine learning, and deep learning in cyberspace. **International Conference on Computer Networks and Communication Technologies**, 2018. Disponível em: <https://api.semanticscholar.org/CorpusID:169166053>.

GENDRON, Will. **ChatGPT needs to "drink" a water bottle's worth of fresh water for every 20 to 50 questions you ask, researchers say**. Business Insider. Disponível em: <https://www.businessinsider.com/chatgpt-generative-ai-water-use-environmental-impact-study-2023-4>. Acesso em: 10 nov. 2025.

GERSTENBERER, Fatima Cristina Santoro; GERSTENBERER, Guilherme Santoro. Controvérsias acerca do Marco Legal das Startups no Brasil. 2021. Disponível em: <https://app.periodikos.com.br/article/10.5281/zenodo.5948988/pdf/rbcen-1-1-1.pdf>.

GIESTEIRA, Luís Felipe; MATOS, Patrícia de Oliveira. Compras públicas em defesa. *In*: RAUEN, André Tortato (Org.). **Compras públicas para inovação no Brasil : novas possibilidades legais**. Brasília: IPEA, 2022, p. 309–380. Disponível em: <http://repositorio.ipea.gov.br/handle/11058/11623>. Acesso em: 5 nov. 2025.

GILLESPIE, Tarleton. Do Not Recommend? Reduction as a Form of Content Moderation. **Social Media + Society**, v. 8, n. 3, p. 20563051221117552, 2022.

GINGLASS, Mário Roberto. **Soberania e uso de tecnologias emergentes e de serviços de computação em nuvem por empresas públicas federais no Brasil**. Escola Superior de Guerra, 2024. Disponível em: <https://repositorio.esg.br/handle/123456789/1973>.

GOES, Severino. **Estímulo ao setor tecnológico é o principal objetivo da lei das startups**. Consultor Jurídico. Disponível em: <https://www.conjur.com.br/2021-jun-04/estimulo-setor-tecnologico-principal-objetivo-lei-startups/>. Acesso em: 19 nov. 2025.

GONÇALVES, Naira Teresa A. C.; RAPINI, Márcia Siqueira; ANTIGO, Mariangela Furlan. Formação de competências como desafio à inovação no Brasil: uma análise comparativa regional para o período 2012-2019. **Revista de Economia Contemporânea**, v. 28, p. e242802, 2024.

GORWA, Robert; ASH, Timothy Garton. Democratic Transparency in the Platform Society. *In*: TUCKER, Joshua A.; PERSILY, Nathaniel (Orgs.). **Social Media and Democracy**. Cambridge: Cambridge University Press, 2020, p. 286–312. (SSRC Anxieties of Democracy). Disponível em: <https://www.cambridge.org/core/books/social-media-and-democracy/democratic-transparency-in-the-platform-society/F4BC23D2109293FB4A8A6196F66D3E41>. Acesso em: 4 dez. 2025.

GROHMANN, Rafael. Not just platform, nor cooperatives: worker-owned technologies from below. **Communication, Culture and Critique**, v. 16, n. 4, p. 274–282, 2023.

GUPTA, Ritwik; WALKER, Leah; REDDIE, Andrew W. Whack-a-Chip: The Futility of Hardware-Centric Export Controls. 2024. Disponível em: <http://arxiv.org/abs/2411.14425>. Acesso em: 26 nov. 2025.

HACKENBURG, Kobi; TAPPIN, Ben M.; HEWITT, Luke; *et al*. The levers of political persuasion with conversational artificial intelligence. **Science**, v. 390, n. 6777, p. eaea3884, 2025.

HARIHARAN, Venkatesh; NATARAJAN, Sarayu. Digital Sovereignty and Payments: A Case Study of the National Payments Corporation of India. *In*: JIANG, Min; BELLI, Luca (Orgs.). **Digital Sovereignty in the BRICS Countries**. 1. ed. Cambridge: Cambridge University Press, 2025, p. 105–123. Disponível em: <https://www.cambridge.org/core/product/identifier/9781009531085%23CN-bp-5/type/book_part>. Acesso em: 13 nov. 2025.

HARRIS, Tristan. **How Technology is Hijacking Your Mind — from a Former Insider**. Thrive Global. Disponível em: <https://medium.com/thrive-global/how-technology-hijacks-peoples-minds-from-a-magician-and-google-s-design-ethicist-56d62ef5edf3>. Acesso em: 10 nov. 2025.

HE, Alex; ARCESATI, Rebecca. **Data Marketplaces and Governance: Lessons from China**. Centre for International Governance Innovation. Disponível em: <https://www.cigionline.org/articles/data-marketplaces-and-governance-lessons-from-china/>. Acesso em: 11 nov. 2025.

HENDERSON, Rebecca M.; CLARK, Kim B. Architectural Innovation: The Reconfiguration of Existing Product Technologies and the Failure of Established Firms. **Administrative Science Quarterly**, v. 35, n. 1, p. 9, 1990.

HOOVER, Amanda. **Mark Zuckerberg destroyed friendship. Now he wants to replace it with AI.** Business Insider. Disponível em: <https://www.businessinsider.com/mark-zuckerberg-destroyed-friendship-replace-ai-companions-loneliness-2025-5>. Acesso em: 6 dez. 2025.

HRYNKIV, Olga; LAVRIJSSEN, Saskia. Not Trading With the Enemy: The Case of Computer Chips. **Journal of World Trade**, v. 58, n. 1, 2024. Disponível em: <https://kluwerlawonline.com/api/Product/CitationPDFURL?file=Journals\TRAD\TRAD2024003.pdf>. Acesso em: 29 out. 2025.

HUMAN RIGHTS WATCH. **World Report 2025 | Human Rights Watch**. [s.l.: s.n.], 2025. Disponível em: <https://www.hrw.org/world-report/2025>. Acesso em: 4 dez. 2025.

HYATT, Katherine; RYLE, Patrick M.; MCKNIGHT, Mark A. Semiconductor production, geopolitics and the CHIPS ACT of 2022: a theoretical analysis. **Digital Policy, Regulation and Governance**, v. 27, n. 1, p. 1–16, 2024.

IDEC; INSTITUTO LOCOMOTIVA. **Acesso à internet móvel pelas classes CDE**. São Paulo: IDEC e Instituto Locomotiva, 2021. Disponível em: <https://idec.org.br/sites/default/files/pesquisa_locomotiva_relatorio.pdf>. Acesso em: 3 mar. 2023.

IGNATOV, Alexander; KERIMI, Danil. Russia's securitised approach to AI sovereignty. **The African Journal of Information and Communication (AJIC)**, n. 35, p. 1–11, 2025.

ITU-T - INTERNATIONAL TELECOMMUNICATION UNION. Recommendation ITU-T X.1205: Overview of Cybersecurity. Disponível em: <file:///C:/Users/user/Downloads/T-REC-X.1205-200804-I!!PDF-E.pdf>. Acesso em: 31 ago. 2024.

JACKSON, Rosanna. The purpose of policy space for developing and developed countries in a changing global economic system. **Research in Globalization**, v. 3, p. 100039, 2021.

JACOBIDES, Michael G.; LIANOS, Ioannis. Ecosystems and competition law in theory and practice. **Industrial and Corporate Change**, v. 30, n. 5, p. 1199–1229, 2021.

JAJODIA, Sushil; ALBANESE, Massimiliano. An Integrated Framework for Cyber Situation Awareness. *In*: LIU, Peng; JAJODIA, Sushil; WANG, Cliff (Orgs.). **Theory and Models for Cyber Situation Awareness**. Cham: Springer International Publishing, 2017, v. 10030, p. 29–46. (Lecture Notes in

Computer Science). Disponível em: <http://link.springer.com/10.1007/978-3-319-61152-5_2>. Acesso em: 25 set. 2025.

JIA, Liu; BOJIKIAN, Neusa Maria Pereira; TEDESCHI, Aline; *et al*. STRATEGIC MANEUVERING IN BRAZIL'S 5G DEPLOYMENT AMIDST UNITED STATES-CHINA TECHNOLOGICAL RIVALRY. **Revista Tempo do Mundo**, n. 34, p. 419–451, 2024.

JIANG, Min. **U.S. Ban on Huawei: Superpowers' Insecurities and Nightmares**. CyberBRICS. Disponível em: <https://cyberbrics.info/u-s-ban-on-huawei-superpowers-insecurities-and-nightmares/>. Acesso em: 11 nov. 2025.

JIANG, Min; BELLI, Luca. Digital Sovereignty in the BRICS Countries. 2024.

JIANG, Min; BELLI, Luca (Orgs.). **Digital Sovereignty in the BRICS Countries: How the Global South and Emerging Power Alliances Are Reshaping Digital Governance**. 1. ed. [s.l.]: Cambridge University Press, 2025. Disponível em: <https://www.cambridge.org/core/product/identifier/9781009531085/type/book>. Acesso em: 20 ago. 2025.

JIANG, Min; BELLI, Luca (Orgs.). **Digital Sovereignty in the BRICS Countries: How the Global South and Emerging Power Alliances Are Reshaping Digital Governance**. 1. ed. Cambridge: Cambridge University Press, 2025. Disponível em: <https://www.cambridge.org/core/product/identifier/9781009531085/type/book>. Acesso em: 11 nov. 2025.

JONES, Erik; WHITWORTH, Andrew. The Unintended Consequences of European Sanctions on Russia. **Survival**, v. 56, n. 5, p. 21–30, 2014.

JR, Gilberto Scofield. **Alliance between Meta and Trump is likely to create informational, economic and geopolitical conflicts around the world**. The Conversation. Disponível em: <http://theconversation.com/alliance-between-meta-and-trump-is-likely-to-create-informational-economic-and-geopolitical-conflicts-around-the-world-246872>. Acesso em: 10 out. 2025.

JUDGE, E.F.; KORHANI, A.M. Disinformation, Digital Information Equality, and Electoral Integrity. **Election Law Journal: Rules, Politics, and Policy**, v. 19, n. 2, p. 240–261, 2020.

JÚLIO WIZIACK. **Para liberar Huawei, Bolsonaro obriga teles a construírem uma rede de telefonia só para o governo**. Folha de S.Paulo. Disponível em: <https://www1.folha.uol.com.br/mercado/2021/01/para-liberar-huawei-bolsonaro-obriga-teles-a-construirem-uma-rede-de-telefonia-so-para-o-governo.shtml>. Acesso em: 29 out. 2025.

KALANTZAKOS, Sophia. The Race for Critical Minerals in an Era of Geopolitical Realignments. **The International Spectator**, v. 55, n. 3, p. 1–16, 2020.

KAMEPALLI, Sai Krishna; RAJAN, Raghuram G.; ZINGALES, Luigi. Kill Zone. 2020. Disponível em: <https://papers.ssrn.com/abstract=3594344>. Acesso em: 10 nov. 2025.

KLIMEK, Peter; BAUM, Sophia; GERSCHBERGER, Markus; *et al*. **Systemic Trade Risk Suppresses Comparative Advantage in Rare Earth Dependent Industries**. arXiv.org. Disponível em: <https://arxiv.org/abs/2508.00556v1>. Acesso em: 26 nov. 2025.

KREMPL, Stefan. Criminal Court: Microsoft's email block a wake-up call for digital sovereignty. 2025. Disponível em: <https://www.heise.de/en/news/Criminal-Court-Microsoft-s-email-block-a-wake-up-call-for-digital-sovereignty-10387383.html>.

KUMAR, Pramod. THE EVOLUTION OF INFORMATION WARFARE: FROM PROPAGANDA TO CYBERATTACKS.

KUMAR, Purushottam; KUMAR, Dr Prakash. Vendor Lock-In Situation and Threats in Cloud Computing. v. 7, n. 9, 2022.

LANDYMORE, Frank. **Meta Is Being Incredibly Sketchy About Training Its AI on Your Private Photos**. Futurism. Disponível em: <https://futurism.com/meta-sketchy-training-ai-private-photos>. Acesso em: 10 nov. 2025.

LASTRES, Helena M M; CASSIOLATO, José Eduardo; DANTAS, Marcos. **Panorama da economia de dados no Brasil nos anos 2020**. Rio de Janeiro: RedeSist, 2024. (Economia de dados: conceitos, sistemas de mensuração e políticas em países selecionados e no Brasil). Disponível em: <https://www.ie.ufrj.br/images/IE/grupos/redesist/SITE/PROJETOS/22/NT13%20Dantas%20Lastres%20Cassiolato.pdf>. Acesso em: 24 out. 2025.

LASTRES, Helena Maria Martins; CASSIOLATO, José Eduardo; DANTAS, Marcos (Orgs.). **ECONOMIA POLÍTICA DE DADOS E SOBERANIA DIGITAL: conceitos, desafios e experiências no mundo**. Avaré, SP: Editora Contracorrente, 2025.

LAZER, David M. J.; BAUM, Matthew A.; BENKLER, Yochai; *et al*. The science of fake news. **Science**, v. 359, n. 6380, p. 1094–1096, 2018.

LEE, Keun; MALERBA, Franco; PRIMI, Annalisa. The fourth industrial revolution, changing global value chains and industrial upgrading in emerging economies. **Journal of Economic Policy Reform**, v. 23, n. 4, p. 359–370, 2020.

LENHART, Amanda; YBARRA, Michele; ZICKUHR, Kathryn; *et al*. Online Harassment, Digital Abuse, and Cyberstalking in America. **Data & Society Research Institute**, 2016.

LESSIG, Lawrence. **Code: And Other Laws of Cyberspace**. Sydney: ReadHowYouWant.com, 2009.

LESSIG, Lawrence. The law of the horse: What cyber law might teach. **Harv. L. Rev.**, v. 113, p. 501, 1999.

LESWING, Kif. **Nvidia CEO Jensen Huang warns China is "not behind" in AI**. CNBC. Disponível em: <https://www.cnbc.com/2025/04/30/nvidia-ceo-jensen-huang-says-china-not-behind-in-ai.html>. Acesso em: 19 nov. 2025.

LEVI-FAUR, David. **From "Big Government" to "Big Governance"?** [s.l.]: Oxford University Press, 2012. Disponível em: <https://academic.oup.com/edited-volume/34384/chapter/291586068>. Acesso em: 19 jan. 2024.

LI, Pengfei; YANG, Jianyi; ISLAM, Mohammad A.; *et al*. Making AI Less "Thirsty": Uncovering and Addressing the Secret Water Footprint of AI Models. 2025. Disponível em: <http://arxiv.org/abs/2304.03271>. Acesso em: 10 nov. 2025.

LI, Yanchao; GEORGHIOU, Luke. Signaling and accrediting new technology: Use of procurement for innovation in China. **Science and Public Policy**, v. 43, n. 3, p. 338–351, 2016.

LIANOS, Ioannis. **Competition Law for the Digital Era: A Complex Systems' Perspective**. Rochester, NY: Centre for Law, Economics and Society - UCL, 2019. (Research Paper Series). Disponível em: <https://papers.ssrn.com/abstract=3492730>. Acesso em: 12 nov. 2025.

LILIAN CUNHA. **Apagão de WhatsApp e cia. traz prejuízo a empresas, que podem processar serviços**. CNN Brasil. Disponível em: <https://www.cnnbrasil.com.br/tecnologia/apagao-de-whatsapp-e-cia-traz-prejuizo-a-empresas-que-podem-processar-servicos/>. Acesso em: 29 out. 2025.

LIMA, Bernardo; NALIN, Carolina. **Governo já traça estratégia para taxar big techs. Veja as alternativas na mesa**. O Globo. Disponível em: <https://oglobo.globo.com/economia/noticia/2025/07/19/governo-ja-traca-estrategia-para-taxar-big-techs-veja-as-alternativas-na-mesa.ghtml>. Acesso em: 15 set. 2025.

LIN, Hause; CZARNEK, Gabriela; LEWIS, Benjamin; *et al*. Persuading voters using human–artificial intelligence dialogues. **Nature**, p. 1–8, 2025.

LIN, Judy. **China invested US$290.8 billion in semiconductor projects between 2021-2022**. DIGITIMES Asia. Disponível em: <https://www.digitimes.com/news/a20230627VL205/china-ic-manufacturing-semiconductor-chips+components.html>. Acesso em: 10 nov. 2025.

LUCCIONI, Sasha. **The mounting human and environmental costs of generative AI**. Ars Technica. Disponível em: <https://arstechnica.com/gadgets/2023/04/generative-ai-is-cool-but-lets-not-forget-its-human-and-environmental-costs/>. Acesso em: 10 nov. 2025.

LUNDBERG, Jonas. Situation awareness systems, states and processes: a holistic framework. **Theoretical Issues in Ergonomics Science**, v. 16, n. 5, p. 447–473, 2015.

LUNDVALL, Bengt-Åke. **Innovation System Research and Policy: Where it came from and where it might go**. [s.l.: s.n.], 2007.

LUNDVALL, Bengt-Åke. National Systems of Innovation: Towards a Theory of Innovation and Interactive Learning. *In*: **The Learning Economy and the Economics of Hope**. [s.l.]: Anthem Press, 2016, p. 85–106. Disponível em: <https://www.jstor.org/stable/j.ctt1hj9zjd.9>. Acesso em: 22 set. 2025.

MA, Aifang. Regulation in pursuit of artificial intelligence (AI) sovereignty: China's mix of restrictive and facilitative modalities. **The African Journal of Information and Communication (AJIC)**, n. 34, p. 1–16, 2024.

MACASKILL, Ewen. WikiLeaks website pulled by Amazon after US political pressure. **WikiLeaks website pulled by Amazon after US political pressure**, 2010. Disponível em: <https://www.theguardian.com/media/2010/dec/01/wikileaks-website-cables-servers-amazon>. Acesso em: 15 set. 2025.

MACASKILL, Ewen; DANCE, Gabriel; CAGE, Feilding; *et al*. **NSA files decoded: Edward Snowden's surveillance revelations explained**. the Guardian. Disponível em: <https://www.theguardian.com/world/interactive/2013/nov/01/snowden-nsa-files-surveillance-revelations-decoded>. Acesso em: 2 dez. 2025.

MAGALHÃES, Larissa; BEN DHAOU, Soumaya. **Open Data and Emerging Technologies: Connecting SDG Performance and Digital Transformation**. [s.l.]: CyberBRICS, 2023. Disponível em: <https://cyberbrics.info/open-data-and-emerging-technologies-connecting-sdg-performance-and-digital-transformation/>. Acesso em: 13 nov. 2025.

MAGEE, Tamlin. **Big tech's support for Trump isn't a moral about-face – it's business**. Raconteur. Disponível em: <https://www.raconteur.net/technology/tech-tribute-trump-oped>. Acesso em: 11 nov. 2025.

MAJONE, Giandomenico. From the Positive to the Regulatory State: Causes and Consequences of Changes in the Mode of Governance on JSTOR. **Journal of Public Policy**, v. 17, n. 2, p. 139–167, .

MALATJI, Masike; TOLAH, Alaa. Artificial intelligence (AI) cybersecurity dimensions: a comprehensive framework for understanding adversarial and offensive AI. **AI and Ethics**, 2024. Disponível em: <https://doi.org/10.1007/s43681-024-00427-4>. Acesso em: 6 jun. 2024.

MARCUS, Gary. Sam Altman's pants are totally on fire. Disponível em: <https://garymarcus.substack.com/p/sam-altmans-pants-are-totally-on>. Acesso em: 16 nov. 2025.

MATOS, Mara. **CNCiber cria grupo de trabalho para avaliar Lei Geral da Cibersegurança - TELETIME News**. Disponível em: <https://teletime.

com.br/09/10/2025/cnciber-cria-grupo-de-trabalho-para-avaliar-lei-geral-da-ciberseguranca/>. Acesso em: 10 nov. 2025.

MAYER, Maximilian; LU, Yen-Chi. Global structures of digital dependence and the rise of technopoles. **New Political Economy**, v. 30, n. 5, p. 755–774, 2025.

MAZZUCATO, Mariana. **O estado empreendedor: desmascarando o mito do setor público vs. privado**. [s.l.]: Penguin-Companhia das Letras, 2021.

MAZZUCATO, Mariana. **O Estado empreendedor: Desmascarando o mito do setor público vs. setor privado**. Trad. Elvira Serapicos. São Paulo: Portfolio-Penguin, 2014.

MAZZUCATO, Mariana. **The Entrepreneurial State**. London: Penguin, 2018.

MAZZUCATO, Mariana. **The Value of Everything**. [s.l.: s.n.], 2019. Disponível em: <https://www.penguin.co.uk/books/280466/the-value-of-everything-by-mazzucato-mariana/9780141980768>. Acesso em: 6 nov. 2025.

MCMORROW, Ryan; WU, Zijing; SEVASTOPULO, Demetri; *et al*. **US warns against using Huawei chips 'anywhere in the world'**. Financial Times. Disponível em: <https://www.ft.com/content/2033b5b3-974d-4d40-8498-1c46d3a8db79>.

MEDEIROS, Breno Pauli; GOLDONI, Luiz Rogério Franco; SILVA, Carla Morena Vitoria Gomes. Brazil. *In*: CHRISTOU, George; VOSSE, Wilhelm; BURTON, Joe; *et al* (Orgs.). **The Palgrave Handbook on Cyber Diplomacy**. Cham: Springer Nature Switzerland, 2025, p. 673–688. Disponível em: <https://link.springer.com/10.1007/978-3-031-93385-1_30>. Acesso em: 10 out. 2025.

MELLO, Gustavo Bernardes. **Governança por missões no Brasil: um olhar sobre os desafios de Coordenação na Nova Indústria Brasil a partir da transformação digital.** Escola Nacional de Administração Pública - Enap, 2025. Disponível em: <https://repositorio.enap.gov.br/handle/1/9159>.

MELO, Ricardo Lacerda de. Soberania Digital e Desenvolvimento: um olhar crítico sobre as possibilidades e limites do Brasil nas tecnologias digitais. Entrevista com José Eduardo Cassiolato. v. 26, n. 3, 2024. Disponível em: <https://periodicos.ufs.br/eptic/article/view/22127/16398>.

MENDO, Marcelo; VIANA, Frederico; PASSOS, Thiago. **Brazil in the global race for rare earths**. Valor Internacional. Disponível em: <https://valorinternational.globo.com/economy/news/2025/09/30/brazil-in-the-global-race-for-rare-earths.ghtml>. Acesso em: 6 nov. 2025.

MENDONÇA, Hudson; PORTELA, Bruno Monteiro; NETO, Adalberto do Rego Maciel. Contrato público de soluções inovadoras: racionalidade fundamental e posicionamento no mix de políticas de inovação que atuam pelo lado da demanda. *In*: **Compras públicas para inovação no Brasil : novas possibilidades legais**. Brasília: IPEA, 2022, p. 467–492. Disponível em: <http://repositorio.ipea.gov.br/handle/11058/11623>.

MERCEDES, Sonia Seger Pereira; RICO, Julieta A. P.; POZZO, Liliana de Ysasa. Uma revisão histórica do planejamento do setor elétrico brasileiro. **Revista USP**, n. 104, p. 13–36, 2015.

META, Mike IsaacMike Isaac has reported on; SINCE 2010, Its Apps. Mark Zuckerberg Defends Embrace of Trump Administration in Meta Q&A. **The New York Times**, 2025. Disponível em: <https://www.nytimes.com/2025/01/30/technology/mark-zuckerberg-meta-trump.html>. Acesso em: 10 out. 2025.

MISRA, Manu; PANDAY, Jyoti; ZINGALES, Nicolo. Applying the CII Framework to DPIs considerations, challenges and opportunities. **T20 Policy Brief**, 2024. Disponível em: <https://hdl.handle.net/10438/36195>. Acesso em: 11 nov. 2025.

MONSERRATE, Steven Gonzalez. The Cloud Is Material: On the Environmental Impacts of Computation and Data Storage. **MIT Case Studies in Social and Ethical Responsibilities of Computing**, n. Winter 2022, 2022. Disponível em: <https://mit-serc.pubpub.org/pub/the-cloud-is-material/release/2>. Acesso em: 11 nov. 2025.

MORGENTHAU, Hans J. **A política entre nações**. [s.l.]: Universidade de Brasilia, 2003.

MOURÃO, Giovanni. O Globo. **Justiça suspende regulamentação de Uber e 99 em Niterói**, 2018. Disponível em: <https://oglobo.globo.com/rio/bairros/justica-suspende-regulamentacao-de-uber-99-em-niteroi-23150962>. Acesso em: 29 out. 2025.

MOZILLA. **Mozilla Investigation: YouTube Algorithm Recommends Videos that Violate the Platform's Very Own Policies**. Mozilla Foundation. Disponível em: <https://www.mozillafoundation.org/en/blog/mozilla-investigation-youtube-algorithm-recommends-videos-that-violate-the-platforms-very-own-policies/>. Acesso em: 4 dez. 2025.

MULHOLLAND, Jessica. **What Obama Did for Tech: Cloud by Default**. GovTech. Disponível em: <https://www.govtech.com/computing/What-Obama-Did-for-Tech-Cloud-by-Default.html>. Acesso em: 6 nov. 2025.

NADIM, Marjan; FLADMOE, Audun. Silencing Women? Gender and Online Harassment. **Social Science Computer Review**, v. 39, n. 2, p. 245–258, 2021.

NASCIMENTO, Henrique Fernandes; SAKAY, Danilo; TORISU, Cristiane Kazuko; *et al*. Desafios e aprendizados na execução de encomenda tecnológica: o registro da experiência no setor espacial brasileiro. *In*: RAUEN, André Tortato (Org.). **Compras públicas para inovação no Brasil : novas possibilidades legais**. Brasília: IPEA, 2022, p. 493–531. Disponível em: <https://repositorio.ipea.gov.br/server/api/core/bitstreams/c5f52657-edb2-40ae-85aa-5c5f4d2196f4/content>. Acesso em: 5 nov. 2025.

NETO, Germano P. Johansson; COSTA, Viviane C. Farias da; GASPAR, Walter Britto. Brazil's Artificial Intelligence Plan (PBIA) of 2024: Enabler of AI sovereignty? **The African Journal of Information and Communication (AJIC)**, n. 34, p. 1–15, 2024.

NETO, José Francisco da Cruz; JARDIM, Alexandre Maniçoba da Rosa Ferraz; SOUZA, Luciana Sandra Bastos de; *et al*. Desertificação: uma visão geral dos processos e conceitos, fundamentados em aplicação de índices orbitais através do sensoriamento remoto. **Research, Society and Development**, v. 10, n. 11, p. e585101119950–e585101119950, 2021.

NEWMAN, Nic; FLETCHER, Richard; ROBERTSON, Craig T.; *et al*. **Reuters Institute digital news report 2024**. [s.l.]: Reuters Institute for the Study of Journalism, 2024. Disponível em: <https://reutersinstitute.politics.ox.ac.uk/digital-news-report/2024>. Acesso em: 10 nov. 2025.

NIC.BR. **Conectividade significativa: propostas para medição e o retrato da população no Brasil**. São Paulo: CGI.br, 2024. (Cadernos NIC.br - Estudos setoriais). Disponível em: <https://cetic.br/media/docs/publicacoes/7/20240415183307/estudos_setoriais-conectividade_significativa.pdf>. Acesso em: 5 fev. 2025.

NIC.BR. **Conectividade significativa: propostas para medição e o retrato da população no Brasil**. São Paulo: CGI.br, 2024. (Cadernos NIC.br - Estudos setoriais). Disponível em: <https://cetic.br/media/docs/publicacoes/7/20240415183307/estudos_setoriais-conectividade_significativa.pdf>. Acesso em: 5 fev. 2025.

NYE, J.S. **O Futuro Do Poder**. Trad. M. Lopes. [s.l.]: BENVIRA, 2012. Disponível em: <https://books.google.com.br/books?id=OSLLuAAACAAJ>.

OATLEY, Thomas. **Toward a political economy of complex interdependence**. Disponível em: <https://journals.sagepub.com/doi/full/10.1177/1354066119846553>. Acesso em: 23 set. 2025.

OFFE, Claus. Governance: An "Empty Signifier"? **Constellations**, v. 16, n. 4, p. 550–562, 2009.

OLLAIK, Leila Giandoni; MEDEIROS, Janann Joslin. Instrumentos governamentais: reflexões para uma agenda de pesquisas sobre implementação de políticas públicas no Brasil. **Revista de Administração Pública**, v. 45, n. 6, p. 1943–1967, 2011.

OPARA-MARTINS, Justice; SAHANDI, Reza; TIAN, Feng. Critical analysis of vendor lock-in and its impact on cloud computing migration: a business perspective. **Journal of Cloud Computing**, v. 5, n. 1, p. 4, 2016.

ORSI, Fabienne; CORIAT, Benjamin. The New Role and Status of Intellectual Property Rights in Contemporary Capitalism. **Competition & Change**, v. 10, n. 2, p. 162–179, 2006.

PACHECO, Rodrigo. **PL 2338/2023**. Senado Federal. Disponível em: <https://www25.senado.leg.br/web/atividade/materias/-/materia/157233>. Acesso em: 10 nov. 2025.

PAGE, Amba Kakarchive; PAGE, Sarah Myers Westarchive; PAGE, Meredith Whittakerarchive. **Make no mistake—AI is owned by Big Tech**. MIT Technology

Review. Disponível em: <https://www.technologyreview.com/2023/12/05/1084393/make-no-mistake-ai-is-owned-by-big-tech/>. Acesso em: 16 nov. 2025.

PAGE, Will Douglas Heavenarchive. **How AGI became the most consequential conspiracy theory of our time**. MIT Technology Review. Disponível em: <https://www.technologyreview.com/2025/10/30/1127057/agi-conspiracy-theory-artifcial-general-intelligence/>. Acesso em: 16 nov. 2025.

PAK, Aidan. The CUDA Advantage: How NVIDIA Came to Dominate AI And The Role of GPU Memory in Large-Scale Model Training. Disponível em: <https://medium.com/@aidanpak/the-cuda-advantage-how-nvidia-came-to-dominate-ai-and-the-role-of-gpu-memory-in-large-scale-model-e0cdb98a14a0>. Acesso em: 10 nov. 2025.

PARSHEERA, Smriti. Net neutrality in India: From rules to enforcement. *In*: BELLI, Luca; PAHWA, Nikhil; MANZAR, Osama (Orgs.). **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. Disponível em: <https://cyberbrics.info/the-value-of-internet-openness-in-times-of-crisis/>. Acesso em: 3 mar. 2023.

PARSHEERA, Smriti. Stack is the New Black?: Evolution and Outcomes of the 'India-Stackification' Process. **Computer Law & Security Review**, v. 52, p. 105947, 2024.

PAULINO, Isabela. **Sebrae Startups completa dois anos com 18 mil startups cadastradas e mais de 100 mil atendimentos realizados**. Anprotec. Disponível em: <https://anprotec.org.br/site/2025/06/sebrae-startups-completa-dois-anos-com-18-mil-startups-cadastradas-e-mais-de-100-mil-atendimentos-realizados/>. Acesso em: 18 nov. 2025.

PEREIRA, Laurence Duarte Araújo; JÚNIOR, José Luiz de Moura Faleiros. Regulação das plataformas digitais no Brasil e a defesa da soberania nacional. **Revista de Ciências do Estado**, v. 9, n. 1, p. 1–22, 2024.

PEREZ, C. Technological revolutions and techno-economic paradigms. **Cambridge Journal of Economics**, v. 34, n. 1, p. 185–202, 2010.

PERSILY, Nathaniel; TUCKER, Joshua A. (Orgs.). **Social Media and Democracy**. Cambridge: Cambridge University Press, 2020. (SSRC Anxieties of Democracy). Disponível em: <https://www.cambridge.org/core/books/social-media-and-democracy/E79E2BBF03C18C3A56A5CC393698F117>. Acesso em: 15 nov. 2025.

PHAM, Sherisse. **US move against Huawei could slow the global rollout of 5G**. CNN Business. Disponível em: <https://www.cnn.com/2019/05/16/tech/huawei-us-5g-rollout>. Acesso em: 12 nov. 2025.

PIMENTEL, Vitor Paiva; PARANHOS, Julia; CHIARINI, Tulio. Desdobramentos da nova lei de licitações nas parcerias para o desenvolvimento produtivo de saúde. *In*: RAUEN, André Tortato (Org.). **Compras públicas para inovação no Brasil: novas possibilidades legais**. Brasília: IPEA, 2022. Disponível em: <https://repositorio.ipea.gov.br/server/api/core/bitstreams/c5f52657-edb2-40ae-85aa-5c5f4d2196f4/content>.

PINHEIRO, Camilla; COSTA, Edwaldo. AS FAKE NEWS SOBRE O PL DAS FAKE NEWS: MANIPULAÇÃO ALGORÍTMICA NO DEBATE SOBRE REGULAÇÃO DAS PLATAFORMAS DIGITAIS NO BRASIL. **ARACÊ**, v. 7, n. 6, p. 30432–30455, 2025.

PINTO, Renata Ávila. **Digital Sovereignty or Digital Colonialism? New tensions of privacy, security and national policies. | EBSCOhost**. Disponível em: <https://openurl.ebsco.com/contentitem/gcd:133035238?sid=ebsco:plink:crawler&id=ebsco:gcd:133035238>. Acesso em: 11 mar. 2025.

PITRON, Guillame. The Geopolitics of the Rare-Metals Race. **The Washington Quarterly**, v. 45, n. 1, p. 135–150, 2022.

POHLMANN, Kim. Austria's Ministry of Economy takes decisive steps toward digital sovereignty. Disponível em: <https://nextcloud.com/blog/austrias-ministry-of-economy-takes-decisive-steps-toward-digital-sovereignty/>. Acesso em: 6 nov. 2025.

POPIEL, Pawel; VASUDEVAN, Krishnan. Platform frictions, platform power, and the politics of platformization. **Information, Communication & Society**, v. 27, n. 10, p. 1867–1883, 2024.

PORTER, Michael E. How Competitive Forces Shape Strategy. **Harvard Business Review**, v. 57, 1979. Disponível em: <https://hbr.org/1979/03/how-competitive-forces-shape-strategy>. Acesso em: 12 nov. 2025.

PRESTES, Elisa Gomes. The digital geopolitics of 5G: elements to understand the Chinese technological development of the fifth generation of mobile telephony. **GEOUSP**, v. 26, p. e194823, 2022.

PROCHNIK, Victor; LABRUNIE, Mateus Lino; SILVEIRA, Marco Antonio; *et al*. A política da política industrial: o caso da Lei de Informática. **Revista Brasileira de Inovação**, v. 14, p. 133–152, 2015.

PUBLISHED, Jowi Morales. **'China is going to win the AI race' — Nvidia CEO Jensen Huang decries the price of electricity in the US, contrasts it with China's subsidized pricing**. Tom's Hardware. Disponível em: <https://www.tomshardware.com/tech-industry/artificial-intelligence/china-is-going-to-win-the-ai-race-nvidia-ceo-jensen-huang-decries-the-price-of-electricity-in-the-us-contrasts-it-with-chinas-subsidized-pricing>. Acesso em: 19 nov. 2025.

QUINELATO, João. **Marco Legal das Startups: avanços e retrocessos**. JOTA Jornalismo. Disponível em: <https://www.jota.info/coberturas-especiais/inova-e-acao/marco-legal-das-startups-avancos-e-retrocessos>. Acesso em: 19 nov. 2025.

RAUEN, André Tortato. COMPRAS PÚBLICAS PARA INOVAÇÃO NO BRASIL: O PODER DA DEMANDA PÚBLICA. *In*: **Compras públicas para inovação no Brasil : novas possibilidades legais**. Brasília: IPEA, 2022, p. 15–38. Disponível em: <https://repositorio.ipea.gov.br/server/api/core/bitstreams/c5f52657-edb2-40ae-85aa-5c5f4d2196f4/content>.

RAUEN, André Tortato. Concursos para inovação: como a licitação na modalidade concurso pode estimular o desenvolvimento e a introdução de soluções no mercado brasileiro. *In*: RAUEN, André Tortato (Org.). **Compras públicas para inovação no Brasil : novas possibilidades legais**. Brasília: IPEA, 2022, p. 431–466. Disponível em: <https://repositorio.ipea.gov.br/server/api/core/bitstreams/c5f52657-edb2-40ae-85aa-5c5f4d2196f4/content>. Acesso em: 5 nov. 2025.

RAUEN, André Tortato. MAPEAMENTO DAS COMPRAS FEDERAIS DE P&D SEGUNDO USO DA LEI DE INOVAÇÃO NO PERÍODO 2010-2015. *In*: RAUEN, André Tortato (Org.). **Políticas de inovação pelo lado da demanda no Brasil**. Brasília: IPEA, 2022, p. 481.

RESNICK, Mitchel; BERG, Robbie; EISENBERG, Michael. Beyond Black Boxes: Bringing Transparency and Aesthetics Back to Scientific Investigation. **Journal of the Learning Sciences**, v. 9, n. 1, p. 7–30, 2000.

RIBEIRO, Márcio Moretto; ORTELLADO, Pablo. O que são e como lidar com as notícias falsas. **Sur - Revista Internacional de Direitos Humanos**, v. 15, n. 27, p. 71–83, 2018.

RICHTER, Felix. **Infographic: Big Three Hold Dominant Lead in Accelerating Cloud Market**. Statista Daily Data. Disponível em: <https://www.statista.com/chart/18819/worldwide-market-share-of-leading-cloud-infrastructure-service-providers>. Acesso em: 5 mar. 2026.

RIKAP, Cecilia. **Big Tech: Not Only Market But Also Knowledge and Information Gatekeepers**. Institute for New Economic Thinking. Disponível em: <https://www.ineteconomics.org/perspectives/blog/big-tech-not-only-market-but-also-knowledge-and-information-gatekeepers>. Acesso em: 19 set. 2025.

RIKAP, Cecilia. **Dynamics of Corporate Governance Beyond Ownership in AI**. Common Wealth. Disponível em: <https://www.common-wealth.org/publications/dynamics-of-corporate-governance-beyond-ownership-in-ai>. Acesso em: 5 out. 2024.

RIKAP, Cecilia. **Dynamics of Corporate Governance Beyond Ownership in AI**. Disponível em: <https://www.common-wealth.org/publications/dynamics-of-corporate-governance-beyond-ownership-in-ai>. Acesso em: 19 set. 2025.

RIKAP, Cecilia. Varieties of corporate innovation systems and their interplay with global and national systems: Amazon, Facebook, Google and Microsoft's strategies to produce and appropriate artificial intelligence. **Review of International Political Economy**, v. 31, n. 6, p. 1735–1763, 2024.

ROBERTO, José; GERALDO, Murilo Afonso; BIASOTO JR, Viana. Economia digital, micronegócios, máxima produtividade. **Revista Conjuntura Econômica**, v. 74, n. 2, p. 22–25, 2020.

RODRIGUES, Alex. **Notificada, Google retira link para texto contra PL das Fake News**. Agência Brasil. Disponível em: <https://agenciabrasil.ebc.com.br/geral/noticia/2023-05/notificada-google-retira-link-para-texto-contra-pl-das-fake-news>. Acesso em: 10 nov. 2025.

ROMEU, Artur. Big tech's attempts to weaken information space regulations worldwide exposed by new cross-country investigation supported by RSF. **Reporters Without Borders**, 2025. Disponível em: <https://rsf.org/en/big-tech-s-attempts-weaken-information-space-regulations-worldwide-exposed-new-cross-country>. Acesso em: 10 nov. 2025.

ROVENSKAYA, Elena; IVANOV, Alexey; HATHIARI, Sarah; *et al*. An ecological perspective to master the complexities of the digital economy. **npj Complexity**, v. 2, n. 1, p. 16, 2025.

SALAMON, Lester M. **The Tools of Government: A Guide to the New Governance**. Oxford: Oxford University Press, USA, 2002.

SÁNCHEZ, C.H. Export control on cybertechnologies: An analysis of the Wassenaar Agreement and its implications for cybersecurity. **Revista Chilena de Derecho y Tecnologia**, v. 7, n. 1, p. 61–78, 2018.

SANTOS, Naedja Karla Petrucio dos; ALMEIDA, Tiago Oliveira de; RAMALHO, Ângela Maria Cavalcanti; *et al*. Revolução digital e mercado de trabalho: da uberização às plataformas digitais. **Caderno Pedagógico**, v. 21, n. 10, p. e9933–e9933, 2024.

SAURA GARCÍA, Carlos. Digital expansionism and big tech companies: consequences in democracies of the European Union. **Humanities and Social Sciences Communications**, v. 11, n. 1, p. 448, 2024.

SCHMID, Stefka; LAMBACH, Daniel; DIEHL, Carlo; *et al*. Arms Race or Innovation Race? Geopolitical AI Development. **Geopolitics**, v. 0, n. 0, p. 1–30, 2025.

SCOFIELD, Laura; VIANA, Natalia. **Como as Big Techs mataram o PL das Fake News**. Agência Pública. Disponível em: <https://apublica.org/2025/09/como-as-big-techs-mataram-o-pl-das-fake-news/>. Acesso em: 10 nov. 2025.

SENGUPTA, Amrita; BARBOSA, Alexandre Costa; SAMDUB, Mila T. Understanding interrelationships between AI and digital public infrastructure (DPI) in India and Brazil. **The African Journal of Information and Communication (AJIC)**, n. 35, p. 1–11, 2025.

SHAPERO, Julia. **Nvidia navigates US-China "tightrope" in AI chip sales**. The Hill. Disponível em: <https://thehill.com/policy/technology/5441397-nvidia-us-china-ai-chips/>. Acesso em: 27 ago. 2025.

SHAXSON, Nicholas; ROCK, Brianna; BLANKERTZ, Aline. Google's Hidden Empire. 2025. Disponível em: <https://arxiv.org/abs/2511.02931>.

SHCHERBOVICH, Andrey. Data Protection and Cybersecurity Legislation of the Russian Federation in the Context of the "Sovereignization" of the Internet in Russia. *In*: BELLI, Luca (Org.). **CyberBRICS: Cybersecurity Regulations in the BRICS Countries**. Cham: Springer International Publishing, 2021, p. 67–131. Disponível em: <https://doi.org/10.1007/978-3-030-56405-6_3>. Acesso em: 29 set. 2025.

SHIONA MCCALLUM, BBC. **WhatsApp diz que nenhum governo o fará enfraquecer sua criptografia**. G1. Disponível em: <https://g1.globo.com/tecnologia/noticia/2022/07/30/whatsapp-diz-que-nenhum-governo-o-fara-enfraquecer-sua-criptografia.ghtml>. Acesso em: 29 out. 2025.

SILVA, Ergon Cugler de Moraes; ROCHA, Isabela; VAZ, Carlos; *et al*. **Contratos, Códigos e Controle A Influência das Big Techs no Estado Brasileiro**. São Paulo: [s.n.], 2025. Disponível em: <https://bit.ly/contratos-big-techs>.

SPADONI, Pedro. STF, Anatel, Banco Central: o que incomoda as big techs no Brasil. Disponível em: <https://olhardigital.com.br/2025/08/21/pro/porque-big-techs-reclamam-de-stf-anatel-banco-central-no-brasil/>. Acesso em: 15 set. 2025.

SRG. **Cloud Market Gets its Mojo Back; AI Helps Push Q4 Increase in Cloud Spending to New Highs**. Synergy Research Group. Disponível em: <https://www.srgresearch.com/articles/cloud-market-gets-its-mojo-back-q4-increase-in-cloud-spending-reaches-new-highs>. Acesso em: 13 nov. 2025.

STOKER, Gerry. Governance as theory: five propositions. **International Social Science Journal**, v. 68, n. 227–228, p. 15–24, 2018.

STRANGE, Susan. **States and markets**. 1. ed. London: Continuum, 1988. Disponível em: <https://www.goodreads.com/en/book/show/1072754.States_and_Markets>. Acesso em: 10 nov. 2025.

SUNKEL, Oswaldo. **Capitalismo Transnacional y desintegración nacional en américa latina**. Buenos Aires: Ediciones Nueva Visión, 2025. (Colección Fichas, 6). Disponível em: <https://web.archive.org/web/20250810163525/https://repositorio.esocite.la/830/>. Acesso em: 10 nov. 2025.

TECMUNDO. **Vivo dá um ano de assinatura gratuita da IA Perplexity Pro aos clientes**. TecMundo: Tudo sobre Tecnologia, Entretenimento, Ciência e Games. Disponível em: <https://www.tecmundo.com.br/software/294653-vivo-disponibiliza-1-ano-assinatura-gratuita-ia-perplexity-pro.htm>. Acesso em: 10 out. 2025.

TEECE, David J. Next-generation competition: New concepts for understanding how innovation shapes competition and policy in the digital economy. **JL Econ. & Pol'y**, v. 9, p. 97, 2012.

THE WHITE HOUSE. **Defending American Companies and Innovators From Overseas Extortion and Unfair Fines and Penalties**. The White House. Disponível em: <https://www.whitehouse.gov/presidential-actions/2025/02/defending-american-companies-and-innovators-from-overseas-extortion-and-unfair-fines-and-penalties/>. Acesso em: 12 nov. 2025.

TOI, Staff. Trump's sanctions on ICC prosecutor said to have halted tribunals work. 2025. Disponível em: <https://www.timesofisrael.com/trumps-sanctions-on-icc-prosecutor-said-to-have-halted-tribunals-work/>. Acesso em: 15 set. 2025.

TONG, Xin; WAN, Xiaomeng. National industrial investment fund and China's integrated circuit industry technology innovation. **Journal of Innovation & Knowledge**, v. 8, n. 1, p. 100319, 2023.

TUSIKOV, Natasha. **Chokepoints: Global Private Regulation on the Internet**. [s.l.]: Univ of California Press, 2016.

U.S. CONGRESS. Clarifying Lawful Overseas Use of Data Act (CLOUD Act). Disponível em: <https://www.congress.gov/bill/115th-congress/house-bill/4943>. Acesso em: 15 set. 2025.

UYARRA, Elvira; FLANAGAN, Kieron. Understanding the Innovation Impacts of Public Procurement. **European Planning Studies**, v. 18, n. 1, p. 123–143, 2010.

VAIDHYANATHAN, Siva. **Antisocial Media: How Facebook Disconnects Us and Undermines Democracy**. [s.l.]: Oxford University Press, 2022. Disponível em: <https://doi.org/10.1093/oso/9780190056544.001.0001>. Acesso em: 15 nov. 2025.

VALOR ECONÔMICO. **Por que o Telegram foi suspenso no Brasil? Entenda**. Valor Econômico. Disponível em: <https://valor.globo.com/empresas/noticia/2023/04/26/por-que-o-telegram-foi-suspenso-no-brasil-entenda.ghtml>. Acesso em: 29 out. 2025.

VIPRA, Jai. Towards AI sovereignty: The good, the bad, and the ugly of AI policy in India. **The African Journal of Information and Communication (AJIC)**, n. 35, p. 1–11, 2025.

VITTORAZZI, Davi. **STF forma tese para responsabilizar big techs por conteúdos de terceiros**. CNN Brasil. Disponível em: <https://www.cnnbrasil.com.br/politica/stf-forma-tese-para-responsabilizar-big-techs-por-conteudos-de-terceiros/>. Acesso em: 15 set. 2025.

WALTZ, Kenneth. **Man, the State, and War: A Theoretical Analysis**. [s.l.]: Columbia University Press, 2018. Disponível em: <https://www.degruyterbrill.com/document/doi/10.7312/walt18804/html>. Acesso em: 15 set. 2025.

WALTZ, Kenneth N. Structural Realism after the Cold War. **International Security**, v. 25, n. 1, p. 5–41, 2000.

WANG, Wayne Wei. China's digital transformation: Data-empowered state capitalism and social governmentality. **The African Journal of Information and Communication (AJIC)**, n. 31, 2023. Disponível em: <https://ajic.wits.ac.za/article/view/16296>. Acesso em: 6 nov. 2025.

WANG, Wayne Wei. Contextualizing Personal Information: Privacy's Post-Neoliberal Constitutionalism and Its Heterogeneous Imperfections in China. Disponível em: <https://cyberbrics.info/contextualizing-personal-information-privacys-post-neoliberal-constitutionalism-and-its-heterogeneous-imperfections-in-china/>. Acesso em: 11 nov. 2025.

WATANABE, Phillippe; BOTTALLO, Ana. **Programa de R$ 1 bilhão para repatriar cientistas é criticado por pesquisadores**. Jornal de Brasília. Disponível em: <https://jornaldebrasilia.com.br/noticias/politica-e-poder/programa-de-r-1-bilhao-para-repatriar-cientistas-e-criticado-por-pesquisadores/>. Acesso em: 18 nov. 2025.

WEISS, Linda; THURBON, Elizabeth. The Business of Buying American: Public Procurement as Trade Strategy in the USA. **Review of International Political Economy**, v. 13, n. 5, p. 701–724, 2006.

WEN, Wen; ZHU, Feng. How Do Complementors Respond to the Threat of Platform Owner Entry? Evidence from the Mobile App Market. **SSRN Electronic Journal**, 2016. Disponível em: <http://www.ssrn.com/abstract=2848533>. Acesso em: 10 nov. 2025.

WERNER, Deborah; LAZARO, Lira Luz Benites. The policy dimension of energy transition: The Brazilian case in promoting renewable energies (2000–2022). **Energy Policy**, v. 175, p. 113480, 2023.

WESTHUIZEN, Janis van der. Huawei or the US way? Why Brazil and South Africa did not securitize 5G. **Revista Brasileira de Política Internacional**, v. 67, p. e016, 2024.

WIDDER, David Gray; WEST, Sarah; WHITTAKER, Meredith. Open (For Business): Big Tech, Concentrated Power, and the Political Economy of Open AI. 2023. Disponível em: <https://papers.ssrn.com/abstract=4543807>. Acesso em: 5 set. 2023.

WINTOUR, Patrick. **US defence secretary warns Huawei 5G will put alliances at risk**. The Guardian. Disponível em: <https://www.theguardian.com/us-news/2020/feb/15/us-defence-secretary-warns-us-alliances-at-risk-from-huawei-5g>. Acesso em: 27 ago. 2025.

WU, Tim. **The Age of Extraction: How Tech Platforms Conquered the Economy and Threaten Our Future Prosperity**. [s.l.]: Knopf, 2025.

XIANG, Chloe. **GitHub Users File a Class-Action Lawsuit Against Microsoft for Training an AI Tool With Their Code**. Vice. Disponível em: <https://www.vice.com/en/article/bvm3k5/github-users-file-a-class-action-lawsuit-against-microsoft-for-training-an-ai-tool-with-their-code>. Acesso em: 21 nov. 2023.

XINHUA NEWS AGENCY. **Decision of the Central Committee of the Communist Party of China on Several Major Issues Concerning Upholding and Improving the Socialist System with Chinese Characteristics and Promoting the Modernization of the National Governance System and Governance Capacity**. Gov.CN. Disponível em: <https://www.gov.cn/zhengce/2019-11/05/content_5449023.htm>. Acesso em: 11 nov. 2025.

ZHANG, Pengxiang; CHEN, Liang; YANG, Yang; *et al*. Marching to the Beat: The Role of Complementor Alignment in the Architectural Evolution of Ecosystems. **Journal of Management**, p. 01492063251368267, 2025.

ZHU, Feng; IANSITI, Marco. Why Some Platforms Thrive and Others Don't. **Harvard Business Review**, v. 97, p. 118, 2019.

ZHU, Feng; LIU, Qihong. Competing with complementors: An empirical look at Amazon.com. **Strategic Management Journal**, v. 39, n. 10, p. 2618–2642, 2018.

ZINGALES, Nicolo. **Open Source AI: um conceito à procura da sua definição**. JOTA Jornalismo. Disponível em: <https://www.jota.info/opiniao-e-analise/colunas/ia-regulacao-democracia/open-source-ai-um-conceito-a-procura-da-sua-definicao>. Acesso em: 11 nov. 2025.

ZINGALES, Nicolo; AZEVEDO, Paula Farani de. **A aplicação do direito antitruste em ecossistemas digitais: desafios e propostas**. Rio de Janeiro:

FGV Direito Rio, 2022. Disponível em: <http://bibliotecadigital.fgv.br:80/dspace/handle/10438/32889>. Acesso em: 3 maio 2023.

ZINGALES, Nicolo; FARANI DE AZEVEDO, Paula. Direito antitruste e ecossistemas digitais: mapeando o debate. *In*: ZINGALES, Nicolo; FARANI DE AZEVEDO, Paula (Orgs.). Rio de Janeiro: FGV Editora, 2022, p. 13–46.

ZINGALES, Nicolo; RENZETTI, Bruno. Digital Platform Ecosystems and Conglomerate Mergers: A Review of the Brazilian Experience. **World Competition**, v. 45, n. 4, 2022. Disponível em: <https://kluwerlawonline.com/api/Product/CitationPDFURL?file=Journals\WOCO\WOCO2022021.pdf>. Acesso em: 4 dez. 2025.

ZINGALES, Nicolo; RODRIGUES, ISABEL CRISTINA VELOSO DE OLIVEIRA; COUTO, Natália de Macedo; *et al*. Análise de obrigações de transparência das plataformas de rede social: evidências empíricas no Brasil. **Revista de Direito Econômico e Socioambiental**, v. 17, n. 1, 2026. Disponível em: <https://doi.org/10.7213/rev.dir.econ.soc.v17i1.32604>. Acesso em: 9 dez. 2026.

ZUBOFF, Shoshana. **The age of surveillance capitalism: the fight for a human future at the new frontier of power**. First trade paperback edition. New York, NY: PublicAffairs, 2020.

A Proposed Framework for a "Buy European" Regulation of Strategic Digital Procurement.

About RISC-V. Disponível em: <https://riscv.org/about/>. Acesso em: 19 nov. 2025.

About Universal and Meaningful Connectivity. Disponível em: <https://www.itu.int/itu-d/sites/projectumc/home/aboutumc/>. Acesso em: 10 nov. 2025.

Aláfia Lab | Desigualdades informativas e polarização política. Disponível em: <https://alafialab.org/projeto/desigualdades-informativas-e-polarizacao-politica/>. Acesso em: 10 nov. 2025.

Army Launches Detachment 201: Executive Innovation Corps to Drive Tech Transformation. www.army.mil. Disponível em: <https://www.

army.mil/article/286317/army_launches_detachment_201_executive_innovation_corps_to_drive_tech_transformation>. Acesso em: 10 out. 2025.

Autodiagnóstico - iGOVSISP. Governo Digital. Disponível em: <https://www.gov.br/governodigital/pt-br/estrategias-e-governanca-digital/sisp/autodiagnostico-igovsisp/autodiagnostico>. Acesso em: 25 nov. 2025.

Big AI: Cloud infrastructure dependence and the industrialisation of artificial intelligence. Disponível em: <https://journals.sagepub.com/doi/epdf/10.1177/20539517241232630?src=getftr&utm_source=tfo&getft_integrator=tfo>. Acesso em: 25 set. 2025.

Brazil rises in international cybersecurity ranking. Serviços e Informações do Brasil. Disponível em: <https://www.gov.br/en/government-of-brazil/latest-news/2022/brazil-rises-in-international-cybersecurity-ranking>. Acesso em: 10 nov. 2025.

TUDO CELULAR. **Claro fecha parceria com OpenAI para incluir ChatGPT em planos fixos e móveis**. Disponível em: <https://www.tudocelular.com/mercado/noticias/n239790/claro-parceria-openai-chatgpt-beneficio-planos.html>. Acesso em: 10 out. 2025.

Community networks - the Internet by the people, for the people.1.1.

Criteria catalogue C5. Federal Office for Information Security. Disponível em: <https://www.bsi.bund.de/EN/Themen/Unternehmen-und-Organisationen/Informationen-und-Empfehlungen/Empfehlungen-nach-Angriffszielen/Cloud-Computing/Kriterienkatalog-C5/kriterienkatalog-c5.html?nn=909536>. Acesso em: 10 nov. 2025.

Cybersecurity Collaboration Center. Disponível em: <https://www.nsa.gov/About/Cybersecurity-Collaboration-Center/>. Acesso em: 6 nov. 2025.

Da Estrutura A Funcao: Novos Estudos de Teoria do Direito – Bobbio Norberto – Touché Livros. Disponível em: <https://www.touchelivros.com.br/da-estrutura-a-funcao-novos-estudos-de-teoria-do-direito/>. Acesso em: 22 out. 2025.

Data Center Map - Colocation, Cloud and Connectivity. Disponível em: <https://www.datacentermap.com/>. Acesso em: 12 nov. 2025.

DeepSeek-R1 Release | DeepSeek API Docs. Disponível em: <https://api-docs.deepseek.com/news/news250120>. Acesso em: 7 nov. 2025.

Donald Trump is trying to silence his critics. He will fail. **The Economist**, 2025. Disponível em: <https://www.economist.com/leaders/2025/09/25/donald-trump-is-trying-to-silence-his-critics-he-will-fail>. Acesso em: 7 out. 2025.

Embedded Autonomy | Princeton University Press. Disponível em: <https://press.princeton.edu/books/paperback/9780691037363/embedded-autonomy>. Acesso em: 6 nov. 2025.

Emotional risks of AI companions demand attention. **Nature Machine Intelligence**, v. 7, n. 7, p. 981–982, 2025.

EPSTEIN, Robert. **Why Google Poses a Serious Threat to Democracy, and How to End That Threat**. AIBRT, 16 jun. 2019. Disponível em: <https://www.judiciary.senate.gov/imo/media/doc/Epstein%20Testimony.pdf>. Acesso em: 15 nov. 2025.

European Union Cloud Sovereignty Framework Version 1.2.1 – Oct. 2025.

Examining China's Grand Strategy For RISC-V - Jamestown. Disponível em: <https://jamestown.org/examining-chinas-grand-strategy-for-risc-v/>. Acesso em: 19 nov. 2025.

Foreign Intelligence Surveillance Act. Disponível em: <https://irp.fas.org/agency/doj/fisa/>. Acesso em: 9 out. 2025.

Friends for sale: the rise and risks of AI companions. Disponível em: <https://www.adalovelaceinstitute.org/blog/ai-companions/>. Acesso em: 6 dez. 2025.

Governance, uses, sovereignty, RGPD, cyber risks: how do local authorities manage their data? - Labo. Disponível em: <https://labo.societenumerique.gouv.fr/en/articles/governance-uses-sovereignty-rgpd-risks-cyber-how-communities-manage-their-data/>. Acesso em: 24 set. 2025.

Handbook for Cyber Stress Tests | ENISA. Disponível em: <https://www.enisa.europa.eu/publications/handbook-for-cyber-stress-tests>. Acesso em: 3 dez. 2025.

Home. Conecta Startup Brasil. Disponível em: <https://conectastartupbrasil.org.br/>. Acesso em: 18 nov. 2025.

How AI Is Transforming Data Centers and Ramping Up Power Demand. Disponível em: <https://www.goldmansachs.com/insights/articles/how-ai-is-transforming-data-centers-and-ramping-up-power-demand>. Acesso em: 16 nov. 2025.

Huawei: Por que os EUA consideram a gigante chinesa de tecnologia uma ameaça à segurança nacional. 2018. Disponível em: <https://www.bbc.com/portuguese/internacional-46510746>. Acesso em: 15 set. 2025.

India Stack. Disponível em: <https://indiastack.org/>. Acesso em: 25 set. 2025.

InovAtiva Brasil. InovAtiva. Disponível em: <https://www.inovativa.online/inovativa-brasil/>. Acesso em: 18 nov. 2025.

Kylin (operating system). *In*: **Wikipedia**. [s.l.: s.n.], 2025. Disponível em: <https://en.wikipedia.org/w/index.php?title=Kylin_(operating_system)&oldid=1315406804>. Acesso em: 19 nov. 2025.

Kylin_OS/index. Disponível em: <https://web.archive.org/web/20040926085248/http://www.kylin.org.cn/>. Acesso em: 19 nov. 2025.

Lonely? Meta CEO Mark Zuckerberg's got you covered with AI friends. **The Economic Times**, 2025. Disponível em: <https://economictimes.indiatimes.com/news/international/global-trends/lonely-meta-ceo-mark-zuckerbergs-got-you-covered-with-ai-friends/articleshow/120846982.cms?from=mdr>. Acesso em: 6 dez. 2025.

MADE IN CHINA 2025 The making of a high-tech superpower and consequences for industrial countries.

MCom libera R$ 1,5 bilhão do Funttel para BNDES e Finep financiarem inovação em telecom até 2027. Tele.Sintese. Disponível em: <https://

telesintese.com.br/mcom-libera-r-15-bilhao-do-funttel-para-bndes-e-finep-financiarem-inovacao-em-telecom-ate-2027/>. Acesso em: 6 nov. 2025.

Meaningful Connectivity. Disponível em: <https://globaldigitalinclusion.org/our-work/meaningful-connectivity/>. Acesso em: 10 nov. 2025.

Meta pretende usar chats com IA para anunciar produtos. CNN Brasil. Disponível em: <https://www.cnnbrasil.com.br/tecnologia/meta-pretende-usar-chats-com-ia-para-anunciar-produtos/>. Acesso em: 10 out. 2025.

Microsoft allegedly blocked the email of the Chief Prosecutor of the International Criminal Court. 2025. Disponível em: <https://dig.watch/updates/microsoft-allegedly-blocked-the-email-of-the-chief-prosecutor-of-the-international-criminal-court>. Acesso em: 15 set. 2025.

Ministry of Commerce Notice 2024 No. 46: Notice Concerning Strengthening Controls on Exports of Relevant Dual-Use Items to the United States. Disponível em: <https://cset.georgetown.edu/publication/china-rare-earth-export-ban/>. Acesso em: 26 nov. 2025.

N° 82 - Novembre 2025. Arcep. Disponível em: <https://www.arcep.fr/newsletters/le-post-new/n-82-novembre-2025.html>. Acesso em: 13 nov. 2025.

Network self-determination: When building the Internet becomes a right. 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: 25 set. 2025.

Neutralidade da rede, o zero-rating e o Marco Civil da Internet. vLex. Disponível em: <https://vlex.com.br/vid/neutralidade-da-rede-zero-800704285>. Acesso em: 15 nov. 2025.

Neutralidade de rede e ordem econômica. Omci.gov.br. Disponível em: <https://www.omci.org.br/jurisprudencia/207/neutralidade-de-rede-e-ordem-economica/>. Acesso em: 15 nov. 2025.

Opinião: IA generativa "grátis" é a nova fronteira da colonização digital. Folha de S.Paulo. Disponível em: <https://www1.folha.uol.com.br/tec/2025/09/ia-generativa-gratis-e-a-nova-fronteira-da-colonizacao-digital.shtml>. Acesso em: 5 mar. 2026.

(PDF) Rethinking Technology Stack Selection with AI Coding Proficiency. ResearchGate. Disponível em: <https://www.researchgate.net/publication/395526006_Rethinking_Technology_Stack_Selection_with_AI_Coding_Proficiency>. Acesso em: 8 out. 2025.

PIIE Briefing 21-5: Scoring 50 years of US industrial policy, 1970-2020. Disponível em: <https://www.piie.com/sites/default/files/documents/piieb21-5.pdf>. Acesso em: 6 nov. 2025.

PNAD Contínua TIC 2016: 94,2% das pessoas que utilizaram a Internet o fizeram para trocar mensagens | Agência de Notícias. Agência de Notícias - IBGE. 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: 14 out. 2025.

Portal da Câmara dos Deputados. Disponível em: <https://www2.camara.leg.br/legin/fed/decret/2004/decreto-5156-26-julho-2004-533126-publicacaooriginal-16208-pe.html>. Acesso em: 2 dez. 2025.

Positivo Servers industrializa servidores para supercomputador Pégaso. Exame. Disponível em: <https://exame.com/bussola/positivo-servers-industrializa-servidores-para-supercomputador-pegaso/>. Acesso em: 6 nov. 2025.

Relatório Seminário Pilha IA Soberana.

SAP and OpenAI partner to launch sovereign 'OpenAI for Germany'. Disponível em: <https://openai.com/global-affairs/openai-for-germany/>. Acesso em: 13 nov. 2025.

SecNumCloud pour les fournisseurs de services Cloud | ANSSI. Disponível em: <https://cyber.gouv.fr/secnumcloud-pour-les-fournisseurs-de-services-cloud>. Acesso em: 10 nov. 2025.

SINAPAD - Sistema Nacional de Processamento de Alto Desempenho. Disponível em: <https://www.lncc.br/sinapad/>. Acesso em: 2 dez. 2025.

Sovereignty-as-a-service: How big tech companies co-opt and redefines digital sovereignty. Disponível em: <https://journals.sagepub.com/doi/epub/10.1177/01634437251395003>. Acesso em: 17 nov. 2025.

The New Politics of Interdependence - Henry Farrell, Abraham Newman, 2015. Disponível em: <https://journals.sagepub.com/doi/10.1177/0010414014542330>. Acesso em: 26 nov. 2025.

The Open Source AI Definition – 1.0. Disponível em: <https://opensource.org/ai/open-source-ai-definition/>. Acesso em: 19 nov. 2025.

The Society for Worldwide Interbank Financial Telecommunication (SWIFT): Cooperative governance for network innovation, standards, and community. Routledge & CRC Press. Disponível em: <https://www.routledge.com/The-Society-for-Worldwide-Interbank-Financial-Telecommunication-SWIFT-Cooperative-governance-for-network-innovation-standards-and-community/Scott-Zachariadis/p/book/9780415631648>. Acesso em: 26 nov. 2025.

Towards a Sovereign Digital Infrastructure of Commons.

Trump's sanctions on ICC prosecutor have halted tribunal's work. AP News. Disponível em: <https://apnews.com/article/icc-trump-sanctions-karim-khan-court-a4b4c02751ab84c09718b1b95cbd5db3>. Acesso em: 10 out. 2025.

Unicorn Hunting 2022: Top Countries & Industries for Unicorn Companies. Disponível em: <https://tipalti.com/blog/unicorn-hunting-2022/>. Acesso em: 13 nov. 2025.

US BIS Export Controls to Restrict China's Capability to Produce Advanced Semiconductors 2024.

US BIS 2025 Commerce Closes Export Controls Loophole for Foreign-Owned Semiconductor Fabs in China.

Why AI companions and young people can make for a dangerous mix. News Center. Disponível em: <https://med.stanford.edu/news/insights/2025/08/ai-chatbots-kids-teens-artificial-intelligence.html>. Acesso em: 6 dez. 2025.

Work with La Suite numérique. Disponível em: <https://lasuite.numerique.gouv.fr/en>. Acesso em: 17 nov. 2025.

World Bank Document. Disponível em: <https://documents1.worldbank.org/curated/en/843301610630752625/pdf/Pandemic-Trade-Covid-19-Remote-Work-and-Global-Value-Chains.pdf>. Acesso em: 25 nov. 2025.

XiangShan: open-source high-performance RISC-V processor. Disponível em: <https://riscv-europe.org/summit/2023/media/proceedings/plenary/2023-06-07-09h30-Yungang-BAO-slides.pdf>. Acesso em: 19 nov. 2025.

Zero Rating. Disponível em: <https://zerorating.wordpress.com/>. Acesso em: 12 nov. 2025.

中华人民共和国国家情报法 (National Intelligence Law of the People's Republic of China). Disponível em: <https://www.lawinfochina.com/display.aspx?id=23733&lib=law>. Acesso em: 15 set. 2025.

Conheça melhor a editora Lumen Juris

www.lumenjuris.com.br
@lumenjuriseditora
publique@lumenjuris.com.br

Ao longo dos últimos anos, o assunto da soberania digital emergiu como um dos temas mais debatidos nos círculos das políticas digitais. A soberania digital é um conceito central no debate contemporâneo sobre a autonomia tecnológica dos Estados e o direito à autodeterminação individual e coletiva. Nas nossas pesquisas sobre soberania digital, elaboradas entre 2020 e 2025 e citadas ao longo deste estudo, definimos este conceito como "a capacidade de entender o funcionamento das tecnologias digitais, conseguir desenvolvê-las e regulá-las efetivamente, exercendo, portanto, autodeterminação, poder e controle sobre ativos digitais tais como dados, softwares, hardwares e redes eletrônicas."

Este trabalho analisa a soberania digital como autonomia tecnológica, consagrada no artigo 219 da Constituição Federal e no direito à autodeterminação, sem equivaler à autarquia digital. Destaca a necessidade de abordagem sistêmica para mitigar riscos de dependência tecnológica e explorar oportunidades de desenvolvimento. Propõe um framework com a metáfora da "Pilha" para mapear interconexões entre camadas técnicas e de governança em IA. Examina riscos como perda de competitividade financeira, capacidade estatal de compreensão e regulação social, econômica e democrática, e prestação de serviços essenciais.

Explora atores, arranjos e instrumentos subaproveitados para governança efetiva, propondo caminhos institucionais e políticas públicas de curto, médio e longo prazos. Enfatiza a soberania digital como projeto de Estado, vital para desenvolvimento nacional e cooperação internacional baseada em regras compartilhadas e arquiteturas abertas.

Crucialmente, o estudo propõe caminhos concretos para fortalecer a autonomia tecnológica do Brasil, mostrando que soberania digital não é isolamento, mas projeto de Estado voltado a preservar capacidade de escolha, promover desenvolvimento e incentivar cooperação internacional baseada em regras abertas e arquiteturas compartilhadas.

FGV DIREITO RIO

Lumen Juris Direito | 35

ISBN:978-85-519-3956-7

9 788551 939567