



Soberania Digital no Brasil

Diagnóstico, Desafios e Caminhos sob a perspectiva da Ciência,
Tecnologia e Inovação



Texto para Discussão - Soberania digital no brasil: diagnóstico, desafios e caminhos sob a perspectiva da ciência, tecnologia e inovação

Equipe técnica do MCTI

Henrique de Oliveira Miguel (*Secretário de Ciência, Tecnologia e Inovação para a Transformação Digital – SETAD/MCTI*)

Hugo Valadares (*Diretor - DECTI*)

Eliana Cardoso Emediato (*Coordenadora-Geral - CGGD*)

André Rafael Costa e Silva (*Coordenador - COPID*)

Adriana Anunciato Depieri (*Analista de Ciência e Tecnologia*)

Daniel Boson (*Gestor*)

Amauri Casarin Junior (*Analista de Ciência e Tecnologia*)

Equipe técnica do CGEE

Caetano Christophe Rosado Penna (*Diretor supervisor*)

Caroline Nascimento Pereira (*Líder de projeto*)

Isabela Quadros Dantas Barros

Marcus Vinicius Paiva (*Estagiário*)

Consultor técnico e autor do texto

Luca Belli (FGV-RJ)

As opiniões emitidas nesta publicação são de exclusiva e de inteira responsabilidade do autor, não exprimindo, necessariamente, o ponto de vista do Ministério da Ciência, Tecnologia e Inovação ou o Centro de Gestão e Estudos Estratégicos (CGEE).



Sumário

Sumário Executivo	6
1 Introdução.....	8
1.1 Contexto tecnológico, jurídico e político	10
1.2 Os desafios da soberania digital para o Brasil	12
1.3 O papel essencial da Ciência, Tecnologia e Inovação (CT&I) para construir a soberania digital	13
1.4 Objetivos e justificativa	16
1.5 Metodologia e limites analíticos	17
2 Fundamentos da Soberania Digital.....	19
2.1 Definições e abordagens conceituais.....	20
2.2 Dimensão informacional	21
2.3 Dimensão infraestrutural	22
2.4 Dimensão lógica	23
2.5 Dimensão de cibersegurança, ciberdefesa e segurança nacional	23
2.6 Dimensão de interdependência instrumentalizada	25
3 Diagnóstico do Cenário Brasileiro.....	27
3.1 Marcos regulatórios distantes da realidade: dados, conectividade significativa e IA.....	27
3.2 Políticas de inovação e instrumentos de fomento existentes	29
3.3 Infraestrutura nacional: nuvens públicas, data centers, HPC e redes de pesquisa.....	30
3.4 Ecossistema científico e industrial: capacidades, fragilidades e lacunas.....	31
3.5 Minerais críticos: uma oportunidade “de ouro”	33
3.6 A implementação do PBIA: o começo da jornada rumo à autonomia tecnológica.....	34
3.7 Governança institucional e atores envolvidos.....	36
4 Experiências Internacionais Relevantes	38
4.1 Estados Unidos: a administração pública como cliente âncora.....	38
4.2 China: política industrial, governança integrada e <i>open source</i>	39
4.3 União Europeia: limites estruturais e potencial do <i>Cloud Sovereignty Framework</i>	41
4.4 Suíça: um LLM aberto, transparente e soberano	42
4.5 Finlândia: adoção de software livre para soberania digital cidadã.....	43
4.6 O caso do Uruguai: construção da soberania digital a partir das bases.....	44
4.7 México: a promessa do supercomputador mais potente da América Latina.....	45
4.8 Índia Stack: soberania por meio de infraestruturas públicas digitais e conectividade significativa	47
4.9 Lições e elementos adaptáveis ao contexto brasileiro	48



5	Construção de um Ecossistema Digital Nacional Tecnicamente Autônomo e Aberto	51
5.1	A pilha como metáfora analítica para a arquitetura tecnológica e de governança dos sistemas digitais.....	51
5.2	A Pilha Digital Brasileira como arquitetura sociotécnica de autonomia tecnológica	54
5.3	Bolsas de dados e intercâmbio informacional.....	57
5.4	Centros de excelência, redes de pesquisa e alianças estratégicas	58
5.5	Padrões, interoperabilidade e reprodutibilidade científica	59
5.6	Uma plataforma nacional de comunicação e colaboração profissional baseada em tecnologias <i>open source</i> e IA brasileira.....	60
5.7	A construção de um ecossistema digitalmente soberano por meio da CT&I	62
6	Recomendações Estratégicas de Regulação e Governança	66
6.1	Ajustes regulatórios necessários	66
6.2	Governança multissetorial.....	67
6.3	Alavancar as compras públicas para estimular a indústria nacional.....	68
6.4	Framework de compliance e certificação em segurança e proteção de dados	69
7	Política De Desenvolvimento Tecnológico e produtivo para a Soberania Digital.....	71
7.1	Fortalecimento da infraestrutura tecnológica fundamental	71
7.2	Estímulo ao desenvolvimento de modelos, software e hardware	72
7.3	Incentivo ao <i>open source</i> como vetor de autonomia.....	73
7.4	Desenvolvimento de ecossistemas de inovação e integração com setores estratégicos da economia	74
7.5	Mecanismos público-privados e instrumentos financeiros	75
8	Cooperação Internacional para a Soberania Digital: Padrões, Regimes Jurídicos, Ciência e Indústria	77
8.1	Uma inserção qualificada na governança internacional	78
8.2	Cooperação no âmbito do sistema das Nações Unidas.....	79
8.3	Cooperação em clubes e mecanismos regionais de governança: BRICS, Mercosul e diálogos UE-Mercosul	80
8.4	Cooperação bilateral estratégica: semicondutores, IA e infraestrutura crítica	80
8.5	A cooperação técnica em organismos internacionais de padronização.....	81
9	Caminhos para Implementação	84
9.1	Priorização estratégica e métricas de impacto	84
9.2	Sequenciamento de políticas e investimentos por meio de alianças setoriais.....	85
9.3	Riscos, obstáculos e mitigação	86
9.4	Conjunto de indicadores e monitoramento	88



10	Conclusões.....	90
	10.1 Recomendações para estudos futuros	92
	Referências Bibliográficas	94



Sumário Executivo

O presente texto para discussão introduz os fundamentos conceituais, institucionais e tecnológicos da soberania digital brasileira e propõe diretrizes para o desenvolvimento de um ecossistema digital nacional capaz de promover maior autonomia tecnológica. Com base na literatura especializada, o documento defende que a soberania digital não é sinônimo de autarquia digital, mas deve ser compreendida como a capacidade de entender o funcionamento, desenvolver e regular efetivamente tecnologias digitais.

Tal capacidade é essencial para o Estado exercer controle jurídico, técnico e operacional sobre ativos digitais e infraestruturas críticas, que desempenham um papel essencial para a funcionamento da sociedade, da economia e da democracia brasileira. Nessa perspectiva, portanto a soberania digital constitui-se como elemento central para preservar o direito à autodeterminação (informacional) individual e coletiva.

O diagnóstico apresentado evidencia que o Brasil possui importantes ativos institucionais e científicos, mas enfrenta problemas e dependências significativas em várias dimensões que compõem a soberania digital, como hardware, conectividade, processamento de dados, governança e (efetividade de) frameworks regulatórios, e financiamento. A fragmentação regulatória e institucional, a dependência tecnológica, e a ausência de uma abordagem integrada à cibersegurança, às tecnologias abertas e à interoperabilidade, limitam a autonomia tecnológica nacional e expõem o país a enormes riscos geopolíticos e geoeconômicos.

A partir dessa análise, esse texto propõe uma série de medidas voltadas a fortalecer a autonomia tecnológica nacional. Tais medidas incluem ajustes regulatórios, aprimoramento da governança multissetorial, uso estratégico de compras públicas, criação de um Framework Brasileiro de Soberania Digital, fortalecimento da infraestrutura computacional nacional, estímulo ao desenvolvimento e uso de modelos de inteligência artificial e softwares abertos, políticas industriais orientadas a setores estratégicos, criação de alianças setoriais estratégicas, cooperação internacional, e mecanismos permanentes de financiamento e monitoramento.

Nesta perspectiva, a Ciência, Tecnologia e Inovação (CT&I) desempenham um papel estratégico extremamente relevante, que precisa ser explorado de maneira mais assertiva como elemento propulsor essencial da soberania digital brasileira, para articular a construção de um ecossistema digital tecnologicamente autônomo, aberto e cooperativo. Como demonstram as experiências internacionais analisadas, o uso estratégico da CT&I representa o “ingrediente secreto” adotado por todos os países com maior destaque na construção de sua autonomia tecnológica.

À luz das análises desenvolvidas neste texto, as recomendações convergem para um objetivo central: alavancar a transformação digital como vetor de desenvolvimento econômico, inclusão social e autonomia tecnológica, articulando infraestrutura, ciência, indústria e governança em um projeto nacional de longo prazo. Por fim, reconhecendo a complexidade



temática, o texto destaca a necessidade de se analisar de maneira pormenorizada as dimensões examinadas, identificando áreas mais relevantes a serem priorizadas no curto e médio prazo e estabelecer métricas para monitorar avanços em tais áreas.



1 Introdução

A discussão contemporânea sobre soberania digital exige uma abordagem analítica e institucionalmente situada, que considere simultaneamente os aspectos tecnológicos, jurídicos, econômicos e geopolíticos que estruturam as novas dinâmicas de poder nos ecossistemas digitais. A afirmação da soberania, tradicionalmente associada ao domínio territorial, militar e normativo dos Estados, passa a exigir capacidade efetiva de governar infraestruturas digitais complexas, padrões técnicos, fluxos massivos de dados, arquiteturas computacionais de larga escala e sistemas de inteligência artificial (IA) com crescente autonomia operacional.

As pesquisas mais recentes e estruturadas sobre soberania digital e suas dimensões, oferecem uma moldura teórica sofisticada para compreender esse cenário.¹ Neste sentido, a soberania digital é caracterizada pela interdependência entre dimensões tecnológicas, normativas e econômicas e defensivas, e pela crescente tensão entre o clássico poder estatal e o poder corporativo, derivado do controle efetivo sobre infraestruturas digitais, e a capacidade de se regular setores inteiros da economia, ou mesmo populações, por meio de arquiteturas digitais.² O Brasil, como país em desenvolvimento, caracterizado pela dependência em várias dimensões tecnológicas, enfrenta desafios específicos e relevantes, porém apresenta um leque interessante de ativos particularmente valiosos.

Antes de se concentrar nas vulnerabilidades brasileiras, cabe frisar que o país possui vantagens comparativas relevantes³: setores econômicos com alta aplicabilidade tecnológica, como saúde, finanças, educação, agronegócio, mineração e energia, que podem se beneficiar da transformação digital, da adoção e desenvolvimento de IA; amplas reservas de minerais críticos, essenciais para a produção de hardware e a transição energética global e; sistemas de Internet das Coisas de ampla escala, que permitem ampla coleta de dados; infraestrutura de comunicações robusta, com redes de fibra ótica e conectividade que podem ser ampliadas para reduzir desigualdades e fortalecer o acesso digital; população diversa e numerosa, que forma massa crítica para o desenvolvimento e validação de soluções digitais em larga escala; localização geográfica estratégica, aliada à estabilidade democrática, que favorece parcerias internacionais em meio à reconfiguração geopolítica global; e matriz energética

¹ BELLI, Luca *et al*, **Soberania Digital e Inteligência Artificial no Brasil: rumo à autonomia tecnológica**, RIO DE JANEIRO, RJ: Lumen Juris, 2026; BELLI, Luca; JIANG, Min, Digital Sovereignty in the BRICS Countries, 2024; FLORIDI, Luciano, The Fight for Digital Sovereignty: What It Is, and Why It Matters, Especially for the EU, **Philosophy & Technology**, v. 33, n. 3, p. 369–378, 2020; POHLE, Julia; THIEL, Thorsten, **Digital sovereignty**, disponível em: <<https://policyreview.info/concepts/digital-sovereignty>>. acesso em: 11 mar. 2025; BELLI, Luca; GASPAR, Walter B, The Quest for AI Sovereignty, Transparency and Accountability, 2023.

² O controle absoluto que grandes empresas detêm sobre seus ecossistemas digitais pode ser comparado a uma verdadeira soberania privada transnacional, como argumentado por MACKINNON, Rebecca, **Consent of the Networked: The Worldwide Struggle For Internet Freedom**, USA: Basic Books, Inc., 2012; CHANDER, Anupam, Facebookistan, **North Carolina Law Review**, v. 90, n. 5, p. 1807, 2012; BELLI, Luca, Structural Power as a Critical Element of Social Media Platforms' Private Sovereignty, 2022; GU, Hongfei, Data, Big Tech, and the New Concept of Sovereignty, **Journal of Chinese Political Science**, v. 29, n. 4, p. 591–612, 2024.

³ Um diagnóstico atualizado de tais ativos encontra-se no Plano Brasil Digital 2030.



predominantemente renovável, que atrai investimentos com viés em sustentabilidade e contribui para uma transformação digital ambientalmente sustentável.

Cumpre enfatizar que soberania digital não significa isolamento ou autarquia digital, mas a capacidade de alavancar tais ativos pelo uso estratégico do mercado interno (art. 219 da CF), empoderamento social e fortalecimento da concorrência, da inovação, e da (ciber)segurança⁴ e da defesa nacional e da cooperação internacional. Nesta perspectiva, a Ciência, Tecnologia e Inovação (CT&I) desempenham um papel estratégico extremamente relevante, que precisa ser alavancado de maneira mais assertiva como elemento propulsor essencial da soberania digital brasileira, na perspectiva de se construir um ecossistema digital tecnologicamente autônomo, aberto e cooperativo. Porém, para alcançar essa situação ideal, múltiplos obstáculos precisam ser enfrentados.

Entre os desafios sistêmicos mais relevantes destacam-se o subfinanciamento, o subaproveitamento e a insegurança da infraestrutura crítica; as dependências tecnológicas em várias dimensões tais como semicondutores, computação em nuvens e plataformas de comunicação; a fragmentação e inefetividade regulatória; a ausência de coordenação institucional robusta; e as dificuldades de integração entre CT&I, indústria e Estado. Num tal contexto, a necessidade de construir uma estratégia nacional coerente, juridicamente consistente e tecnicamente adequada é, portanto, imperativa.

A compreensão desses desafios implica reconhecer que a abstração da noção de soberania digital pode ser operacionalizada para garantir que a transformação digital permita a nação brasileira de permanecer soberana e ao Estado brasileiro de exercer de maneira efetiva suas competências constitucionais: proteger direitos fundamentais, assegurar a segurança nacional, fomentar o progresso científico e a autonomia tecnológica e promover o desenvolvimento econômico e industrial. Em um cenário de crescente automação e de concentração internacional de capacidades computacionais, a autonomia governamental depende de controle sobre os ativos digitais essenciais para o funcionamento da economia, da sociedade e da democracia brasileiras.

A capacidade de controle efetivo sobre bases de dados, infraestruturas críticas, sistemas de IA, cadeias de suprimentos torna-se, portanto, uma função da capacidade de se entender o funcionamento de tais ativos, conseguir escolher livremente qual opção tecnológica adotar, desenvolver alternativas e conseguir implementar efetivamente a legislação nacional. A inexistência desses elementos colapsa a soberania estatal e coloca em risco o sistema político-institucional e a capacidade de formulação e implementação de políticas públicas estruturantes, como (ciber)segurança pública, defesa, saúde, educação, administração tributária e liberdade econômica e proteção social. Dessa forma, a discussão sobre soberania digital é também uma discussão sobre o próprio exercício da cidadania e sobre a autonomia não somente tecnológica, mas até política, do país.

⁴ Esse termo é utilizado para designar simultaneamente a cibersegurança e a segurança nacional.



1.1 Contexto tecnológico, jurídico e político

O cenário tecnológico é marcado pela concentração da capacidade computacional nas mãos de poucas empresas globais, capazes de controlar infraestrutura de nuvem, plataformas digitais, semicondutores, *clusters* de computação de alto desempenho, sistemas de IA proprietários e extensas bases de dados.⁵ Segundo estudos recentes, a dependência de países em desenvolvimento desses atores privados gera desafios que se manifestam por meio de custos crescentes, perda de capacidade regulatória nos setores que prestam ou utilizam serviços automatizados, riscos de descontinuidade e insegurança de tais serviços, assimetrias informacionais, desproteção contra o uso coercitivo ou adversário das dependências tecnológicas, extração não tributada e captura de recursos – informacionais, científico-culturais e minerários –, além da possibilidade de captura regulatória.⁶

Adicionalmente, a cadeia de suprimento de hardware e software, essencial para a soberania computacional, encontra-se concentrada, com grande parte da produção avançada localizada em Taiwan (semicondutores), Coreia (memórias) e EUA (cadeia de valor da computação em nuvem), e a litografia controlada por empresas europeias. Entre os principais pontos críticos estão: *i*) servidores, chips e semicondutores importados; *ii*) equipamentos de rede baseados em arquiteturas proprietárias estrangeiras; *iii*) serviços de nuvem e processamento avançado concentrados em *hyperscalers*⁷ internacionais, com implicações de jurisdição, continuidade de serviço e lock-in; *iv*) sistemas operacionais proprietários amplamente utilizados na administração pública, sem distribuições nacionais de larga escala para sistemas operacionais abertos; e *v*) ferramentas de segurança cibernética e monitoramento majoritariamente desenvolvidos fora do país. Esses fatores combinados reduzem o controle jurídico e operacional sobre sistemas sensíveis e dificultam a consolidação de um ecossistema digital nacional robusto.

No campo jurídico, o Brasil desenvolveu marcos regulatórios importantes, como o Marco Civil da Internet (Lei nº 12.965/2014), o Marco Legal de Ciência, Tecnologia e Inovação (Lei nº 13.243/2016), a Lei Geral de Proteção de Dados (Lei 13.709/2018), a Lei de Governo Digital

⁵ MCMAHON, M. et al. (2021), “Scale, market power and competition in a digital world: Is bigger better?”, *OECD Science, Technology and Industry Working Papers*, No. 2021/01, OECD Publishing, Paris; WU, Tim, *The Curse of Bigness: Antitrust in the New Gilded Age*, **Faculty Books**, 2018; LIANOS, Ioannis; IVANOV, Alexey, *Digital Era Competition BRICS Report*, 2019.

⁶ BELLI, Luca; GASPAR, Walter B; COUTO, Natalia; *et al.* **Soberania Digital e Inteligência Artificial no Brasil: rumo à autonomia tecnológica**. RIO DE JANEIRO, RJ: Lumen Juris, 2026.; COULDRY, Nick; MEJIAS, Ulises A, *The Costs of Connection: How Data Are Colonizing Human Life and Appropriating It for Capitalism*, **ResearchGate**, 2024; COULDRY, Nick; MEJIAS, Ulises A, *Data colonialism: rethinking big data’s relation to the contemporary subject*, 2018; **Data for development**, Geneva: United Nations, 2024; RIKAP, Cecilia, **Dynamics of Corporate Governance Beyond Ownership in AI**, disponível em: <<https://www.commonwealth.org/publications/dynamics-of-corporate-governance-beyond-ownership-in-ai>>, acesso em: 19 set. 2025.

⁷ O termo *hyperscaler* é usado para definir uma empresa provedora de serviços digitais capaz de operar infraestrutura computacional em escala massiva, caracterizada por data centers distribuídos globalmente, arquitetura altamente automatizada e capacidade de provisionar computação, armazenamento e rede de forma elástica. Esses provedores, como AWS, Microsoft Azure e Google Cloud, sustentam serviços de nuvem, inteligência artificial e processamento de grandes volumes de dados, exercendo influência estrutural sobre cadeias tecnológicas, fluxos informacionais e ecossistemas econômicos que dependem de sua infraestrutura.



(Lei nº 14.129/2021), além de regulamentações setoriais de cibersegurança⁸ e vários planos e estratégias voltada à promoção da inovação e do desenvolvimento da indústria nacional.⁹ No entanto, apesar desses avanços, o país carece de investimentos estratégicos e ainda não dispõe de legislação capaz de regular de forma abrangente, isto é, enquadrando riscos, e ao mesmo tempo, estimulando o desenvolvimento e a adoção, os sistemas de IA, a cibersegurança, a interoperabilidade e a concorrência nos mercados digitais.

Ademais, este texto ressalta que, apesar dos relevantes avanços normativos, a existência de instrumentos regulatórios é condição necessária, porém insuficiente para a construção da soberania digital brasileira.¹⁰ A fragmentação institucional, a implementação parcial da legislação, a fragilidade técnica do órgão central para coordenar e maximizar os esforços de atores públicos, privados, acadêmicos e sociais dificultam a execução sistêmica e efetiva dessas políticas. Soma-se a isso a insuficiência – em escala, especialização e dedicação exclusiva – de equipes permanentes voltadas para desenvolvimento de políticas de CT&I para setores e tecnologias complexas (computação de alto desempenho, arquiteturas abertas, cadeia de valor de IA, computação quântica, cibersegurança, Internet das Coisas, biotecnologias, etc.), o que limita a capacidade do Estado de transformar diretrizes em entregas concretas e sustentáveis.

Por fim, no plano político, o mundo assiste uma reconfiguração das forças tecnológicas entre blocos que competem pela liderança em IA, infraestruturas digitais, computação quântica e outras tecnologias disruptivas, bem como pela definição de padrões e mecanismos de governança capazes de conduzi-las. Países como Estados Unidos e China estruturaram políticas industriais coordenadas, alavancam estavelmente e massivamente CT&I como elementos essenciais de sua visão desenvolvimentista, e mobilizaram investimentos – públicos e privados – trilionários para garantir não somente a autossuficiência tecnológica, mas o domínio sobre infraestruturas digitais.

⁸ Uma análise atualizada e detalhada de todas as regulamentações em vigor em matéria de cibersegurança até a se encontra disponível em 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.

⁹ Entre as atualizações normativas mais relevantes neste sentido, podemos destacar a Lei nº 14.968/2024, que aperfeiçoa a política industrial para o setor de TICs, ajusta incentivos, cria o Programa Brasil Semicondutores (Brasil Semicon); a Lei nº 14.968/2024, que atualizou e adequou a concessão de incentivos incluindo parâmetros relacionados a tecnologias nacionais (TECNAC); e a Lei nº 14.302/2022 e a Lei nº 14.968/2024 que trouxeram ajustes e prorrogações para o regime de incentivos ao Programa de Apoio ao Desenvolvimento Tecnológico da Indústria de Semicondutores (novo PADIS).

¹⁰ Como demonstra, de maneira paradigmática, a experiência europeia, a ampla produção normativa é, por si só, insuficiente para alcançar uma situação de soberania digital na ausência de alternativas tecnológicas desenvolvidas localmente. BRIA, Francesca; TIMMERS, Paul; GERNONE, Fausto. EuroStack – a European alternative for digital sovereignty. Bertelsmann Stiftung. Gütersloh., 2025, p. 127.

Além disso, conforme relatório organizado pela própria Comissão Europeia e de autoria do ex-Presidente do Banco Central Europeu, Mario Draghi, o foco na mera produção normativa, em detrimento de uma implementação racionalizada e de uma sólida política industrial, é suscetível de gerar obstáculos e prejuízos ao desenvolvimento. DRAGHI, Mario. The future of European competitiveness: Part A: a competitiveness strategy for Europe. Luxembourg: Publications Office of the European Union, 2025.



Apesar de não ter alcançado uma soberania tecnológica proporcional à sua capacidade regulatória, a União Europeia e seus Estados-membros desenvolveram iniciativas interessantes voltadas a construir autonomia estratégica, como será abordado no capítulo 4. De modo complementar, países como Índia, México e Uruguai oferecem perspectivas interessantes sobre como “potências intermediárias”, e até países menores, vêm construindo sua soberania digital por meio de iniciativas estratégicas.

Neste contexto complexo, embora o Brasil disponha de massa crítica científica e de uma base industrial relevante, ainda carece de visão estratégica integrada capaz de conectar regulação, política industrial, governança, segurança cibernética, pesquisa, desenvolvimento e inovação. Particularmente, como será destacado nos capítulos 5 e 9, o país dispõe de ativos extremamente valiosos que podem ser organizados por meio de alianças setoriais estratégicas para fortalecer a autonomia tecnológica. Portanto, o diagnóstico apresentado por este texto deveria ser utilizado, idealmente, para subsidiar a formulação dessa visão estratégica, contribuindo para o esforço urgente de reverter, reduzir e, de preferência, eliminar as dependências tecnológicas do país.

1.2 Os desafios da soberania digital para o Brasil

Como destacado na seção precedente, a soberania digital deve ser compreendida como a capacidade de entender o funcionamento, desenvolver e regular efetivamente tecnologias digitais.¹¹ A principal implicação desse argumento é que o país não será soberano se depender integralmente de infraestruturas e sistemas operados por agentes estrangeiros, cujos incentivos e interesses econômicos e geopolíticos não convergem com as prioridades nacionais e podem, em determinados contextos, prejudicar a soberania e segurança do Estado. Esse problema se torna mais agudo no campo da computação em nuvem, particularmente relevante para adoção de sistemas de IA, no qual a posição dominante de grandes empresas globais exacerba o fenômeno do *vendor lock-in*, ou seja, a dependência de um provedor específico que impõe custos de transação elevados para uma eventual migração ou substituição de plataforma.¹² O Brasil, portanto, precisa enfrentar simultaneamente desafios jurídicos, institucionais e tecnológicos.

A consolidação da soberania digital no Brasil enfrenta desafios significativos, pois empresas, universidades e a administração pública permanecem amplamente dependentes de tecnologias estrangeiras. Administrações públicas e empresas privadas utilizam majoritariamente serviços de nuvem e software estrangeiros, além de ferramentas de cibersegurança desenvolvidas no exterior. As universidades dependem de plataformas acadêmicas, softwares científicos e infraestruturas de computação de alto desempenho (ou

¹¹ Veja-se nota nº 1.

¹² 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.



HPC, no acrônimo inglês) importadas. A maior parte dos atores públicos, privados e sociais opera com sistemas operacionais, suítes de produtividade, equipamentos de rede e soluções de virtualização fornecidos por grandes corporações internacionais. A sociedade brasileira, por sua vez, depende de redes sociais estrangeiras para comunicação.

Essas dependências estruturais tendem a comprometer a autonomia tecnológica nacional, reduzem a capacidade de implementar plenamente a legislação, especialmente no que se refere à proteção de dados pessoais e informações sensíveis, dificultam a auditoria e a adaptação de sistemas e limitam o desenvolvimento de soluções locais de alto valor estratégico.

No campo institucional, o país enfrenta dificuldades de coordenação entre um amplo conjunto de ministérios, agências reguladoras, centros de pesquisa e empresas. A ausência de uma abordagem orgânica para a governança da soberania digital impede que políticas públicas sejam implementadas de forma coordenada. A falta de estabilidade institucional e instrumentos de fomento continuado torna difícil sustentar projetos de longo prazo em hardware, software e modelos de IA.

Por fim, há desafios normativos. A ausência de padrões de interoperabilidade obrigatórios, escassez de requisitos de transparência e auditoria de IA, falta de certificação nacional de cibersegurança, e incapacidade de auditar sistemas de infraestruturas críticas e serviços essenciais com critérios próprios, e ausência de políticas públicas para incentivar o desenvolvimento e a adoção de tecnologias em *open source*.

1.3 O papel essencial da Ciência, Tecnologia e Inovação (CT&I) para construir a soberania digital

Como mencionado acima, CT&I são amplamente reconhecidas como prioridades nacionais nos países tecnologicamente mais avançados, constituindo um dos principais vetores de competitividade econômica, soberania nacional e digital e (ciber)segurança. A partir dos anos 1950 e particularmente ao longo da Guerra Fria, os Estados Unidos consolidaram a noção de que a supremacia tecnológica é fundamento estratégico de sua segurança nacional, percepção que, desde então, orienta investimentos contínuos em pesquisa científica, desenvolvimento tecnológico e inovação industrial.¹³ Assim, a maioria dos desenvolvimentos de alta tecnologia nas últimas décadas foi impulsionada pelo imperativo de segurança da Guerra Fria de manter a vantagem tecnológica. Administrações públicas com orçamento bilionário como a Administração Nacional da Aeronáutica e Espaço (NASA) e a Agência de Projetos de Pesquisa Avançada de Defesa dos EUA (DARPA) foram estabelecidas – e atuaram nos últimos 65 anos –

¹³ PIIE Briefing 21-5: Scoring 50 years of US industrial policy, 1970-2020.



para coordenar iniciativas de desenvolvimento em CT&I capazes de manter a superioridade e, consequentemente, a soberania e a segurança nacional.¹⁴

Esse entendimento estruturou ecossistemas robustos de universidades, centros de pesquisa, empresas de base tecnológica e agências governamentais, permitindo não apenas avanços científicos disruptivos, mas também a consolidação de autonomia tecnológica em áreas críticas como defesa, semicondutores, computação, telecomunicações e, mais recentemente, uso e desenvolvimento de IA e outras tecnologias disruptivas. Experiências semelhantes podem ser observadas em países como Japão, Coreia do Sul, China, e Israel, nos quais a CT&I ocupa posição central nas estratégias de desenvolvimento de longo prazo.¹⁵

No contexto da transformação digital contemporânea, marcada pela convergência entre elementos tecnológicos, geopolíticos e geoeconômicos, a centralidade da CT&I torna-se ainda mais evidente. A capacidade de um país de desenvolver, adaptar e governar tecnologias digitais estratégicas passou a ser determinante para sua inserção de maneira autônoma e soberana na economia e governança global. Nesse cenário, o papel do Ministério da Ciência, Tecnologia e Inovação (MCTI) é central para a articulação, coordenação e orientação estratégica do ecossistema nacional de CTI, tendo a responsabilidade para organizar e integrar os diversos atores do sistema – universidades, institutos de pesquisa, agências de fomento, empresas, startups, governos estaduais e municipais, e sociedade civil – a partir de uma visão estratégica compartilhada, capaz de alinhar esforços e recursos em torno de objetivos comuns.

Essa função articuladora é essencial para evitar fragmentação institucional, sobreposição de iniciativas e dispersão de investimentos, problemas recorrentes em sistemas de inovação pouco coordenados. A atuação do MCTI deve se dar com base na definição clara de objetivos de curto, médio e longo prazo, compatíveis com os desafios diagnosticados neste texto e com as necessidades de desenvolvimento econômico e social do país. No curto prazo, isso envolve a criação de condições habilitadoras, como infraestrutura digital, formação de recursos humanos e marcos regulatórios adequados. No médio prazo, requer o fortalecimento de capacidades tecnológicas nacionais em áreas estratégicas, a consolidação de cadeias produtivas intensivas em conhecimento e a ampliação da interação entre ciência e mercado. No longo prazo, implica a construção de autonomia tecnológica sustentável, com capacidade de inovação contínua e liderança em nichos tecnológicos relevantes.

As competências institucionais do MCTI, em especial aquelas atribuídas à Secretaria de Ciência e Tecnologia para a Transformação Digital, conforme estabelecido no Decreto nº 11.493/2023, refletem esse papel estratégico de articulador com capacidade institucional. Entre essas competências destacam-se a formulação e coordenação de políticas públicas para a transformação digital e o estímulo à pesquisa e ao desenvolvimento de tecnologias

¹⁴ BELLI, Luca, **De la gouvernance à la régulation de l'internet**, Paris: Berger Levrault, 2015; MALLIK, Amitav, **Technology and security in the 21st century: a demand-side perspective**, Oxford: Oxford Univ. Press, 2005.

¹⁵ Uma compilação das despesas internas brutas em pesquisa e desenvolvimento CT&I, elaborada pela UNESCO, pode ser consultada em **View - UIS Data Browser**, disponível em: <<https://uis-data-browser-frontend-9qoly6dvy-ixt1.vercel.app/view>>. acesso em: 4 jan. 2026.



digitais emergentes. Essas atribuições posicionam a Secretaria como um eixo estruturante da agenda digital brasileira, com responsabilidade direta sobre a integração entre CT&I e transformação digital, bem como sobre a facilitação e criação de alianças setoriais e o monitoramento das ações voltados ao aprimoramento da soberania digital, como destaca-se nas Seções 3.6 e 9.4.

A visão estratégica que orienta essas ações vem sendo articulada, por meio da elaboração da nova Estratégia Nacional de Ciência, Tecnologia e Inovação (ENCTI 2024–2030).¹⁶ A ENCTI visa estabelecer diretrizes e prioridades para o desenvolvimento científico e tecnológico do país, reconhecendo explicitamente a transformação digital como vetor transversal e estruturante. A proposta de ENCTI 2024–2030 representa um avanço relevante ao problematizar explicitamente a soberania digital como dimensão estratégica do desenvolvimento nacional. Neste sentido, se reconhece que a dependência tecnológica em áreas críticas, como infraestruturas digitais, plataformas, dados, semicondutores e cadeia de valor de IA, compromete a autonomia decisória do Estado e a capacidade do país de capturar valor econômico e social da transformação digital. Ao propor uma abordagem sistêmica, a Estratégia busca alinhar políticas de CTI às demandas da sociedade digital, promovendo a convergência entre pesquisa científica, desenvolvimento tecnológico, inovação empresarial e políticas públicas. Esse alinhamento é fundamental para a construção de um ecossistema digital que seja, simultaneamente, inovador, aberto e soberano.

Além disso, no âmbito específico da IA, as ações a serem coordenadas pelo MCTI já estão delineadas no Plano Brasileiro de Inteligência Artificial (PBIA). Entre suas ações estratégicas, destacam-se aquelas voltadas ao fortalecimento de infraestrutura computacional, dados, formação de talentos e governança, no âmbito do Sistema Nacional de Processamento de Alto Desempenho (SINAPAD). Este sistema adquire papel central ao prover capacidade nacional de processamento de alto desempenho, fundamental tanto para pesquisa científica quanto para aplicações avançadas de IA, modelagem, simulações e ciência de dados.

Apesar de ter uma natureza evolutiva, o PBIA contribui à construção de um ecossistema digital aberto e tecnologicamente autônomo, que, como destacara este texto, é essencial para a soberania digital brasileira. Porém, apesar da centralidade crescente das tecnologias digitais, observa-se uma lacuna relevante no financiamento estruturado de CT&I Digital. No âmbito do Fundo Nacional de Desenvolvimento Científico e Tecnológico (FNDCT), apenas o Programa 11 – IA Brasil – possui vinculação clara com tecnologias digitais.¹⁷ Essa limitação contrasta com a amplitude dos desafios associados à soberania digital, que extrapolam a IA e incluem

¹⁶ EM 18/12/2025 08H09, Publicado, **Participe da Consulta Pública da Estratégia Nacional de Ciência, Tecnologia e Inovação (ENCTI) 2024-2034**, Centro Brasileiro de Pesquisas Físicas - CBPF, disponível em: <<https://www.gov.br/cbpf/pt-br/assuntos/noticias/participe-da-consulta-publica-da-estrategia-nacional-de-ciencia-tecnologia-e-inovacao-enci-2024-2034>>. acesso em: 4 jan. 2026.

¹⁷ BRASIL. Ministério da Ciência, Tecnologia e Inovação. Programas estruturantes e mobilizadores. Disponível em: <https://www.gov.br/mcti/pt-br/acompanhe-o-mcti/fndct/paginas/planejamento/programas-estruturantes-e-mobilizadores/programas-estruturantes-e-mobilizadores>. Acesso em: 4 jan. 2026.



arquiteturas abertas de software e hardware, semicondutores, tecnologias quânticas, cibersegurança, entre outras.

Diante disso, como será destacado na Seção 5.1 deste texto, torna-se recomendável a criação de um programa específico do FNDCT dedicado à soberania digital, com foco em tecnologias digitais estratégicas e infraestruturas críticas. Tal programa permitiria maior previsibilidade orçamentária, indução de capacidades nacionais e alinhamento com as diretrizes da ENCTI e do PBIA. A integração entre ENCTI, PBIA e demais políticas setoriais deve ser orientada por uma lógica de missão¹⁸, na qual desafios nacionais concretos – como conectividade significativa universal, cibersegurança, soberania de dados, infraestruturas públicas digitais, competitividade industrial digital etc – funcionem como motores do desenvolvimento nacional. Nesta perspectiva, a CT&I configura-se como o alicerce para a promoção de um ecossistema digital nacional que seja resiliente, competitivo e soberano.

1.4 Objetivos e justificativa

Este texto para discussão técnica tem como objetivo principal oferecer uma análise abrangente, porém apresentada de forma concisa, sistemática e juridicamente fundamentada da soberania digital no contexto brasileiro.¹⁹ Busca-se fornecer subsídios técnicos e jurídicos para que formuladores de políticas públicas possam compreender a complexidade dos desafios existentes e construir uma visão estratégica nacional consistente, capaz de integrar regulação, governança, fomento, (ciber)segurança e sustentabilidade, alinhada às necessidades de longo prazo do país.

O documento também visa elaborar recomendações práticas e juridicamente estruturadas, capazes de orientar investimentos, reformas institucionais, mecanismos regulatórios, cooperação internacional, e políticas industriais e de CT&I voltadas a estimular um ecossistema digital brasileiro autônomo e aberto. A justificativa é inequívoca: sem autonomia tecnológica, o Estado brasileiro não terá condições de exercer plenamente suas competências constitucionais, proteger o interesse público e garantir que ativos digitais sejam operados de modo seguro, auditável, transparente e alinhado à ordem jurídica nacional. A soberania digital, portanto, não é apenas um requisito técnico, mas uma condição jurídica e política para viabilizar o direito fundamental à autodeterminação da população brasileira.

¹⁸ MAZZUCATO, Mariana; PENNA, Caetano C. R., **Mission-Oriented Finance for Innovation: New Ideas for Investment-Led Growth**, [s.l.]: Bloomsbury Publishing PLC, 2015; MAZZUCATO, Mariana, Mission-oriented innovation policies: challenges and opportunities, **Industrial and Corporate Change**, v. 27, n. 5, p. 803–815, 2018.

¹⁹ Para uma análise mais pormenorizada, sugere-se a leitura da obra com base na qual foi elaborada esse texto: BELLI *et al*, **Soberania Digital e Inteligência Artificial no Brasil: rumo à autonomia tecnológica**.



1.5 Metodologia e limites analíticos

O presente texto para discussão foi elaborado pelo Professor Luca Belli, em qualidade de consultor independente, com base em uma abordagem qualitativa e analítico-interpretativa, combinando diferentes métodos de produção e validação de conhecimento. O processo metodológico adotado buscou assegurar consistência conceitual, alinhamento com o estado da arte do debate sobre soberania digital e aderência às prioridades da agenda nacional de CT&I. Inicialmente, a elaboração deste texto envolveu uma revisão sistemática da literatura acadêmica e institucional relevante. Essa revisão foi complementada por análise doutrinária de (propostas de) marcos normativos e estratégicos que estruturam o debate contemporâneo sobre o papel do Estado na promoção de capacidades tecnológicas soberanas.

O processo também foi informado pela participação do consultor no seminário nacional “Pilha de IA Nacional vai discutir autonomia tecnológica e soberania digital”²⁰, que contribuiu para a incorporação de perspectivas atualizadas e pluralizadas provenientes de especialistas, gestores públicos, pesquisadores e representantes do ecossistema de inovação. Adicionalmente, o texto foi construído de forma iterativa, a partir de diversas reuniões técnicas organizadas por equipes do MCTI e do Centro de Gestão e Estudos Estratégicos (CGEE), nas quais versões iniciais do texto e assuntos específicos foram debatidas e aprimoradas coletivamente.

Como instrumento de apoio ao processo de redação, foram utilizadas ferramentas de IA generativa, com a finalidade específica de destilar, sintetizar e organizar ideias previamente elaboradas pelo consultor em publicações acadêmicas, relatórios técnicos e contribuições institucionais anteriores. O uso dessas ferramentas teve caráter meramente auxiliar e não substitutivo, estando restrito à sistematização textual e à melhoria da clareza expositiva, sem prejuízo da autoria intelectual, da responsabilidade analítica e do juízo crítico do consultor.

Apesar do esforço metodológico empreendido, este texto apresenta limitações inerentes ao seu formato, escopo e finalidade. Trata-se de um documento de natureza sintética e estratégica, voltado a subsidiar o debate e a formulação de políticas públicas, não tendo como objetivo oferecer uma análise acadêmica exaustiva ou plenamente compreensiva de todas as dimensões envolvidas no tema da soberania digital. A análise aprofundada e sistêmica da soberania digital exige estudos abrangentes e análise específicas de dimensões essenciais que, porém, não são diretamente relacionadas à CT&I, como por exemplo regulação de plataformas, integridade da informação, riscos de IA, etc. Tal nível de detalhamento e recortes metodológicos extrapolam o escopo desta nota.

Para uma análise mais aprofundada e sistemática do tema no contexto brasileiro, recomenda-se a consulta à obra “Soberania Digital e Inteligência Artificial no Brasil: rumo à autonomia tecnológica”²¹ que inclui apresentação da Ministra Luciana Santos e prefácio da Ministra Esther Dweck e oferece tratamento extensivo das bases conceituais, dos marcos regulatórios e das

²⁰ Relatório Seminário Pilha IA Soberana.

²¹ BELLI *et al*, **Soberania Digital e Inteligência Artificial no Brasil: rumo à autonomia tecnológica**.



implicações estruturais, tecnológicas e geopolíticas associadas ao tema. Essa referência permite complementar as reflexões aqui apresentadas e aprofundar aspectos que, neste texto, são necessariamente tratados de forma sintética, disponibilizando ainda amplo referencial bibliográfico para o aprofundamento de cada elemento abordado.

Assim, este texto não deve ser interpretado como um diagnóstico definitivo ou uma proposta fechada de política pública, mas como um subsídio qualificado ao debate estratégico em andamento, capaz de orientar reflexões, aprofundamentos futuros e decisões institucionais sobre como construir um ecossistema digital tecnologicamente autônomo por meio da CT&I. Ao explicitar seus próprios limites, o documento reafirma seu papel como ponto de partida para análises mais detalhadas e para a construção coletiva de estratégias voltadas ao fortalecimento da soberania digital brasileira a partir da CT&I.



2 Fundamentos da Soberania Digital

A soberania digital é um conceito multidimensional que abrange o domínio normativo, a capacidade de governança efetiva sobre infraestruturas, o controle sobre fluxos de dados, a autonomia tecnológica em hardware e software e a proteção contra riscos sistêmicos e geopolíticos que se manifestam em arquiteturas digitais globais. Seu fundamento reside na noção clássica de soberania como poder supremo exercido dentro de um território, reinterpretada à luz de um ambiente digital interconectado no qual provedores privados (e no caso brasileiro, frequentemente estrangeiros) exercem funções normativas e estruturantes por meio de sua capacidade de definir as arquiteturas de produtos, serviços digitais e cadeias globais de suprimentos.²²

Cabe ressaltar que, no Brasil, a soberania digital tem fundamento constitucional. Embora não mencionada expressamente pela Constituição de 1988, decorre diretamente dos princípios constitucionais da soberania nacional, da redução das desigualdades sociais e da promoção da inovação e da autonomia tecnológica. O artigo 1º, inciso I, o artigo 3º, incisos II e III, e os artigos 218 e 219 reforçam essas bases ao reconhecer a soberania, a ciência, tecnologia e inovação como instrumentos de fortalecimento da independência econômica e do bem-estar social. Assim, a soberania digital emerge como imperativo jurídico destinado a assegurar autonomia nacional em um cenário de profunda interdependência tecnológica.

Neste contexto, é importante enfatizar que a arquitetura técnica dos ativos digitais deve ser considerada como uma forma de regulação que pode limitar ou condicionar a capacidade dos Estados de exercer sua autoridade, de empresas de operar, e o pleno gozo de direitos individuais.²³ A soberania digital, portanto, não se reduz à legislação ou a políticas públicas: exige o controle efetivo, a capacidade de desenvolver e de auditar infraestruturas técnicas e lógicas que moldam o ambiente informacional.

Essa abordagem revela que a soberania digital é menos uma característica estática e mais uma condição operacional composta por capacidades acumuladas e em evolução contínua. É preciso ter domínio sobre as infraestruturas de comunicação, sobre os padrões técnicos que regem a interoperabilidade dos sistemas, sobre a capacidade de armazenar, tratar e proteger dados, sobre a cadeia de suprimentos em hardware de vários tipos, inclusive no que diz respeito à minérios críticos e fontes de energia, e sobre mecanismos de desenvolvimento e auditoria de modelos e algoritmos.

A recente transformação tecnológica, impulsionada e acelerada pela digitalização devida à pandemia de Covid-19, apenas intensificou o peso do controle sobre infraestruturas digitais e

²² STRANGE, Susan, **States and markets**, 1. ed. London: Continuum, 1988; LESSIG, Lawrence, **Code: And Other Laws of Cyberspace**, Sydney: ReadHowYouWant.com, 2009; BELLI, Luca, **Structural Power as a Critical Element of Social Media Platforms' Private Sovereignty** (2022). In Edoardo Celeste, Amélie Heldt and Clara Iglesias Keller (Eds). **Constitutionalising Social Media**. (Hart 2022).; BELLI, Luca, **De la gouvernance à la régulation de l'internet**, Paris: Berger Levrault, 2015.

²³ Idem.



ativos informacionais no exercício da soberania.²⁴ Assim, para Estados que dependem fortemente de infraestruturas, serviços e plataformas operadas por agentes estrangeiros, a falta de controle sobre tais ativos, ou de alternativas, torna-se uma considerável vulnerabilidade sistêmica, jurídica, econômica e estratégica. Apesar de seus inúmeros ativos, o Brasil se encontra em situação de vulnerabilidade na maioria das dimensões que serão examinadas neste texto, exigindo que os fundamentos aqui expostos sirvam de base para a construção de políticas públicas robustas.

2.1 Definições e abordagens conceituais

A definição de soberania digital não é uniforme, mas converge em torno de duas dimensões. A primeira, centrada no Estado, entende soberania digital como o conjunto de capacidades e competências que permitem ao país exercer controle efetivo sobre infraestruturas críticas, fluxos e bases de dados, cadeias de suprimentos tecnológicos e uso de tecnologias digitais.

A segunda, de caráter mais relacional, compreende a soberania digital como a capacidade de um ator específico – estatal ou não – de estabelecer normas e exercer controle em um ambiente no qual a arquitetura técnica das redes, sistemas e plataformas permite ou limita o exercício dessa capacidade. Assim, a soberania não é apenas um atributo jurídico, mas constitui uma disputa pelo controle sobre camadas técnicas que definem a capacidade de compreender o funcionamento, desenvolver e regular efetivamente as tecnologias digitais.²⁵

Outra abordagem relevante, comum na literatura europeia, associa soberania digital à autonomia estratégica e à redução de dependências externas em setores considerados críticos, como computação em nuvem, semicondutores, inteligência artificial e cibersegurança.²⁶ Países que não controlam essas camadas tecnológicas tornam-se vulneráveis a interrupções de suprimentos, riscos geopolíticos, falhas de infraestrutura, abuso de poder de mercado e restrições contratuais impostas por fornecedores estrangeiros.

Com base nessas perspectivas, pode-se afirmar, portanto que a soberania digital é, portanto, inseparável da capacidade técnica de desenvolver e operar as infraestruturas que sustentam o ecossistema informacional contemporâneo. Ela se torna também um imperativo jurídico de regulação efetiva de tecnologias digitais, na medida em que Estados devem garantir a aplicação

²⁴ 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; BELLI, Luca; GASPAS, 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; 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; BELLI, Luca; GUGLIELMI, Gilles J., *L'État digital: numérisation de l'administration publique et administration publique du numérique*, Boulogne-Billancourt: Berger-Levrault, 2022.

²⁵ 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.

²⁶ FLORIDI, The Fight for Digital Sovereignty; POHLE; THIEL, *Digital sovereignty*.



eficaz das normas constitucionais e legais destinadas à proteção de direitos fundamentais, de preservação da segurança nacional e à continuidade de serviços públicos essenciais.

2.2 Dimensão informacional

A dimensão informacional da soberania digital é, talvez, a mais discutida, pois envolve o controle sobre fluxos de dados pessoais, governamentais, industriais e científicos. Os dados adquirem um papel particularmente relevante como insumos estratégicos para o treinamento e a operação de sistemas de IA, para a formulação de políticas públicas e para o efetivo fornecimento de serviços essenciais, como saúde, comunicação, finanças e defesa. O marco jurídico brasileiro, com destaque para a Lei Geral de Proteção de Dados, oferece instrumentos importantes, mas insuficientes para garantir plena autonomia informacional.

A insuficiência decorre, de um lado, da implementação ainda incipiente da própria LGPD²⁷ e, de outro, dos limites da própria lei, cujo objetivo é regular o tratamento de dados pessoais, mas não estimular a pesquisa, o desenvolvimento e a adoção de produtos e serviços nacionais baseados no processamento de dados. Apesar da proteção legal, e até constitucional da autodeterminação informativa, tal garantia torna-se esvaziada se não for acompanhada de políticas de estímulo ao desenvolvimento de produtos e serviços capazes de traduzir o disposto normativo em tecnologias adotadas em escala.

Além disso, como será detalhado adiante, o país ainda não desenvolveu plataformas públicas robustas para o intercâmbio seguro de dados, tampouco sistemas avançados de certificação ou auditoria de dados, que desempenham um papel instrumental para estimular o uso seguro e lícito de tais ativos no interesse nacional. Neste contexto, cabe frisar que apesar da LGPD ter instituído a Agência Nacional de Proteção de Dados desde 2020, o regulador ainda não definiu padrões sobre interoperabilidade ou segurança de dados, dois assuntos cruciais para permitir a soberania de dados e o funcionamento de plataformas de intercâmbio de dados.

A dimensão informacional também abrange a capacidade de garantir que dados estratégicos do Estado e de setores essenciais permaneçam sob jurisdição nacional. O uso intensivo de nuvens estrangeiras, muitas vezes submetidas a legislações extraterritoriais que podem obrigar o provedor a permitir acesso governamental, como o CLOUD Act²⁸ e a seção 702 do FISA dos Estados Unidos²⁹, coloca em risco a soberania nacional ao criar condições para que dados sensíveis sejam acessados por autoridades estrangeiras.

A soberania informacional requer, portanto, tanto a elaboração e implementação efetiva de instrumentos regulatórios quanto o desenvolvimento e adoção de infraestruturas digitais nacionais alternativas as opções dominantes. Não parecem necessárias, nem desejáveis,

²⁷ BELLI, Luca; ZINGALES, Nicolo; BAKONYI, Erica, **LGPD: lei que pega ou lei que não pega?**, JOTA Jornalismo, disponível em: <<https://www.jota.info/opiniao-e-analise/colunas/direitos-tecnologias/lgpd-lei-que-pegou-ou-lei-que-nao-pegou>>. acesso em: 9 dez. 2025.

²⁸ U.S. CONGRESS, Clarifying Lawful Overseas Use of Data Act (CLOUD Act).

²⁹ UNITED STATES OF AMERICA, **Foreign Intelligence Surveillance Act**, disponível em: <<https://www.intel.gov/foreign-intelligence-surveillance-act>>. acesso em: 11 dez. 2025.



medidas de expropriação indireta ou venda coercitiva de subsidiárias estrangeiras por alegada ameaça à segurança de informação, tal como se observa no precedente administrativo e legislativo norte-americano em relação ao TikTok³⁰. Porém, sem *enforcement* efetivo da proteção de dados e segurança da informação, sem *data centers* públicos de alta segurança, e sem governança eficiente de cibersegurança, a autodeterminação informativa do país permanece ilusória.

2.3 Dimensão infraestrutural

A soberania infraestrutural refere-se ao controle sobre as estruturas físicas que sustentam a operação dos sistemas digitais. Isso inclui redes de telecomunicação, cabos submarinos, data centers, nuvens de computação, clusters de alto desempenho e, sobretudo, a cadeia de suprimentos de semicondutores.

A dependência brasileira nesse campo é profunda. A maior parte da infraestrutura crítica é controlada e gerenciada por empresas privadas estrangeiras. Em razão de modelos de patrocínio de aplicativos em zero rating³¹, o acesso à internet móvel é artificialmente direcionado para um conjunto restrito de serviços, principalmente redes sociais do grupo Meta, que concentram dados de usuários e vêm explorando tal acesso privilegiado para criar novas dependências em serviços de IA generativa. O treinamento de modelos de IA depende de capacidade computacional de alto desempenho fornecida por *hyperscalers* estrangeiros. Não há produção relevante de semicondutores avançados e os data centers governamentais de alta segurança são ainda muito limitados.³²

A literatura jurídica e de políticas públicas reconhece que a soberania infraestrutural é o eixo central da autonomia tecnológica. Sem capacidade computacional própria, o Estado não consegue garantir que suas necessidades estratégicas sejam atendidas, especialmente em setores como pesquisa, defesa, saúde, energia, petróleo e gás, e finanças. Ademais, a dependência infraestrutural tende a ser explorada para acumular dados em bases proprietárias, gerar *insights* valiosos sobre setores inteiros da população ou da economia e utilizar tais dados para desenvolvimento de tecnologias de ponta, criando barreiras competitivas praticamente intransponíveis para empresas excluídas desse acesso privilegiado.³³

Por fim, dependência infraestrutural simultaneamente cria e amplifica riscos geopolíticos, pois fornecedores podem interromper serviços, aumentar preços, impor cláusulas contratuais

³⁰ YOUNG, Scott, Is the new US TikTok safer?

³¹ **Zero Rating**, Zero Rating, disponível em: <<https://zerorating.wordpress.com/publications/>>. acesso em: 10 dez. 2025.

³² Relatório Seminário Pilha IA Soberana.

³³ WU, Tim, **The Age of Extraction: How Tech Platforms Conquered the Economy and Threaten Our Future Prosperity**, [s.l.]: Knopf, 2025. RIKAP, **Dynamics of Corporate Governance Beyond Ownership in AI**; 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.



restritivas ou ser pressionados por governos estrangeiros. A falta de capacidade nacional para produzir ou ao menos encapsular chips (*packaging*) de última geração limita o desenvolvimento de modelos avançados de IA, diminui a competitividade do país e restringe sua participação em cadeias de valor global.

2.4 Dimensão lógica

A dimensão lógica diz respeito ao domínio sobre software, algoritmos, bibliotecas, frameworks, sistemas operacionais e padrões técnicos que constituem a base operacional das tecnologias digitais e da inteligência artificial. A soberania lógica é frequentemente negligenciada, mas é um elemento essencial da autonomia tecnológica. Sem capacidade de compreender, desenvolver e regular efetivamente essa camada, o Estado, bem como qualquer outro ator, não consegue auditar sistemas, verificar integridade algorítmica, modular infraestrutura, adaptar modelos às necessidades nacionais ou garantir conformidade com normas juridicamente vinculantes.

O Brasil depende quase integralmente de softwares estrangeiros proprietários ou parcialmente abertos, tanto em sistemas operacionais quanto em *frameworks* de IA. Isso impede auditoria ou modificação, limita interoperabilidade e cria dependência estrutural tecnológica. Neste contexto, a promoção do desenvolvimento e adoção em escala de tecnologias em *open source*, a garantia da interoperabilidade sistêmica, e o desenvolvimento de infraestruturas públicas digitais tornam-se ferramentas essenciais para alcançar a soberania digital na camada lógica.³⁴

Cabe frisar que padrões e protocolos técnicos funcionam, de fato, como normas privadas que podem ser utilizadas para promover a abertura e a colaboração ou, ao contrário, restringir a ação dos usuários de tecnologia, sejam tais usuários indivíduos, empresas ou administrações públicas. Se o Estado não promover a adoção e uso de padrões abertos, perde capacidade regulatória prática. A soberania lógica, portanto, exige políticas que promovam software livre, padrões abertos, repositórios públicos de modelos e bibliotecas nacionais de IA. Essa camada é especialmente crítica para IA, pois os modelos de fundação são a base lógica de aplicações avançadas em setores essenciais.

2.5 Dimensão de cibersegurança, ciberdefesa e segurança nacional

A soberania digital e a cibersegurança se fortalecem mutuamente e se sobrepõem parcialmente. A soberania depende de capacidade efetiva de proteger infraestruturas críticas, dados, serviços públicos essenciais e sistemas de IA contra-ataques, espionagem, manipulação ou interferência estrangeira. Ao mesmo tempo, a dependência tecnológica e,

³⁴ EUROPEAN WORKING TEAM ON DIGITAL COMMONS, *Towards a Sovereign Digital Infrastructure of Commons*, Paris, France: [s.n.], 2022.



consequentemente, a incapacidade de compreender, desenvolver e regular efetivamente ativos digitais prejudica e, em certos casos, impossibilita a cibersegurança.³⁵

Sem domínio técnico, inclusive sobre a origem, a lógica e as dependências de cada componente, torna-se impossível mapear vulnerabilidades, avaliar riscos sistêmicos, antecipar ataques sofisticados e formular políticas eficazes de resiliência cibernética. A soberania digital exige, portanto, autonomia cognitiva: a capacidade de compreender, auditar e governar de forma independente a infraestrutura tecnológica que sustenta a vida nacional.

O Brasil enfrenta desafios significativos nesse campo, especialmente pela grande dependência de soluções estrangeiras de cibersegurança. Embora tais soluções possam ser tecnicamente avançadas, a terceirização da cibersegurança para fornecedores internacionais, sujeitos a jurisdições e regulações de outros países, pode fragilizar a autonomia nacional. A dependência de softwares proprietários, equipamentos cujo código não é auditável e serviços de nuvem sem plena garantia de soberania jurídica cria vulnerabilidades que extrapolam a esfera técnica e se estendem ao campo jurídico e geopolítico.

Diante desse cenário, a construção de soberania digital requer medidas estruturais que extrapolam a simples formulação de uma legislação de cibersegurança, apesar de tal legislação ser necessária, como enfatizado explicitamente pela própria Estratégia Nacional de Cibersegurança (E-Ciber), instituída pelo decreto 12.573/2025. O Brasil necessita de um marco jurídico nacional, bem como de uma Agência Nacional de Cibersegurança com competências claras, autonomia técnica e capacidade operacional. Contudo, tais medidas institucionais devem ser acompanhadas de políticas industriais, educacionais e tecnológicas que estimulem o desenvolvimento e a adoção de soluções nacionais de cibersegurança.³⁶

Assim, a soberania digital constitui dimensão indissociável da segurança nacional e da defesa do Estado, na medida em que a infraestruturas digitais, sistemas de comunicação, e soluções de IA passaram a integrar o núcleo das capacidades estratégicas estatais. A dependência estrutural de tecnologias estrangeiras – especialmente quando controladas por empresas sujeitas a jurisdições externas e a regimes legais que autorizam acesso governamental a dados – cria vetores de vulnerabilidade que extrapolam o domínio econômico, alcançando riscos concretos de espionagem, sabotagem, interrupção de serviços críticos e coerção geopolítica.

No atual cenário de alta tensão internacional, conflitos híbridos e sanções comerciais, a possibilidade de suspensão unilateral de serviços de nuvem, restrição de atualizações de software, bloqueio de licenças ou imposição de sanções tecnológicas compromete a continuidade administrativa, a integridade de bases de dados sensíveis e a operacionalidade de sistemas de comando e controle. A soberania digital, nesse contexto, não se limita à proteção contra-ataques externos, mas envolve a garantia de que o Estado detenha domínio efetivo e resiliente sobre a arquitetura tecnológica que

³⁵ 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; BELLI, Luca; PAULI, Breno; COUTO, Natália, **Governança da cibersegurança no Brasil: entender o passado, esclarecer o presente e construir o futuro**.

³⁶ BELLI, Luca *et al*, **Governança e regulação da cibersegurança no Brasil**, [s.l.: s.n.], 2025.



sustenta suas funções essenciais, inclusive defesa, inteligência, finanças públicas e infraestrutura crítica.

Paralelamente, o direcionamento de investimentos públicos – notadamente por meio de compras governamentais, encomendas tecnológicas e políticas de inovação orientadas por missão, como se destacara na Seção 3.2 – pode catalisar a formação de cadeias produtivas nacionais em áreas como semicondutores, computação em nuvem, criptografia e IA. Tal estratégia não apenas reduz vulnerabilidades externas, mas também estimula a geração de empregos qualificados, a retenção de talentos e a criação de propriedade intelectual doméstica, com efeitos multiplicadores sobre a produtividade e a competitividade internacional do País.

A soberania digital, portanto, deve ser compreendida simultaneamente como política de segurança e como política de desenvolvimento: ao mitigar riscos estratégicos decorrentes da dependência tecnológica, o Estado também cria condições para dinamizar o mercado interno, fortalecer sua base industrial e, no longo prazo, garantir que a defesa do Estado seja operada sob controles jurisdicionais plenamente brasileiros.

2.6 Dimensão de interdependência instrumentalizada

O uso de tecnologias digitais é afetado por riscos sistêmicos que não podem ser mitigados apenas por leis ou instituições nacionais. Esses riscos resultam da interdependência entre países, da concentração de mercado em plataformas globais, de vulnerabilidades nas cadeias de suprimentos, da dependência de nuvens estrangeiras e do desequilíbrio de poder entre Estados e corporações. A literatura de governança digital destaca que empresas globais podem impor arquiteturas técnicas e contratuais que substituem normas jurídicas, limitando a atuação de outros países ou empresas explorando dependências difíceis de reverter.³⁷

A soberania digital precisa ser compreendida à luz das vulnerabilidades inerentes às redes globais altamente interconectadas que estruturam a economia e a tecnologia contemporâneas. Embora a globalização tenha ampliado positivamente fluxos de informação, capital e bens, ela também consolidou topologias de rede profundamente assimétricas, nas quais poucos países, sobretudo os Estados Unidos e, em determinadas cadeias, a China, concentram posições de controle sobre infraestruturas críticas. Esses *hubs* acumulam vantagens sistêmicas e podem explorar posições para transformar a interdependência em dependências estruturais, fragilizando a autonomia de países periféricos ou semiautônomos. Trata-se de uma condição que ameaça diretamente a soberania digital, pois reduz a capacidade de um Estado de governar seus próprios recursos tecnológicos e informacionais.

É nesse contexto que se manifesta a chamada “interdependência instrumentalizada” (*weaponized interdependence*), caracterizada pelo uso coercitivo das posições centrais nas redes globais. O primeiro mecanismo desse fenômeno é o efeito panóptico, pelo qual o controle de infraestruturas estratégicas permite a extração de conhecimento sensível. O segundo é o efeito estrangulamento (*chokepoint*), pelo qual Estados controladores restringem

³⁷ FARRELL, Henry; NEWMAN, Abraham L., *Weaponized Interdependence: How Global Economic Networks Shape State Coercion*, **International Security**, v. 44, n. 1, p. 42–79, 2019.



o acesso de terceiros a tecnologias essenciais, impondo custos econômicos e políticos severos.³⁸

Nos últimos anos, tais mecanismos tornaram-se particularmente visíveis nas cadeias de semicondutores e de minerais críticos. Os Estados Unidos impuseram restrições amplas à exportação de chips avançados, equipamentos de litografia e *know-how* associado, limitando o acesso de diversos países – especialmente a China e outros membros do BRICS – a tecnologias indispensáveis para sistemas de IA, computação de alto desempenho e aplicações militares. Essas medidas evidenciam o poder estrutural derivado do domínio de patentes, design e equipamentos especializados.

Em resposta, a China intensificou controles sobre exportações de minerais críticos processados, como gálio e germânio, insumos essenciais para a fabricação de semicondutores, telecomunicações e tecnologias de energia. Essa dinâmica revela que ambos os lados buscam instrumentalizar suas posições na cadeia global, transformando recursos industriais em instrumentos de pressão geopolítica.

A instrumentalização da interdependência leva Estados vulneráveis a buscar alternativas que minimizem riscos. Como será abordado na próxima seção, para o Brasil, compreender esse cenário é importante: dependências em semicondutores estrangeiros, nuvens públicas internacionais, plataformas digitais oligopolizadas e cadeias de suprimento concentradas aumentam a exposição do país tanto ao efeito panóptico quanto ao efeito estrangulamento.

³⁸ *Ibid.*



3 Diagnóstico do Cenário Brasileiro

O diagnóstico do cenário brasileiro em soberania digital exige uma análise integrada das dimensões regulatórias, institucionais, tecnológicas e industriais. A partir dessa matriz conceitual, observa-se que o país possui capacidades relevantes, especialmente em âmbito científico, mas enfrenta limitações graves em infraestruturas de hardware, conectividade significativa, governança de dados, padronização, integração institucional e capacidade industrial em semicondutores e hardware acelerador.

Como apontado ao longo do Seminário Nacional “Pilha de IA: Desafios para Autonomia Tecnológica e Soberania Digital”,³⁹ o Brasil opera com um déficit estrutural que dificulta, ou até impede, a produção de modelos avançados de IA, atrapalha a reprodutibilidade científica, limita a autonomia informacional e reduz a competitividade nacional. É nesse contexto que o diagnóstico deve examinar, de forma sistemática, o marco regulatório, a política de inovação, a infraestrutura nacional, o ecossistema científico e industrial e a governança institucional vigente.

3.1 Marcos regulatórios distantes da realidade: dados, conectividade significativa e IA

O arcabouço regulatório brasileiro possui importantes instrumentos jurídicos, mas ainda carece de coerência sistêmica, densidade normativa e efetividade suficiente para lidar com os desafios contemporâneos. A LGPD constitui referência essencial e define a autodeterminação informativa como um princípio fundamental em seu artigo 2º, mas sua aplicação permanece limitada. Diversos estudos empíricos recentes⁴⁰ – em setores digitais críticos como redes sociais, comércio eletrônico e IA generativa – e avaliações conduzidas pelo TCU⁴¹ demonstram que a fiscalização e o *enforcement* da LGPD seguem insuficientes, afetados por restrições de capacidade institucional, baixa transparência das plataformas e ausência de mecanismos de verificação e fiscalização capazes de acompanhar a sofisticação dos sistemas digitais.

O cenário de conectividade revela desafios ainda mais profundos. Apesar dos dados quantitativos oferecerem um cenário positivo, as análises qualitativas revelam uma situação radicalmente diferente. O artigo 7º do Marco Civil da Internet prescreve que “o acesso à internet é essencial ao exercício da cidadania”. Segundo o relatório do CETIC.br, apenas cerca de 22% da população brasileira possui conectividade significativa, isto é, acesso à internet de

³⁹ Relatório Seminário Pilha IA Soberana.

⁴⁰ BELLI, Luca *et al*, **Redes sociais e LGPD**, [s.l.: s.n.], 2025; **IA Generativa e LGPD: transparência, desafios regulatórios e caminhos para a conformidade**, disponível em: <<https://repositorio.fgv.br/items/ddb2b6b5-d069-42d3-88c8-ac10b9ee3908>>. acesso em: 10 dez. 2025.

⁴¹ Auditoria realizada pelo Tribunal de Contas da União revelou que grande parte das organizações federais avaliadas descumpre dispositivos essenciais da LGPD, identificando falhas significativas em governança e práticas de tratamento de dados pessoais, e segurança da informação. UNIÃO, Tribunal de Contas da, **Auditoria aponta falhas na aplicação da LGPD por organizações federais – Notícias**, Portal TCU, disponível em: <<https://portal.tcu.gov.br/imprensa/noticias/auditoria-aponta-falhas-na-aplicacao-da-lgpd-por-organizacoes-federais>>. acesso em: 11 dez. 2025.



velocidade e condições que permitam o uso pleno, produtivo e não restrito da conexão.⁴² A maior parte dos brasileiros acessa a internet por meio de redes sociais, com planos móveis limitados ou dependentes de práticas de *zero rating*, o que aprofunda desigualdades, distorce a concorrência e condiciona o sucesso de um serviço a sua capacidade econômica ao invés da sua inovação.

No campo regulatório de IA, o Brasil ainda não dispõe de legislação compreensiva. Tramitam no Congresso propostas como o Projeto de Lei nº 2338 junto com pelo menos quinze outros projetos de lei⁴³, mas nenhuma delas foi aprovada. A ausência de um marco jurídico deixa sem regulamentação aspectos essenciais, não somente no que diz respeito à classificação de risco, padrões obrigatórios de transparência e documentação, exigências de supervisão humana, auditorias independentes e governança de modelos utilizados, mas também – criticamente – como estimular o desenvolvimento de sistemas de IA pelo poder público ou por setores estratégicos.

Neste cenário, recentemente, foi proposta pelo executivo a criação do Sistema Nacional para Desenvolvimento, Regulação e Governança de Inteligência Artificial⁴⁴, que além de sanar questões de vício de iniciativa, busca "organizar a atuação coordenada e estratégica do Poder Executivo Federal face à inteligência artificial". Todavia, nota-se que a legislação ainda pouco avança na estruturação de instrumentos necessários para construir capacidades nacionais soberanas.

Essa lacuna é crítica, pois a soberania digital não se sustenta apenas sobre normas de conduta ou intenções programática, mas exige o domínio material das cadeias de valor tecnológico. Observa-se uma desconexão entre a agenda regulatória e a necessidade premente de fomento à infraestrutura computacional de alto desempenho (*High Performance Computing*), à disponibilização de *datasets* governamentais curados para treinamento de modelos e ao incentivo à criação de algoritmos nativos, à estruturação de unidades estratégicas para análise prospectiva de tendências ou para acompanhamento de missões estratégicas.

Ao concentrar esforços desproporcionais na mitigação de riscos sem a contrapartida de uma política de CT&I ativa, orientada por missões e apoiada pelo poder de compra do Estado, o Brasil corre o risco de copiar e colar o modelo europeu – especialmente em seus elementos mais disfuncionais citados acima – estabelecendo um ambiente jurídico sofisticado, porém inefetivo, que na melhor das hipóteses pode regular superficialmente tecnologias importadas. Tal abordagem perpetuaria a dependência tecnológica e a inefetividade regulatória e limitaria o país à posição de consumidor passivo de soluções desenvolvidas em jurisdições que aliam, de forma agressiva, regulação e subsídios industriais.

⁴² NIC.BR, **Conectividade significativa: propostas para medição e o retrato da população no Brasil**, São Paulo: CGI.br, 2024.

⁴³ BELLI, Luca, *Towards AI Regulation in Brazil: Past Policies, Future Paths, and Present Uncertainties*. [S.l.]: [s.n.], [s.d.].

⁴⁴ NACIONAL, Imprensa, **DESPACHO DO PRESIDENTE DA REPÚBLICA - DOU - Imprensa Nacional**, disponível em: <<https://www.in.gov.br/en/web/dou/-/despacho-do-presidente-da-republica-673947267>>. acesso em: 10 dez. 2025.



Portanto, cabe ressaltar que a mera adoção de marcos regulatórios deveria ser enxergada como uma etapa necessária, porém não suficiente para garantir a soberania digital, como será destacado ao longo deste texto. De um lado, a criação de mecanismos efetivos e eficientes de fiscalização e *enforcement* é essencial. De outro lado, a governança da soberania digital deve necessariamente permitir a comunicação e a sinergia entre regulação e políticas de fomento à inovação, ao desenvolvimento de tecnologias digitais.

3.2 Políticas de inovação e instrumentos de fomento existentes

O Brasil possui instrumentos de fomento relevantes, mas insuficientes para sustentar projetos estruturais de longo prazo. Cabe frisar que os fundos setoriais, os recursos do supramencionado Fundo Nacional de Desenvolvimento Científico e Tecnológico (FNDCT), os programas de bolsas e os editais de P&D fornecem suporte pontual à pesquisa acadêmica, mas não criam uma política industrial integrada para semicondutores, hardware acelerador, nuvens soberanas ou produção de modelos de IA em larga escala.⁴⁵

Conquanto existam programas de financiamento ao desenvolvimento tecnológico, o Brasil não logrou alcançar soberania digital em virtude do caráter pontual e desarticulado de tais instrumentos. A disponibilização de recursos, per se, mostra-se insuficiente. Como frisado em precedência, impõe-se a implementação de um modelo de financiamento orientado por missões (*mission-driven*), estruturado para conferir ao país capacidades tecnológicas determinadas e soberania em áreas estratégicas específicas, mediante coordenação sistêmica das políticas públicas de fomento à inovação.⁴⁶

Além disso, apesar dos avanços propostos pelo Plano Brasileiro de IA (PBIA), ainda há notável escassez de programas orientados ao desenvolvimento de infraestrutura crítica, e o país não possui mecanismos de financiamento contínuo comparáveis aos adotados por lideranças globais como Estados Unidos, China ou União Europeia.

Embora o ordenamento brasileiro preveja instrumentos voltados a promoção da inovação por meio de compras públicas, esses instrumentos são raramente direcionados ao fomento de tecnologias digitais nacionais e ao desenvolvimento de componentes essenciais de sistemas de IA, como Unidade de Processamento Gráfico (GPUs), sistemas operacionais, bibliotecas de execução ou frameworks de MLOps, e outras ferramentas voltadas a automatizar, gerenciar e otimizar todo o ciclo de vida do aprendizado de máquina.

⁴⁵ Tal diagnóstico foi detalhado de maneira eloquente ao longo das seções do seminário Pilha de IA: Desafios para Autonomia Tecnológica e Soberania Digital”. Veja-se o Relatório Seminário Pilha IA Soberana.

⁴⁶ MAZZUCATO, Mariana; PENNA, Caetano C. R., **Mission-Oriented Finance for Innovation**. [s.l.]: Bloomsbury Publishing PLC, 2015; **Industrial and Corporate Change**, v. 27, n. 5, p. 803–815, 2018; MAZZUCATO, Mariana; Mission-oriented innovation policies: challenges and opportunities.



Pesquisas recentes⁴⁷ destacam a existência de pelo menos sete instrumentos de compras públicas previstos na Lei nº 14.133/2021 que são adequados para estimular a pesquisa, o desenvolvimento e inovação digital brasileira. 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.

Cabe frisar, contudo, que os instrumentos de fomento atuais seguem um modelo fragmentado, pouco coordenado e submetido a ciclos orçamentários instáveis. A ausência de um programa plurianual dedicado ao desenvolvimento de um ecossistema digital brasileiro tecnologicamente autônomo compromete a continuidade dos projetos, os quais dependem de renovação anual de recursos. Essa volatilidade impede a consolidação de equipes especializadas, a formação de redes nacionais de pesquisa, a cooperação entre indústria e academia e a internacionalização de capacidades científicas. Ademais, a baixa articulação entre o sistema de regulação e o de fomento com a demanda pública impede que as compras governamentais gerem escala e sustentabilidade para iniciativas nacionais. Tal falta de continuidade e estímulo à indústria nacional é refletida na dependência infraestrutural, já mencionada acima.

3.3 Infraestrutura nacional: nuvens públicas, data centers, HPC e redes de pesquisa

As dependências, deficiências e ineficiências infraestruturais brasileiras são um dos pontos centrais deste diagnóstico. Os centros de supercomputação do país, ainda que importantes, não formam uma rede nacional integrada; utilizam arquiteturas heterogêneas, carecem de padrões unificados de MLOps e enfrentam limitações severas para treinar modelos de larga escala.⁴⁸ A situação é agravada pela escassez de GPUs avançadas e pela inexistência de aquisições coordenadas de hardware acelerador, o que impede a formação de clusters nacionais de classe mundial.⁴⁹

As nuvens públicas existentes utilizam arquiteturas e soluções fragmentadas, frequentemente caracterizadas por dependências estruturais de serviços e tecnologias críticas estrangeiras em múltiplas camadas, o que compromete a soberania e dificulta a implementação de padrões de segurança e conformidade. Os data centers governamentais operam com capacidades limitadas, sem redundância e sem padrões avançados de segurança física ou cibernética necessários para hospedar dados sensíveis em larga escala. Por fim, as redes acadêmicas e de pesquisa, embora estratégicas para cooperação científica, ainda não dispõem de

⁴⁷ 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.

⁴⁸ Relatório Seminário Pilha IA Soberana.

⁴⁹ *Ibid.*



throughput (capacidade efetiva de transferência de dados por unidade de tempo) compatível com as demandas de IA moderna, o que restringe o intercâmbio de grandes volumes de dados e o acesso eficiente a infraestrutura de treinamento e inferência, limitando parcerias e projetos de ciência em rede.⁵⁰

Nesse sentido, a expansão da nuvem soberana e da infraestrutura brasileira de computação de alto desempenho deveria ser priorizada a fim de possibilitar a construção de um ecossistema digital autônomo, o desenvolvimento de modelos e sistema de IA brasileiros avançados e a garantia de que dados estratégicos permaneçam protegidos sob jurisdição nacional. Não obstante sua abrangência limitada, merece menção a “Nuvem de Governo”, iniciativa coordenada pelo MGI em parceria com SERPRO e DATAPREV, que disponibiliza a cerca de 250 órgãos federais catálogos de serviços de computação em nuvem pública e híbrida, com o propósito de garantir soberania sobre dados sensíveis e infraestrutura nacional.⁵¹

Cabe ressaltar que ações relativas à computação em nuvem integram, igualmente, outras políticas governamentais, como o PBIa e E-Digital (apesar desta última estratégia estar em fase de reformulação), demonstrando um esforço, ainda que fragmentário, de incorporação da temática da soberania digital no planejamento estratégico nacional. Porém, a inexistência de uma arquitetura federativa de supercomputação impede que instituições compartilhem recursos e limita a capacidade coletiva do sistema científico. Essa deficiência estrutural permanece a despeito de esforços para a criação de consórcios federados, como aqueles coordenados pelo Laboratório Nacional de Computação Científica (LNCC) em parceria com outras instituições, destinados à disponibilização de recursos de computação de alto desempenho em camadas de distribuição aberta, evidenciando a ausência de coordenação sistêmica necessária à otimização da infraestrutura científica nacional. Assim, a definição de padrões técnicos comuns entre instituições é essencial para evitar desperdícios, redundâncias e ineficiências operacionais.

3.4 Ecossistema científico e industrial: capacidades, fragilidades e lacunas

O Brasil possui um ecossistema científico robusto com produção acadêmica ampla e de alto nível, sendo um exportador de talentos. O Brasil mantém uma comunidade científica e acadêmica de alta qualidade nas áreas de ciência de dados, engenharia da computação, matemática e outras disciplinas de base, com produção ampla e reconhecida internacionalmente. Muitos desses profissionais têm atuado com destaque no exterior.

Esse capital humano demonstra que o país possui o substrato intelectual necessário para sustentar um ecossistema nacional de IA e tecnologia de ponta, desde que amparado por políticas consistentes de infraestrutura, financiamento e governança. Entretanto, esse

⁵⁰ *Ibid.*

⁵¹ EM 10/06/2025 19H49, Publicado em 10/06/2025 17h18 Atualizado, **Gestão, Serpro e Dataprev lançam serviços de nuvem de governo para órgãos federais**, Ministério da Gestão e da Inovação em Serviços Públicos, disponível em: <<https://www.gov.br/gestao/pt-br/assuntos/noticias/2025/maio/gestao-serpro-e-dataprev-lancam-servicos-de-nuvem-de-governo-para-orgaos-federais>>. acesso em: 4 jan. 2026.



potencial convive com uma vulnerabilidade crítica: o êxodo de cientistas e pesquisadores qualificados, a chamada “fuga de cérebros”. Estimativas recentes apontam que entre 2015 e 2022 o Brasil perdeu cerca de 6,7 mil pesquisadores que migraram para instituições no exterior.⁵²

Além de dificuldade em retenção de talentos, o país sofre com claros limites no que diz respeito a capacidade industrial. A produção de hardware é incipiente ou inexistente em semicondutores avançados. O país ainda não possui capacidade de fabricação de chips de ponta, nem política industrial coordenada para desenvolver uma cadeia nacional de microeletrônica, apesar dos esforços em curso no âmbito do PBIa e o novo PADIS.

Como destacado acima, um dos maiores gargalos é a dependência de GPUs estrangeiras, cujo acesso é limitado, caro (em função dos preços das GPUs em si, combinados com uma política tarifária expressiva) e sujeito a restrições geopolíticas e de demanda. Essa dependência dificulta a consolidação de startups brasileiras que precisariam de infraestrutura intensiva em computação.

Apesar disso, a indústria de software possui capacidades relevantes, mas não atua de maneira coordenada. O ecossistema de startups de software é vibrante⁵³, porém limitado pela dependência de infraestruturas estrangeiras, carência de modelos nacionais, ausência de dados públicos interoperáveis. Além disso, a produção de tecnologia digital nacional, concentrada em setores estratégicos, como petróleo e finanças, ocorre de maneira isolada e sem articulação federal.

Considerado o potencial do setor de software, esse setor deveria ser alavancado para reconstruir a autonomia tecnológica nacional. O ecossistema de software precisa ser estrategicamente impulsionado, sobretudo por meio do fortalecimento do software livre. De um lado, isso possibilitaria o desenvolvimento de alternativas abertas a plataformas estrangeiras dominantes de comunicação e colaboração – como o *Microsoft Teams* ou o *Google Workspace* – estimulando a integração e adoção de soluções de IA brasileira em ampla escala. Isto é a adoção de plataformas com IA pátria, por exemplo, no âmbito de toda a administração pública, de toda a educação pública, ou de todas as forças armadas, em vez de adotar – e trabalhar gratuitamente para treinar com dados nacionais extremamente valiosos⁵⁴ – os sistemas de IA estrangeiros⁵⁵. De outro, permitiria criar soluções capazes de explorar

⁵² **Fuga de cérebros: o que o Brasil faz para evitar saída de cientistas?** – ABC – Academia Brasileira de Ciências, disponível em: <https://www.abc.org.br/2025/09/01/fuga-de-cerebros-o-que-o-brasil-faz-para-evitar-saida-de-cientistas/?utm_source=chatgpt.com>. acesso em: 10 dez. 2025.

⁵³ ASSOCIAÇÃO BRASILEIRA DAS EMPRESAS DE SOFTWARE, **Mercado Brasileiro De Software: Panorama E Tendências 2008**, [s.l.]: Abes, 2024.

⁵⁴ **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: 4 jan. 2026.

⁵⁵ Cabe frisar que provedores de plataformas dominantes estrangeiras, tais que Meta, Microsoft ou Google, adicionam automaticamente seus sistemas de IA, explorando a posição privilegiada dessas plataformas para “prender” consumidores, por meio do supracitado fenômeno do *lock-in*, e obter domínio em novos mercados relacionado à IA. BELLÍ *et al*, **Soberania Digital e Inteligência Artificial no Brasil: rumo à autonomia tecnológica**. RIO DE JANEIRO, RJ: Lumen Juris, 2026.



integralmente o hardware avançado. Hoje, o uso pleno de GPUs de ponta, como as da NVIDIA, depende de softwares proprietários – como o CUDA e AI Enterprise da NVIDIA – cujo acesso exige licenças contínuas mesmo após a aquisição do equipamento, aprofundando a dependência tecnológica e prejudicando a soberania digital.

3.5 Minerais críticos: uma oportunidade “de ouro”

A relevância estratégica das vastas reservas de minerais críticos no Brasil revela-se de forma cada vez mais nítida no contexto da soberania digital e da economia de tecnologia avançada. O Brasil detém percentuais expressivos das reservas globais de elementos essenciais como nióbio (com quase totalidade das reservas mundiais) e significativa participação em grafite, lítio e terras raras⁵⁶. Tais insumos são indispensáveis para a fabricação de semicondutores, baterias, ímãs permanentes e diversos componentes eletrônicos que constituem a espinha dorsal das cadeias produtivas de alta tecnologia e da economia digital global.

Esses minerais não apenas sustentam a transição energética, veículos elétricos e sistemas de armazenamento de energia, mas também são cruciais para chips avançados, sensores e comunicações, elementos imprescindíveis à infraestrutura digital, à defesa e às capacidades de comando, controle e sensoriamento em ambientes de conflito. Cabe ressaltar que a dependência de importações de matérias-primas processadas e de componentes intermediários intensifica vulnerabilidades geopolíticas⁵⁷, pois apenas a fase de extração no território não assegura controle tecnológico nem agrega valor suficiente à economia nacional, deixando o Brasil prisioneiro de cadeias globais em que o beneficiamento, refino e manufatura final são realizados por atores externos, com captura da maior parte da renda e do know-how tecnológico.

Diante desse quadro, é essencial a adoção de uma política nacional que vá além da mera extração de commodities minerais e que tenha como foco central a “agregação de valor” e o desenvolvimento de capacidades industriais domésticas plenamente integradas às cadeias globais de semicondutores e tecnologias avançadas. Essa política deve incluir estímulos decisivos à pesquisa e desenvolvimento, à ampliação de unidades de refino e processamento dentro do país, e à formação de mão de obra especializada, de modo a incorporar o Brasil nas etapas mais avançadas da produção tecnológica.

Nesse sentido, a criação de uma empresa estatal estruturada de forma análoga à Petrobras, voltada especificamente para a coordenação da exploração, processamento e integração de minerais críticos – seja sob a forma de corporação pública de capital misto ou sociedade anônima de controle federal – emerge como opção de alta relevância estratégica que merece particular atenção. Essa entidade teria por missão articular e internalizar capacidades tecnológicas e industriais, garantindo que os recursos naturais brasileiros não sejam apenas

⁵⁶ SURVEY, U. S. Geological, **Mineral commodity summaries 2025**, [s.l.]: U.S. Geological Survey, 2025.

⁵⁷ MONTANO, David, Critical Dependence on Rare-Earth Minerals.



exportados como matérias-primas, mas convertidos em produtos de maior valor agregado, como semicondutores, componentes eletrônicos e materiais avançados, que sustentem tanto a economia digital quanto a soberania tecnológica do Estado.

O Brasil detém parcela significativa das reservas mundiais de determinados minerais estratégicos, com ocorrências relevantes nos Estados do Amazonas, Bahia, Goiás, Minas Gerais e Sergipe, o que lhe confere vantagem geoeconômica potencial. Contudo, a mera disponibilidade geológica não se converte automaticamente em poder estratégico. A experiência internacional demonstra que os Estados mais bem posicionados na disputa pelo domínio das terras raras e demais minerais críticos não têm se limitado à regulação passiva do mercado, mas vêm adotando intervenções diretas, combinando instrumentos de política industrial, financiamento público, restrições à exportação de insumos estratégicos e participação acionária estatal em empreendimentos minerários e industriais.⁵⁸

Impõe-se, portanto, ação célere e coordenada do Estado brasileiro, com a formulação de políticas específicas para o setor, governança multissetorial altamente integrada, e robustos investimentos em pesquisa e desenvolvimento. É indispensável, ademais, gerar ou adquirir domínio tecnológico sobre métodos de prospecção, extração e beneficiamento – cuja complexidade técnica e riscos ambientais⁵⁹ exigem elevada especialização – bem como estruturar capacidade nacional de refino e processamento químico, etapas nas quais se concentra a maior parte do valor agregado e do conhecimento sensível. Sem essa ascensão na cadeia produtiva, o País permanecerá na posição periférica de exportador de matéria-prima bruta; com ela, poderá consolidar base material consistente para sua soberania digital, industrial e defensiva.

3.6 A implementação do PBIA: o começo da jornada rumo à autonomia tecnológica

O PBIA representa marco normativo e programático relevante na consolidação de uma estratégia nacional voltada à soberania digital. Estruturado em eixos que abrangem infraestrutura computacional, formação de capital humano, inovação empresarial, aplicação governamental e apoio à governança regulatória, o Plano delineia arquitetura institucional coerente com os desafios contemporâneos da economia digital. Mais do que um conjunto de iniciativas isoladas, o PBIA inaugura racionalidade sistêmica de política pública, articulando instrumentos financeiros, regulatórios e operacionais em torno da construção de capacidades estratégicas de longo prazo, que podem ser monitorados por meio de métricas específicas.⁶⁰

⁵⁸ *Ibid.*

⁵⁹ HAN, Yong-He *et al*, Environmental impacts of rare earth elements mining and strategies for sustainable management: A comprehensive review, **Journal of Hazardous Materials**, v. 500, p. 140400, 2025.

⁶⁰ **Plano Brasileiro de Inteligência Artificial**, Ministério da Ciência, Tecnologia e Inovação, disponível em: <<https://www.gov.br/mcti/pt-br/acompanhe-o-mcti/transformacaodigital/plano-brasileiro-de-inteligencia-artificial>>. acesso em: 2 mar. 2026.



No campo da infraestrutura, o fortalecimento da capacidade nacional de computação de alto desempenho constitui elemento central. A ampliação do parque de supercomputação e a modernização de redes acadêmicas e centros nacionais de processamento de dados representam passos concretos para mitigar vulnerabilidades associadas à dependência externa de capacidade computacional. Em um cenário internacional caracterizado pela concentração de poder tecnológico em poucos países e grandes corporações, a posse e o controle de infraestrutura crítica – incluindo datacenters sob jurisdição nacional – são requisitos indispensáveis. A expansão planejada dessas capacidades, apesar de se encontrar ainda em fase inicial de expansão, sinaliza compromisso com a internalização de ativos essenciais à pesquisa científica, ao desenvolvimento industrial e à formulação de políticas públicas baseadas em dados.

No eixo da formação e capacitação, observa-se expansão significativa da oferta educacional em inteligência artificial e áreas correlatas.⁶¹ O aumento de vagas em cursos de graduação e pós-graduação, a concessão de bolsas de pesquisa e a realização de programas de capacitação profissional em larga escala evidenciam reconhecimento de que capital humano é fundamento da soberania tecnológica. A consolidação de massa crítica de pesquisadores, engenheiros, cientistas de dados e gestores públicos qualificados é condição indispensável para que o País não apenas consuma tecnologia, mas participe ativamente de sua concepção, desenvolvimento e regulação. Trata-se de investimento estruturante, cujos efeitos transcendem o horizonte imediato do Plano e incidem sobre a competitividade nacional de longo prazo.

A criação de estruturas dedicadas à coordenação de soluções de IA na administração pública federal, a capacitação de servidores e a implementação de projetos-piloto em áreas estratégicas indicam movimento de internalização de competências tecnológicas no aparelho estatal.⁶² A construção de infraestrutura de dados integrada e a implementação de ambientes computacionais sob controle governamental reforçam a capacidade do Estado de exercer suas funções com maior eficiência e autonomia. Nesse contexto, a perspectiva de uma nuvem soberana, destinada à custódia de dados sensíveis, assume centralidade como instrumento de proteção da informação pública e de redução de dependências externas.

No âmbito empresarial, os mecanismos de fomento à inovação – por meio de crédito, subvenção econômica e parcerias público-privadas – têm estimulado o desenvolvimento de soluções em inteligência artificial aplicadas a múltiplos setores produtivos. A mobilização de instituições financeiras públicas e agências de inovação revela compreensão de que soberania digital não se constrói apenas no setor público, mas exige tecido empresarial dinâmico, capaz de transformar conhecimento em produtos, serviços e processos de alto valor agregado.⁶³

⁶¹ **OBIA**, OBIA, disponível em: <<https://obia.nic.br/>>. acesso em: 2 mar. 2026.

⁶² **Plano Brasileiro de Inteligência Artificial**.

⁶³ *Ibid.*



Apesar dos avanços já observáveis, cumpre reconhecer que o estágio atual corresponde apenas ao início de trajetória complexa e prolongada. A construção da soberania digital é processo incremental, cumulativo e intensivo em conhecimento. Requer estabilidade normativa, previsibilidade regulatória e compromisso político duradouro. O PBIa já estabelece fundamentos relevantes – infraestrutura, capital humano, governança e estímulo à inovação – que sinalizam mudança positiva de paradigma na política tecnológica nacional.

Entretanto, a consolidação da autonomia estratégica brasileira no domínio da IA – e na esfera digital *latu sensu* – dependerá da capacidade de transformar iniciativas em resultados sustentáveis, de assegurar coordenação entre múltiplos atores e de manter visão de longo prazo. O que se observa até o momento é a edificação das bases de um projeto nacional; sua plena realização, contudo, demandará perseverança, investimentos continuados e aperfeiçoamento constante das políticas públicas.

3.7 Governança institucional e atores envolvidos

Como mencionado acima, a governança dos elementos necessários à construção da soberania digital no Brasil é fragmentada. Não existe uma autoridade central com competência para coordenar políticas de infraestruturas, dados, sistemas de IA e segurança cibernética e as autoridades e sistemas existentes ou propostos continuam mantendo-se isoladas ou se sobrepõem. Diversos órgãos exercem atribuições sobre aspectos relacionados à autonomia tecnológica, mas sem mecanismos de coordenação efetivos. Ministérios, autoridades reguladoras, universidades, centros de supercomputação e agências de fomento operam de forma desarticulada e, frequentemente, orientados por objetivos divergentes. Neste contexto, é essencial considerar não somente a função fundamental da CT&I, como força estruturante da soberania digital, mas também o papel essencial que o MCTI deve desempenhar como entidade articuladora com capacidade institucional.

Atualmente, inexistem fóruns capazes de garantir uma articulação sólida e estável entre indústria, academia e governo voltados especificamente para o ecossistema digital nacional, o que impede a construção de políticas industriais sustentadas. Embora existam iniciativas com caráter (mais ou menos) multissetorial, essas instâncias apresentam fragilidade institucional e são alvo de críticas em razão de possível captura por interesses de grandes empresas estrangeiras que financiam as principais associações do setor. Tal dependência financeira compromete a autonomia decisória desses espaços e suscita dúvidas quanto à sua capacidade de representar legitimamente o interesse nacional na formulação de políticas de soberania digital. Além disso, várias empresas nacionais são integradoras de soluções estrangeiras dominantes, o que de fato impede seu posicionamento mais crítico em relação a certos tipos de dependência tecnológica. Neste contexto, a ausência de governança federativa impede que atores público, privados e acadêmicos colaborem em rede.

A única instância de governança existente que poderia ser mobilizada para estimular comunicação, coordenação e cooperação é o Comitê Interministerial sobre Transformação



Digital (CITDigital). Contudo, não está claro como essa instância se coordenaria com o recém proposto Conselho Brasileiro para Inteligência Artificial (CBIA) e o novo Sistema Nacional para Desenvolvimento, Regulação e Governança de Inteligência Artificial.⁶⁴ Para evitar duplicações, sobreposições e conflitos de competências, será necessário um esforço de simplificação e otimização de estruturas, de modo a aproveitar o que já existe e fortalecer o que está sendo criado. O fato de o Sistema proposto ser regulamentado pelo poder executivo permitirá esse tipo de simplificação e coordenação, em tese. Porém, é impossível atualmente avaliar se tal sinergia de fato acontecerá.

Assim, a governança atual deve ser aprimorada para integrar e coordenar os atores brasileiros dos setores de infraestrutura, hardware, software, dados, modelos de IA e aplicações em um sistema coerente. Sem uma governança multissetorial robusta, uma autoridade de coordenação, e sem instrumentos de cooperação, o país permanecerá operando com capacidades dispersas e fragmentadas.

⁶⁴ BRASIL. Presidência da República. **Despacho do Presidente da República**. *Diário Oficial da União*, Brasília: Imprensa Nacional, 2025.



4 Experiências Internacionais Relevantes

A trajetória global em direção à soberania digital revela múltiplos experimentos, arranjos institucionais, tecnológicos e regulatórios que buscam assegurar a autonomia tecnológica face às transformações profundas da economia e da geopolítica da tecnologia. Diversas nações têm articulado, com graus variados, políticas de infraestrutura, regulação de dados, estímulo à indústria local e promoção de software (aberto) como vetores de desenvolvimento tecnológico e soberania nacional.

A análise comparativa dessas experiências fornece insumos valiosos para formulação de uma visão estratégica para o Brasil, demonstrando que autonomia tecnológica não é sinônimo de isolamento, mas de capacidade de decisão sobre normas, ferramentas e infraestrutura. Nesta seção, examinamos sete casos representativos, que destacam iniciativas relevantes lideradas por países (ou conjunto de) com capacidades e dimensões extremamente heterogêneas: os dos Estados Unidos, da China, da União Europeia e, mais recentemente, as iniciativas da Suíça e da Finlândia, acompanhados por Uruguai, México e Índia.

4.1 Estados Unidos: a administração pública como cliente âncora

Nos Estados Unidos, a atuação conjunta do setor público, academia e indústria configura-se como um modelo consolidado de fomento e demanda estratégica. A administração federal, por meio de agências como a *Defense Advanced Research Projects Agency* (DARPA), a *National Science Foundation* (NSF) e institutos de pesquisa como o *National Institutes of Health* (NIH), tem historicamente estimulado maciçamente investimentos em pesquisa e desenvolvimento, consolidando uma base científica que alimenta a indústria privada.⁶⁵ As compras públicas estratégicas, especialmente em áreas de defesa, (ciber)segurança, saúde e tecnologia, funcionam como mecanismo de escala, gerando mercado para inovações desenvolvidas internamente.

O *Buy American Act* foi determinante para a expansão do mercado de *cloud computing* doméstico, fortalecendo a posição dominante dos *hyperscalers* estadunidenses (Google Cloud, AWS e Microsoft Azure), ao compelir a Administração Pública federal a contratar serviços de provedores estadunidenses, mediante contratos de longo prazo e investimentos públicos superiores a US\$ 1 trilhão até 2030. Adicionalmente, o Departamento de Defesa incrementou significativamente o financiamento para sistemas de comando e controle baseados em serviços de nuvem domésticos, com projeção de US\$ 21 bilhões somente em 2026⁶⁶, fortalecendo substancialmente a cadeia nacional de *cloud computing*. De forma ainda

⁶⁵ PIIE Briefing 21-5: Scoring 50 years of US industrial policy, 1970-2020.

⁶⁶ COVERI, Andrea; COZZA, Claudio; GUARASCIO, Dario, Big Tech and the US Digital-Military-Industrial Complex. Disponível em: <<https://www.intereconomics.eu/contents/year/2025/number/2/article/big-tech-and-the-us-digital-military-industrial-complex.html>>. Acesso em: 5 jan. 2026.



mais paradigmática, a SpaceX e sua subsidiária Starlink ascenderam à condição de gigantes do setor aeroespacial e da conectividade satelital essencialmente em razão de contratos públicos bilionários firmados com a NASA, os quais proporcionaram não apenas financiamento, mas também escala operacional e legitimidade técnica.⁶⁷ Tais exemplos evidenciam como compras públicas estrategicamente orientadas transcendem a dimensão transacional, convertendo-se em mecanismo indutor de inovação e soberania tecnológica nacional.

Além disso, a promulgação recente do CHIPS and *Science Act*, ou anúncios como a iniciativa Stargate representa um marco de política industrial deliberada. Essas medidas preveem investimentos massivos em pesquisa, desenvolvimento e produção de semicondutores e infraestruturas computacionais no território nacional, com o objetivo de restabelecer a capacidade de fabricação nacional e reduzir dependências externas. No campo da IA, os Estados Unidos mantêm centros de supercomputação, aceleradores, clusters de alto desempenho e redes de pesquisa de vanguarda, muitos deles em instituições acadêmicas e laboratórios públicos, porém cada vez mais dependentes de infraestruturas de computação em nuvem gerenciada por um número muito limitado de *hyperscalers*.⁶⁸

Esse arranjo demonstra como a combinação entre demanda estatal (compras públicas), financiamento público e base científica permite o surgimento e consolidação de um ecossistema tecnológico robusto. O modelo estadunidense indica que a soberania digital pode ser perseguida a partir de investimento estratégico e coordenação estatal de longo prazo, especialmente quando o Estado assume o papel de cliente âncora. A lição para o Brasil é clara: para desenvolver uma base nacional de IA, é necessário que o governo federal e as administrações públicas (federal, estaduais, municipais) assumam uma demanda coerente por tecnologia nacional, estimulando o mercado interno e promovendo a inovação.

4.2 China: política industrial, governança integrada e *open source*

A configuração chinesa de soberania digital distingue-se pela articulação entre política industrial, regulação e governança liderada pelo Estado, e planificação infraestrutural com ênfase no desenvolvimento nacional de hardware e software. Ao longo das últimas décadas, a China estruturou um conjunto de medidas destinadas a consolidar sua autonomia tecnológica: apoio ao desenvolvimento e adoção de tecnologias em *open source*, investimentos massivos em semicondutores, computação em nuvem, telecomunicações, supercomputação e

⁶⁷ **Inside Elon Musk's Government Contracts**, Built In, disponível em: <<https://builtin.com/articles/elon-musk-government-contracts>>. acesso em: 5 jan. 2026.

⁶⁸ **Market features in AI infrastructure: Competition in artificial intelligence infrastructure**, OECD, disponível em: <https://www.oecd.org/en/publications/competition-in-artificial-intelligence-infrastructure_623d1874-en/full-report/component-6.html>. acesso em: 10 dez. 2025; KAK, Amba; MYERS WEST, Sarah; WHITTAKER, Meredith, **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: 10 dez. 2025.



inteligência artificial, sob a égide de planos estratégicos como o *Internet Plus* e *Made in China 2025*.⁶⁹

Enquanto a primeira política definiu as bases infraestruturais por meio de expansão da conectividade, da capacidade computacional e digitalização da administração pública, a segunda política permitiu o desenvolvimento de uma cadeia interna de design, produção e empacotamento de chips, assim como a formação de *clusters* tecnológicos nacionais, reduzindo a dependência externa. Tal visão foi particularmente relevante no campo da IA, onde a China promoveu a criação de nuvens soberanas, plataformas de dados públicos e privados para facilitar o uso de tais ativos, e o desenvolvimento de modelos e softwares nacionais, frequentemente apoiados por subsídios, incentivos fiscais e encomendas tecnológicas.⁷⁰

A adoção de soluções *open source* também representa um pilar estratégico e frequentemente subestimado do desenvolvimento tecnológico chinês. O governo considera o código aberto como uma ferramenta estratégica de política industrial. Ele busca tanto utilizar o *open source* para manter o acesso a tecnologias estrangeiras quanto fomentar um ecossistema nacional de código aberto, visando fortalecer a autossuficiência tecnológica.⁷¹ Implementando uma análise sistêmica, a China investiu estrategicamente na pesquisa e desenvolvimento de tecnologias em *open source* para trazer abertura nos gargalos das cadeias de suprimentos, especialmente onde o enforcement de patentes estrangeiras determinava uma dependência insustentável. Tal estratégia é particularmente visível no considerável apoio chinês ao RISC-V, um conjunto de instruções baseado no *framework* RISC (do inglês *Reduced Instruction Set Computing*) que permite a qualquer usuário projetar e vender chips e software RISC-V sem precisar pagar royalties.⁷²

Assim o *open source* foi estimulado, não necessariamente como termo ideológico, mas como meio de garantir autonomia, auditabilidade, portabilidade e adaptabilidade às exigências tecnológicas e normativas nacionais. Cabe frisar que a Administração Pública não é o único setor chave que estimula desenvolvimento e adoção de *open source*: gigantes da tecnologia (40,8%), desenvolvedores de software e TIC (32%) e atores das finanças (31,6%) representam os três principais clientes de provedores de serviços *open source*.⁷³ O controle estatal sobre infraestrutura, dados e produção tecnológica tem permitido à China construir uma posição de protagonismo, sustentada por recursos próprios, padronização nacional e forte coordenação institucional.

Essa experiência demonstra que soberania digital não depende unicamente de regulação ou de talento científico, mas de uma visão estratégica que articula produção industrial, infraestrutura crítica, governança institucional e políticas de longo prazo. Para o Brasil, a China oferece um

⁶⁹ 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. 23, n. 52, 2025.

⁷⁰ *Ibid.*

⁷¹ ARCESATI, Rebecca; MEINHARDT, Caroline, China’s Open-Source Tech Development.

⁷² BELLI *et al.*, **Soberania Digital e Inteligência Artificial no Brasil: rumo à autonomia tecnológica**.

⁷³ ARCESATI; MEINHARDT, China’s Open-Source Tech Development. RIO DE JANEIRO, RJ: Lumen Juris, 2026.



exemplo de como políticas industriais coordenadas, unidas ao estímulo à pesquisa, desenvolvimento e à adoção de *open source*, podem gerar autonomia real em toda a cadeia de suprimento digital.

4.3 União Europeia: limites estruturais e potencial do *Cloud Sovereignty Framework*

A União Europeia consolidou, ao longo das últimas décadas, uma abordagem regulatória robusta voltada à proteção de dados, transparência, interoperabilidade e moderação de conteúdo em plataformas digitais. Normas como o GDPR, o DSA, o DMA e o *AI Act*, configuram um arcabouço jurídico sólido, centrado na defesa de direitos fundamentais, na responsabilização e na segurança no uso de sistemas de IA. Porém, a concentração de esforços principalmente na elaboração normativa – ao invés do *enforcement*⁷⁴ de tais normas e na promoção de uma política industrial sólida e coesa – não permitiu aos europeus de evitar a dependência tecnológica.⁷⁵

No âmbito da infraestrutura, iniciativas como o *European Chips Act* sinalizam esforço de reindustrialização e tentativa de reduzir dependências externas em semicondutores, ainda que, até o momento, sem escala suficiente para alterar significativamente a posição europeia nas cadeias globais de hardware. Dentro desse contexto, o chamado *Cloud Sovereignty Framework* europeu emergiu como instrumento interessante, ao definir um *framework* de conformidade regulatória com base no qual devem ser avaliados provedores de serviços de computação em nuvem interessados em participar em licitações públicas no espaço da União.

Em essência, o *framework* define critérios de segurança, proteção e residência de dados, governança jurídica e requisitos de controle sobre operações críticas, assegurando que dados sensíveis e sistemas públicos estejam submetidos à jurisdição europeia. Cabe reiterar que se trata predominantemente de um mecanismo de *compliance*: estabelece exigências que provedores devem cumprir para operar em conformidade, mas não cria políticas industriais, ou mecanismos voltados a estimular a produção de alternativas nacionais ou regionais aos atores dominantes.

Essa característica revela uma limitação estrutural dupla. De um lado, o *framework* não altera a dependência europeia de provedores extrarregionais, especialmente dos Estados Unidos, que continuam detendo a maior parte da infraestrutura e dos serviços de nuvem utilizados por

⁷⁴ Apesar dos frequentes anúncios de multas elevadas ou abertura de novos casos pelas autoridades europeias de concorrência e proteção de dados, apenas uma porcentagem muito limitada dessas multas é efetivamente paga e desses casos são concluídos. Em ambas as situações muitos anos demoram desde que as condutas ilegais foram inicialmente identificadas e as multas pagas acabam configurando valores extremamente reduzidos comparadas aos ganhos realizados, o que levanta importantes questionamentos sobre a efetividade do modelo de regulação da UE. INTERNATIONAL, Cullen, [INFOGRAPHIC] **Top 10 European antitrust fines on Big Tech**, disponível em: <<https://www.cullen-international.com/news/2025/09/-INFOGRAPHIC--Top-10-European-antitrust-fines-on-Big-Tech.html>>. acesso em: 11 dez. 2025; **Big Tech fines tracker**, Proton, disponível em: <<https://proton.me/tech-fines-tracker/>>. acesso em: 11 dez. 2025.

⁷⁵ BRIA, Francesca; TIMMERS, Paul; GERNONE, Fausto. EuroStack – A European Alternative for Digital Sovereignty (February 13, 2025). Bertelsmann Stiftung. Gütersloh. Disponível SSRN: <https://ssrn.com/abstract=5298046> or <http://dx.doi.org/10.2139/ssrn.5298046>



governos e empresas europeias. De outro lado, ao criar um mecanismo de *compliance*, o *framework* representa uma admissão da falta de implementação da abundante legislação existente.

Cabe ressaltar que, ao regular, mas não fomentar, o modelo europeu corre o risco de institucionalizar uma autonomia de natureza predominantemente jurídica, sem alcançar autonomia técnica ou operacional. Há, portanto, risco concreto que a mera exigência de conformidade, sem medidas de estímulo e fortalecimento de capacidades internas, possa aumentar custos de operação para provedores que buscam atender às exigências europeias, sem produzir os benefícios estruturais pretendidos. Em outras palavras, a lição para o Brasil é que a regulação de risco é essencial, porém, em si, não permite alcançar a soberania tecnológica.

4.4 Suíça: um LLM aberto, transparente e soberano

Recentemente, a Suíça lançou Apertus, seu primeiro *large language model* (LLM) em *open source*, multilíngue e conforme a proteção de dados pessoais, desenvolvido por instituições públicas de pesquisa: a ETH Zürich, a EPFL e o *Swiss National Supercomputing Centre* (CSCS).⁷⁶ O lançamento, em setembro de 2025, representou um marco da soberania técnica helvética, pois o projeto disponibiliza não apenas os pesos do modelo, mas também o código-fonte, os dados de treinamento, os scripts de pré-processamento e os checkpoints intermediários, tudo sob licença permissiva e com documentação completa.

Apertus está disponível em duas versões, com 8 bilhões e 70 bilhões de parâmetros, permitindo usos desde educação e pesquisa até aplicações industriais. O modelo foi treinado com um grande conjunto de dados públicos, com especial atenção à diversidade linguística: contempla mais de mil idiomas, com cerca de 40% dos dados em línguas não anglófonas, o que favorece representatividade e inclusão sociocultural.⁷⁷

Cabe frisar, porém, que embora constitua marco significativo em transparência e cooperação multissetorial, o modelo apresenta limitações técnicas e desafios práticos consideráveis. O Apertus possui desempenho substancialmente inferior aos modelos de primeira linha, ficando atrás dos principais modelos, especialmente em tarefas de raciocínio complexo.⁷⁸ Além disso, a reprodutibilidade do modelo constitui um obstáculo significativo. O treinamento consumiu mais de 10 milhões de horas de GPU no supercomputador Alps, tornando sua replicação inacessível à maioria das instituições, restrita essencialmente a laboratórios governamentais ou grandes corporações tecnológicas.

⁷⁶Apertus: a fully open, transparent, multilingual language model | ETH Zurich, disponível em: <https://ethz.ch/en/news-and-events/eth-news/news/2025/09/press-release-apertus-a-fully-open-transparent-multilingual-language-model.html?utm_source=chatgpt.com>. acesso em: 10 dez. 2025.

⁷⁷ Apertus, Swiss AI, disponível em: <<https://www.swiss-ai.org/apertus>>. acesso em: 10 dez. 2025.

⁷⁸ IBRAHIM, Sara, Fact and fiction about the Swiss AI model Apertus.



Os desafios de implementação são consideráveis. O modelo de 70 bilhões de parâmetros demanda centenas de gigabytes e hardware robusto, distanciando-se da simplicidade de APIs comerciais. Os custos operacionais, embora o modelo seja gratuito, incluem despesas significativas com infraestrutura, podendo exigir investimentos de dezenas de milhares de dólares anuais. A operadora Swisscom, reconhecendo essas barreiras, passou a oferecer *Apertus-as-a-service* na plataforma de IA suíça soberana da operadora.⁷⁹ Em síntese, o Apertus estabelece precedente valioso em transparência, mas sua aplicação prática concentra-se no contexto governamental suíço, onde suas capacidades multilíngues regionais justificam as limitações técnicas e custos operacionais.

A iniciativa articula infraestrutura de supercomputação, colaboração acadêmica, financiamento público, preocupação com a acessibilidade e compromisso com a transparência. Portanto, o projeto suíço é particularmente relevante porque demonstra que é possível construir uma base de IA pública, confiável e auditável, por meio de uma abordagem multissetorial e capaz de servir como infraestrutura compartilhada para pesquisa, setor industrial e governo. Porém, é necessário considerar a acessibilidade desde a concepção para evitar que o enorme investimento em capacidade computacional e algorítmica não seja somente um exercício acadêmico.

Essa experiência serve como referência para o Brasil no sentido de que a soberania lógica (modelos e software) e a soberania infraestrutural podem ser buscadas mediante políticas coordenadas, financiamento público, licenciamento aberto e investimento em tecnologia nacional. Porém, como destacado em precedência a propósito do *zero rating*, a preocupação com a acessibilidade dos modelos deve desempenhar um papel crucial para garantir que os investimentos em tecnologia soberana possam ser transformados em produtos e serviços realmente adotados pela população e a indústria nacional.

4.5 Finlândia: adoção de software livre para soberania digital cidadã

A experiência da Finlândia recentemente foi destacada em um “Índice de Soberania Digital”⁸⁰ como um dos países mais avançados no uso de tecnologias auto-hospedadas e *open source* por parte de cidadãos, instituições e setor público. O índice, elaborado pela NextCloud, uma empresa europeia de TI, classifica os países com base na adoção de softwares em código aberto voltado a colaboração, comunicação, hospedagem de arquivos e produtividade que podem ser operados localmente, reduzindo dependência de provedores globais.

A Finlândia lidera o *ranking*, evidenciando forte adesão ao uso de soluções *open source* autônomas por parte de organizações públicas e privadas. Esse elevado grau de adoção demonstra que soberania digital não depende apenas de infraestrutura física ou regulação estatal, mas também de cultura tecnológica, capacidade de auto-hospedagem e autonomia -

⁷⁹ **Apertus: A fully open, transparent, multilingual language model**, disponível em: <<https://www.swisscom.ch/en/about/news/2025/09/02-apertus.html>>. acesso em: 4 jan. 2026.

⁸⁰ DATAETHICS, Finland Wins On Digital Sovereignty In New Index · Dataetisk Tænkehandle tank.



institucional e individual. A mobilização social e institucional em torno do software livre e da infraestrutura autogerida evidencia que a soberania informacional e lógica pode ser promovida de baixo para cima, como fenômeno cultural, liderado por atores sociais e mediante incentivo a comunidades, ecossistemas de desenvolvedores e políticas de inclusão digital.

Para o Brasil, a experiência finlandesa sugere que a consolidação de soberania digital demanda não apenas investimento público e políticas regulatórias, mas também promoção de uma cultura tecnológica alinhada à autonomia, educação digital cidadã, suporte a comunidades open source e estímulos para adoção de infraestruturas locais. Apesar das turbulências, a comunidade do software livre⁸¹, das tecnologias abertas e das redes comunitárias⁸² continua sendo surpreendentemente ativa no Brasil.

Essa abordagem descentralizada, quando combinada a políticas industriais e de governança, pode favorecer a construção de um ecossistema resiliente, democrático, equitativo e menos vulnerável a dependências externas.

4.6 O caso do Uruguai: construção da soberania digital a partir das bases

O Uruguai destaca-se na América Latina como exemplo de um país que, ao longo das últimas décadas, investiu de forma consistente na construção de uma pilha digital integrada, combinando conectividade, infraestrutura computacional robusta e desenvolvimento de software. O sucesso na implementação dessa visão estratégica lhe confere consideráveis vantagens competitivas e relativas de autonomia tecnológica. A estratégia uruguaia demonstra que, apesar das dimensões reduzidas, a soberania digital pode ser alcançada por meio de uma abordagem equilibrada entre políticas públicas de infraestrutura, regulação, incentivo à indústria de TIC e promoção de um ambiente de inovação domesticamente enraizado.

Desde o *Plan Ceibal*, criado em 2005 pelo Decreto nº 144/007, o Uruguai concebeu de maneira ampla a inclusão digital, envolvendo a promoção do acesso à rede, a educação para o uso da tecnologia e o estímulo à sua apropriação pela sociedade.⁸³ Essa iniciativa pioneira distribuiu laptops para alunos e professores em todo o país, promovendo equidade educacional e conectividade universal. Assim, o *Plan Ceibal* se consolidou como um modelo de política pública integrada, alinhando infraestrutura tecnológica, capacitação e inovação para reduzir desigualdades digitais.

Inicialmente, o Uruguai consolidou elevados níveis de conectividade doméstica. Mais de 90% da população possui acesso à banda larga, e mais de 80% dos domicílios estão conectados

⁸¹ Open Source Special Edition MIT Technology Review Brasil 2021.

⁸² BELLI, Luca, **Community Networks: Building Digital Sovereignty and Environmental Sustainability**, Rio de Janeiro, RJ: Publicações Direito Rio, 2023.

⁸³ GOMES, Ana Bárbara; DUARTE, Felipe; ROCILLO, Paloma. Inclusión digital como política pública Brasil y América del Sur en perspectiva. [s.l.]: IRIS, [s.d.]. Disponível em: <<https://irisbh.com.br/wp-content/uploads/2020/05/Inclusion-digital-como-politica-publica-IRIS.pdf>>.



por fibra óptica (FTTH).⁸⁴ Esse grau de cobertura estrutural cria as condições mínimas para a digitalização ampla da sociedade e para a provisão de serviços públicos, privados e de inovação tecnológica com baixa latência e alta confiabilidade. A conectividade significativa e universal – também associada à alfabetização digital elevada – constitui um pilar fundamental do ecossistema digital uruguaio, servindo como base para que demais camadas (infraestrutura computacional, dados, software) sejam operadas de modo coerente e inclusivo.

No que tange à infraestrutura computacional, o Uruguai avançou de modo decisivo. O país possui *data centers* de alto padrão, tanto públicos quanto privados, conectados a vários cabos submarinos internacionais, o que assegura robustez, redundância, eficiência no tráfego internacional de dados e segurança para operações de nuvem, serviços digitais e aplicações críticas.⁸⁵ Esses *data centers* oferecem capacidade computacional compatível com demandas contemporâneas de TIC, *cloud-computing*, serviços digitais e exportação de software, colocando o Uruguai numa posição privilegiada dentro da América Latina.

Na esfera da produção de software e economia digital, o Uruguai vem se consolidando como uma liderança regional. Exportações de software per capita o destacam entre os primeiros da região.⁸⁶ A existência de empresas de TI, fintechs, serviços de back office, centros de dados e outsourcing tecnológico indica que a combinação de conectividade, infraestrutura e regulação favorável criou espaço para o florescimento de um ecossistema de inovação local competitivo.⁸⁷ Como a China, nosso vizinho soube explorar de software de código aberto de maneira particularmente sábia: a Lei 19.179 de 2013 estabelece a prioridade e obrigatoriedade de uso de software livre na administração pública, salvo justificativa técnica fundamentada em contrário.⁸⁸

A abordagem uruguaia demonstra consciência estratégica sobre os riscos de dependência tecnológica. Em contexto global marcado por concentração de fornecedores de infraestrutura e serviços de nuvem, o desenvolvimento local de centros de dados, de infraestruturas capazes de oferecer conectividade significativa, e a priorização de software livre são escolhas que garantem resiliência, soberania técnica e mitigação de vulnerabilidades à interferência externa.

4.7 México: a promessa do supercomputador mais potente da América Latina

O governo do México anunciou a construção do supercomputador Coatlicue, projetado para ser o mais potente da América Latina, com capacidade estimada de 314 *petaflops* e

⁸⁴ URUGUAY, **Information and Communication Technology**, disponível em: <<https://www.trade.gov/country-commercial-guides/uruguay-information-and-communication-technology>>. acesso em: 10 dez. 2025.

⁸⁵ *Ibid.*

⁸⁶ **Uruguay Digital**, Uruguay Digital, disponível em: <<https://www.gub.uy/uruguay-digital/home>>. acesso em: 10 dez. 2025.

⁸⁷ *Ibid.*

⁸⁸ A lei foi posteriormente detalhada pelo Decreto nº 44/015, de 2015, que regulamentou sua aplicação prática nas instituições uruguaias.



investimento público de seis bilhões de pesos (cerca de 325 milhões de dólares).⁸⁹ Previsto para estar operacional até 2027, o sistema contará com milhares de GPUs e infraestrutura avançada de refrigeração, embora sua localização final ainda dependa de critérios como disponibilidade de energia, água e segurança geológica. O governo o apresenta como peça central de uma estratégia de soberania tecnológica e fortalecimento da capacidade científica e de inteligência artificial no país.

Entre os usos pretendidos estão a modelagem climática de alta resolução, a previsão de desastres naturais e o estudo de recursos hídricos e energéticos. Também foi anunciado que o Coatlicue apoiará pesquisas agrícolas ao integrar grandes volumes de dados ambientais, além de estudos biomédicos baseados em análises genômicas e clínicas.⁹⁰ No âmbito administrativo, o governo projeta utilizar a máquina para processar dados fiscais e aduaneiros, buscando aumentar a eficiência institucional e detectar irregularidades.

Cabe ressaltar que, mesmo que o supercomputador atenda exclusivamente às necessidades estatais de modelagem climática e processamento administrativo em infraestrutura local – conseguindo prescindir de serviços de computação em nuvem estrangeira – tal capacidade já representaria avanço substancial em termos de autonomia tecnológica nacional. A internalização dessas capacidades computacionais estratégicas constitui, per se, conquista significativa para a independência tecnológica do país, ao reduzir vulnerabilidades associadas à dependência de provedores externos e garantir controle sobre dados sensíveis e infraestrutura crítica.

Porém; cabe frisar que, embora o discurso oficial enfatize que o supercomputador ficará disponível para universidades, centros de pesquisa e empresas, ainda há pouca clareza sobre quais projetos públicos ou privados serão realmente integrados ao sistema. Assim, ainda não foram divulgados critérios de priorização, regras de governança, exigências técnicas para submissão de projetos nem mecanismos de transparência, o que gera incerteza sobre quem se beneficiará do novo recurso e como será organizado o acesso. Portanto, é natural se perguntar qual seja a visão estratégica para alavancar este enorme ativo.

Outro desafio relevante diz respeito à adoção das inovações geradas. A existência de uma infraestrutura de supercomputação, por si só, não garante impacto social ou econômico. Falta detalhamento sobre programas de capacitação, incentivos à transferência tecnológica, políticas de inovação e articulação com o setor produtivo, todos necessários para que descobertas científicas ou novos modelos de IA sejam realmente incorporados por instituições públicas, empresas ou pela sociedade.

⁸⁹ REPÚBLICA, Presidencia de la, **Presidenta Claudia Sheinbaum presenta “Coatlicue”, la supercomputadora del pueblo de México y la más poderosa de América Latina**, gob.mx, disponível em: <<http://www.gob.mx/presidencia/prensa/presidenta-claudia-sheinbaum-presenta-coatlicue-la-supercomputadora-del-pueblo-de-mexico-y-la-mas-poderosa-de-america-latina>>. acesso em: 10 dez. 2025.

⁹⁰ GONZÁLEZ, Fernanda, **Coatlicue, así es la supercomputadora que convertirá a México en líder de procesamiento de datos en LATAM**, WIRED, disponível em: <<https://es.wired.com/articulos/coatlicue-asi-es-la-supercomputadora-que-convertira-a-mexico-en-lider-de-procesamiento-de-datos-en-latam>>. acesso em: 10 dez. 2025.



Portanto, o Coatlicue representa um passo ambicioso na infraestrutura tecnológica mexicana, mas seu impacto dependerá em larga medida da implementação do projeto e da clareza sobre prioridades, da definição de uma governança sólida e da criação de condições para que a inovação produzida alcance a população e o desenvolvimento nacional. Tais elementos constituem requisitos essenciais ao êxito de qualquer iniciativa dessa natureza, impondo-se que as iniciativas nacionais os contemplem adequadamente, de modo a assegurar a otimização dos investimentos públicos em recursos computacionais estratégicos

4.8 Índia Stack: soberania por meio de infraestruturas públicas digitais e conectividade significativa

A experiência do Índia Stack representa um dos exemplos mais robustos de transformação digital orientada por visão de longo prazo e por uma estratégia estatal centrada na construção de infraestruturas públicas digitais abertas, interoperáveis e acessíveis.⁹¹ Lançado como um conjunto de plataformas públicas modulares – como o *Aadhaar* (identidade digital), UPI (pagamentos instantâneos), e o *DigiLocker* (documentos digitais) – o Índia Stack foi concebido não apenas como iniciativa tecnológica, mas como política de Estado voltada à inclusão econômica, ao fortalecimento da cidadania e à dinamização da economia digital doméstica. Seu sucesso decorre de uma arquitetura aberta, padronizada e baseada em APIs públicas, que permitiu simultaneamente a expansão de serviços governamentais e o florescimento de um ecossistema privado vibrante, desde fintechs até startups de serviços públicos digitais.

Cabe frisar, porém, que embora a Índia seja frequentemente apresentada como exemplo bem-sucedido de construção de infraestruturas públicas digitais, a literatura crítica⁹² evidencia que esse modelo produz riscos significativos decorrentes da centralização excessiva. O Índia Stack consolidou bases de identidade, pagamentos e dados governamentais em plataformas unificadas e de grande escala, criando um arranjo tecno-político que concentra poder institucional e informacional em poucas entidades estatais e paraestatais. Tal centralização amplia vulnerabilidades sistêmicas, pois uma falha, vazamento ou ataque pode comprometer milhões de pessoas simultaneamente.⁹³ Assim, embora a infraestrutura pública digital indiana tenha gerado ganhos de inclusão e eficiência, também criou assimetrias de poder e dependências estruturais que demandam forte governança, transparência e mecanismos descentralizados de controle social para evitar que centralização se converta em fragilidade institucional.

⁹¹ DRAPER, Hannah *et al*, *A Consumer-centric Approach to DPIs for sustainable financial inclusion*, Brasil: T20 Brasil 2024, 2024.

⁹² PARSHEERA, Smriti, *Stack is the New Black?: Evolution and Outcomes of the ‘India-Stackification’ Process*, *Computer Law & Security Review*, v. 52, p. 105947, 2024; MISRA, Manu; PANDAY, Jyoti; ZINGALES, Nicolo, *Applying the CII Framework to DPIs considerations, challenges and opportunities*, *T20 Policy Brief*, 2024.

⁹³ *Ibid*



Um elemento frequentemente negligenciado, mas crucial para compreender a profundidade da transformação digital indiana, é a política de conectividade significativa.⁹⁴ A Índia adotou medidas regulatórias que proibiram práticas de *zero rating*, reconhecendo que tais modelos distorcem o acesso à internet, favorecem plataformas dominantes e inibem a inovação local.⁹⁵ A partir dessa decisão, o governo indiano incentivou a competição no setor de telecomunicações, o que resultou em queda expressiva dos preços de dados móveis e expansão maciça do acesso à internet.

Essa combinação de regulação pró-concorrencial com políticas de infraestrutura pública permitiu que milhões de pessoas, inclusive em regiões remotas, pudessem acessar serviços digitais governamentais e privados com custos reduzidos e qualidade crescente. A conectividade significativa tornou-se, assim, o alicerce da inclusão digital e da participação social na economia de dados.

A sinergia entre infraestruturas públicas digitais e políticas de conectividade constituiu o núcleo da estratégia indiana para criar um ambiente favorável à inovação doméstica, ao empreendedorismo nacional e à construção de capacidades tecnológicas autônomas. Ecossistemas de startups e empresas tecnológicas puderam desenvolver soluções baseadas diretamente nas APIs públicas do Índia Stack, ampliando a concorrência e reduzindo barreiras de entrada. O resultado é um ciclo virtuoso: infraestruturas abertas reduzem custos de inovação, conectividade significativa amplia a base de usuários e o ecossistema empreendedor gera novas soluções que alimentam a transformação digital.

4.9 Lições e elementos adaptáveis ao contexto brasileiro

A análise comparativa das experiências internacionais revela que a soberania digital não é um conceito monolítico, mas uma construção multifacetada que depende da articulação entre regulação, infraestrutura tecnológica, política industrial, conectividade significativa, cultura de inovação e governança democrática.⁹⁶ Cada país analisado desenvolveu mecanismos próprios para enfrentar vulnerabilidades e consolidar autonomia, oferecendo lições que podem ser adaptadas ao caso brasileiro, respeitando-se as especificidades institucionais, federativas e socioeconômicas do país.

Os Estados Unidos demonstram a força das compras públicas como instrumento de política industrial e como motor de criação de mercados tecnológicos. A utilização do Estado como cliente âncora permitiu a consolidação de empresas nacionais de infraestrutura crítica e de

⁹⁴ BELLI, Luca. **Building Good Digital Sovereignty through Digital Public Infrastructures and Digital Commons in India and Brazil**, Rio de Janeiro, 2024.

⁹⁵ 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.

⁹⁶ JIANG, Min; BELLI, Luca (Orgs.), **Digital Sovereignty in the BRICS Countries.: How the Global South and Emerging Power Alliances Are Reshaping Digital Governance**. Cambridge University Press; 2025. 2024.



computação em nuvem, evidenciando o potencial da demanda estatal para reduzir dependências externas.

A China oferece uma lição complementar. A coordenação estratégica entre planejamento estatal, regulação, investimentos contínuos e estímulo ao *open source* possibilitou a consolidação de atores nacionais e a redução de assimetrias em hardware e software.

A experiência europeia demonstra a necessidade de produzir proteção de direitos fundamentais, padronização técnica e governança democrática, mas a inutilidade da mera adoção de instrumentos normativos na ausência de política industrial que estimule o desenvolvimento e a adoção de tecnologia doméstica. A experiência suíça, mostra que é possível construir inteligência artificial pública, auditável, transparente e multilíngue, como o projeto Apertus, conferindo autonomia científica e demonstrando que tais experiências têm o potencial de reduzir dependências estruturais em modelos fechados, ao passo que sejam tornados acessíveis de forma simples e econômica. A Finlândia, por sua vez, mostra que soberania digital também emerge de práticas descentralizadas, adoção de software livre, auto-hospedagem institucional e investimentos contínuos em competências locais.

Experiências mais próximas ao contexto brasileiro oferecem contribuições adicionais. A Índia, parceiro do grupo BRICS, demonstra o poder de uma visão de longo prazo baseada em infraestruturas públicas digitais abertas e conectividade significativa. Apesar das críticas, a Índia Stack se transformou em ecossistema de inclusão econômica e inovação graças ao desenho modular de APIs públicas e a decisões regulatórias, como a proibição do *zero rating*, que ampliaram conectividade, derrubaram custos de acesso e criaram condições para o florescimento de um mercado doméstico de soluções digitais.

No âmbito latino-americano, a experiência uruguaia demonstra que investir de forma contínua em conectividade universal, *data centers* nacionais e fortalecimento da indústria local de software permite construir autonomia tecnológica mesmo em países de menor escala. Para o Brasil, a lição central é que políticas consistentes e coordenadas podem gerar soberania digital sustentável e competitividade regional. O México, por outro lado, ilustra a importância de se organizar uma articulação efetiva entre investimentos em digitalização e visão estratégica sólida por meio de uma cooperação multissetorial, para incrementar as chances de maximizar o retorno social do investimento público.

Em conjunto, essas experiências comparadas sugerem que o Brasil deve adotar uma abordagem integrada que combine elementos regulatórios, industriais e sociotécnicos. A adaptação dessas lições implica reconhecer que nenhuma dimensão isolada – seja infraestrutura, regulação ou política industrial – é suficiente para assegurar autonomia. O caminho brasileiro passa por articular governança multissetorial, estabelecer unidades ou entidades capazes de coordenar missões tecnológicas de alto impacto, promover industrialização tecnológica baseada em capital nacional, desenvolver infraestruturas públicas abertas, fortalecer conectividade significativa articulada com tecnologias nacionais, incentivar *open source* e consolidar mecanismos democráticos de participação e supervisão. Essas



lições podem orientar um projeto nacional de soberania digital coerente, sustentável e tecnicamente robusto.



5 Construção de um Ecossistema Digital Nacional Tecnicamente Autônomo e Aberto

A construção de um ecossistema nacional digitalmente soberano exige mais do que investimentos materiais ou ajustes regulatórios pontuais. Trata-se de um projeto que envolve coordenação interinstitucional, fortalecimento científico, continuidade de políticas públicas, inserção internacional estratégica e capacidade de organizar recursos técnicos, humanos e financeiros em uma arquitetura coerente e duradoura. A inteligência artificial é um campo técnico, econômico e geopolítico de crescente complexidade; por essa razão, a consolidação de um ecossistema nacional não pode limitar-se à aquisição de equipamentos ou à promulgação de normas. É preciso articular infraestrutura, dados, modelos, formação, governança e cultura tecnológica em uma mesma visão estratégica integrada, orientada à soberania digital.

O Relatório do Seminário Nacional sobre a Pilha de IA Soberana identificou uma série de lacunas estruturais nas camadas física, lógica e informacional, indicando que o Brasil enfrenta desafios simultâneos relacionados à infraestrutura, à produção de software, à disponibilidade de modelos pré-treinados, à governança de dados e à capacidade de operação de sistemas de alta complexidade. Nesse contexto, o ecossistema digital nacional, deve responder a esses desafios por meio de uma governança multissetorial voltada à autonomia tecnológica e capaz de possibilitar colaboração científica, reprodutibilidade, eficiência econômica e segurança.

Este capítulo propõe diretrizes para o desenho desse ecossistema, estruturadas em sete eixos fundamentais: *i)* a pilha como metáfora conceitual; *ii)* as características da pilha brasileira de IA; *iii)* as plataformas de dados e intercâmbio informacional; *iv)* os centros de excelência e redes de pesquisa; *vi)* a padronização técnica; *vii)* a experimentação por meio de um projeto nacional em *open source*; e, *vii)* o papel da CT&I na construção de um ecossistema nacional digitalmente soberano.

5.1 A pilha como metáfora analítica para a arquitetura tecnológica e de governança dos sistemas digitais

O conceito de “pilha” tornou-se, nos últimos anos, uma ferramenta teórica relevante para a compreensão da arquitetura dos sistemas digitais e das relações de poder que deles emergem. No campo da computação, o termo refere-se tradicionalmente às pilhas de software e hardware, representadas como conjuntos de camadas lógicas de abstração que vão do microcódigo e dos semicondutores às interfaces e aplicações.⁹⁷

⁹⁷ Relatório Seminário Pilha IA Soberana.

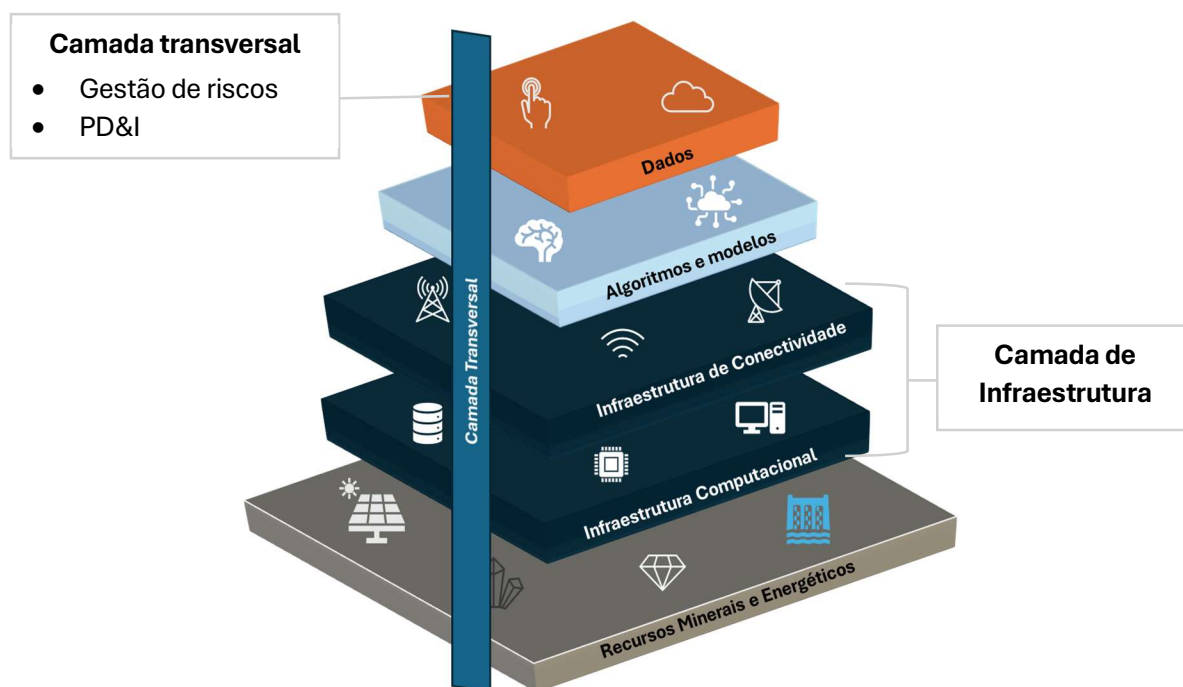


Figura 1. Proposta de Pilha de IA Soberana Brasileira

Cada camada depende da anterior para funcionar, mas opera com relativa autonomia. Entretanto, autores como Benjamin Bratton ampliaram esse conceito para além da engenharia, descrevendo *The Stack* como uma mega infraestrutura planetária composta por seis camadas – Terra, Nuvem, Cidade, Endereçamento, Interface e Usuário – que articulam tecnologia, territorialidade, soberania e governança.⁹⁸ A pilha, nesse sentido alargado, deixa de ser apenas uma metáfora técnica e passa a ser uma teoria político-tecnológica que permite compreender como a infraestrutura digital reorganiza relações de poder e modelos de autoridade no século XXI.

A abordagem da pilha, quando aplicada a soberania em IA⁹⁹, revela a necessidade de se enxergar todos os componentes da pilha como elementos ecossistêmicos, que devem ser enquadrados não somente por regulação, governança e políticas industriais setoriais, mas também por meio de uma abordagem sistêmica capaz de interconectar os subsistemas setoriais. É importante destacar que para alcançar tal ideal é preciso não somente construir capacidades institucionais, regulatórias e de fomento em múltiplos níveis, mas também conectar os resultados de tais esforços. No Brasil, particularmente, o exercício da autoridade

⁹⁸ BRATTON, Benjamin H., *The stack: on software and sovereignty*, Cambridge, Mass. London: MIT press, 2015.

⁹⁹ 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; BELLI, Luca; GASPARG, Walter B; *The Quest for AI Sovereignty, Transparency and Accountability*, Rio de Janeiro, 2024; 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.



estatal não ocorre de forma homogênea em todos os elementos do ecossistema digital, mas de modo fragmentado.

Uma abordagem ecossistêmica, baseada no reconhecimento dos elementos que compõem as pilhas digitais e da interconexão fundamental entre esses elementos, é essencial para que os esforços estatais sejam eficazes e efetivos. Como será exemplificado adiante, mesmo quando o Estado tentar regular camadas específicas, por exemplo adotando normas como a LGPD e criando autoridades como a ANPD, vulnerabilidades e dependências em outras camadas – como a falta de conectividade significativa, a dependência de nuvens, plataformas e sistemas operativos estrangeiros – podem ser exploradas de modo a neutralizar ou prejudicar os esforços regulatórios.

A literatura em engenharia de software e em arquiteturas computacionais reforça essa perspectiva ao demonstrar que vulnerabilidades em camadas profundas, como *firmware*, *drivers*, hardware, podem comprometer toda a cadeia lógica e algorítmica situada acima.¹⁰⁰ Assim, a autonomia tecnológica nacional deve ser construída considerando organicamente as dimensões informacional, infraestrutural, lógica, aplicacional e de capacitação.

O valor heurístico da metáfora da pilha reside em sua capacidade de revelar interdependências estruturais que, de outra forma, permaneceriam invisíveis. A metáfora da pilha mostra que políticas públicas isoladas – regulatórias, industriais ou de segurança – não são suficientes para garantir soberania digital se não forem articuladas de forma sistêmica entre camadas. O uso de tal abordagem permite, ainda, que o Estado identifique gargalos específicos – como dependências externas em GPUs, ausência de padrões de interoperabilidade, fragilidade em governança de dados, insuficiência de plataformas abertas ou carência de competências técnicas – e atue de forma coordenada para resolver tais gargalos de forma orgânica, considerando o impacto e operando em todos os elementos da pilha.

A metáfora da pilha também auxilia na compreensão da distribuição assimétrica de poder entre atores públicos e privados. Grandes plataformas controlam ecossistemas que perpassam toda a pilha desde camadas de interface e sistemas de endereçamento até infraestrutura de acesso e computação em nuvem. É precisamente tal capacidade de entender e atuar em todas as camadas da pilha de maneira coordenada que permite às grandes empresas de tecnologia direcionarem o comportamento dos usuários, concentrar fluxos informacionais, capturar valor econômico e influenciar a evolução de setores inteiros da economia. Em contraste, reguladores setoriais frequentemente começam a identificar práticas potencialmente abusivas apenas de forma tardia e permanecem limitados por recortes institucionais restritos de competência.¹⁰¹

Entretanto, o modelo da pilha possui limites importantes. Como toda metáfora estrutural, ela pode sugerir uma rigidez que não corresponde à complexidade das dinâmicas sociotécnicas contemporâneas. As camadas, embora analiticamente separáveis, são mais permeáveis e

¹⁰⁰ MERA, Alejandro *et al*, DICE: Automatic Emulation of DMA Input Channels for Dynamic Firmware Analysis, 2021; KOCHER, Paul *et al*, Spectre Attacks: Exploiting Speculative Execution, 2018.

¹⁰¹ ZINGALES, Nicolo; AZEVEDO, Paula Farani de, **A aplicação do direito antitruste em ecossistemas digitais: desafios e propostas**, [s.l.]: FGV Direito Rio, 2022.



fluidas do que o modelo sugere e, além disso, os componentes de cada camada podem ser estruturados em pilhas setoriais. A metáfora também corre o risco de obscurecer disputas políticas reais, reduzindo a governança digital a uma simples gestão técnica de níveis interdependentes, quando na verdade envolve conflitos geopolíticos, interesses econômicos, relações de trabalho e desigualdades estruturais.

Além disso, a pilha pode induzir a uma visão excessivamente verticalizada, dificultando a percepção de redes horizontais de cooperação, como consórcios de ciência aberta, infraestruturas federadas, plataformas distribuídas e arranjos comunitários de tecnologia. Outro limite está na tendência de aplicar o modelo de maneira prescritiva, sem considerar particularidades regionais, federativas ou setoriais, o que pode levar a homogeneização das soluções de governança sem considerar especificidade essenciais, resultando na imposição de projetos tecnocráticos que ignoram contextos sociais e institucionais específicos.

Ainda assim, apesar desses limites, o conceito de pilha permanece uma ferramenta analítica poderosa para orientar políticas públicas de soberania digital, especialmente quando adaptado às realidades nacionais e articulado a uma compreensão jurídica e institucional das relações de poder no ecossistema digital. Ao revelar dependências estruturais, identificar gargalos críticos e demonstrar como a autonomia em níveis superiores depende de capacidades acumuladas em níveis inferiores, a metáfora da pilha pode contribuir positivamente para o desenvolvimento de estratégias mais coerentes, integradas e eficazes voltadas a promover a autonomia tecnológica no ecossistema digital pátrio.

5.2 A Pilha Digital Brasileira como arquitetura sociotécnica de autonomia tecnológica

A construção de um ecossistema digital nacional tecnologicamente autônomo requer que a metáfora da pilha seja compreendida não como um arranjo meramente técnico, mas como uma arquitetura sociotécnica e de governança capaz de estruturar a autonomia informacional, infraestrutural, lógica e cognitiva do país.

Inspirada na literatura internacional sobre pilhas computacionais e no modelo proposto por Belli¹⁰², a pilha brasileira deve ser compreendida como uma estrutura em camadas interdependentes que articula infraestruturas físicas, fluxos de dados, lógicas algorítmicas, ferramentas de desenvolvimento e competências humanas, junto com arcabouços regulatórios, governança e políticas de fomento. Nesse sentido, a pilha não é um fim em si mesmo, mas um instrumento de visão estratégica para viabilizar autonomia tecnológica, reduzir vulnerabilidades estruturais e orientar políticas regulatórias, industriais e científicas.

A construção de um ecossistema nacional de inteligência artificial requer uma abordagem em camadas que reflita a natureza interdependente das infraestruturas digitais. Nesta perspectiva, a pilha digital brasileira deve ser concebida como uma arquitetura sociotécnica integrada,

¹⁰² BELLI, Luca; Soberania em Inteligência Artificial: O que é e quais facilitadores essenciais podem tornar o Brasil um país soberano em IA?, Rio de Janeiro, 2024; BELLI, Luca; GASPAR, Walter Britto (Orgs.), **The Quest for AI Sovereignty, Transparency and Accountability**, Rio de Janeiro: FGV Direito Rio, 2023.



composta por pelo menos seis camadas interconectadas: dados; algoritmos e modelos; infraestrutura computacional; infraestrutura de conectividade; recursos minerais e energéticos; e, transversalmente, capacitação e governança.¹⁰³ Essa estrutura evidencia que a soberania digital não reside em um único nível da cadeia tecnológica, mas emerge do alinhamento entre capacidades técnicas, institucionais, materiais e humanas, considerando organicamente todas as camadas.

A camada de dados corresponde ao fundamento informacional da soberania digital. Embora o Brasil detenha políticas avançadas e vasto patrimônio de dados públicos e setoriais, esse setor permanece fragmentado, insuficientemente estruturado e amplamente subaproveitado para alimentar o desenvolvimento de tecnologia nacional, especialmente IA. Como será destacado na próxima seção, a implementação de “bolsas de dados”¹⁰⁴ pode permitir superar esses gargalos técnicos e normativos por meio de plataformas interoperáveis, federações de dados e mecanismos de compartilhamento seguro e indispensável para transformar dados em ativos estratégicos.

A camada de algoritmos e modelos constitui o núcleo lógico da pilha. Atualmente, o país depende quase integralmente de modelos, *frameworks* e bibliotecas estrangeiras, o que cria assimetrias tecnológicas, limita auditoria independente e expõe sistemas públicos e privados a vulnerabilidades.¹⁰⁵ Políticas nacionais devem incentivar o desenvolvimento e a adoção de modelos abertos, multilíngues e culturalmente contextualizados, além de ferramentas e algoritmos otimizados para aplicações nacionais. O desenvolvimento dessa camada é essencial para reduzir dependências, garantir transparência e permitir a adaptação tecnológica contínua.

A camada de infraestrutura pode ser desdobrada em duas subcamadas essenciais: a subcamada de infraestrutura computacional e a subcamada de infraestrutura de conectividade. A primeira subcamada corresponde ao nível material que viabiliza o treinamento, a operação e o escalonamento de modelos avançados. Inclui supercomputadores, *clusters* GPU/TPU, *data centers* e nuvens sob jurisdição nacional. A insuficiência de capacidade computacional nacional impede que pesquisadores, empresas e órgãos governamentais disputem posições estratégicas no cenário global de IA. Essa camada deve ser fortalecida com investimentos contínuos, padronização de ambientes que facilite o uso coletivo.

A subcamada de infraestrutura de conectividade garante que dados, modelos e aplicações possam ser acessados e compartilhados de maneira não discriminatória, segura e eficiente. A garantia da neutralidade da rede e a proibição do *zero rating*, a expansão de redes de alta

¹⁰³ BELLI, Soberania em Inteligência Artificial: O que é e quais facilitadores essenciais podem tornar o Brasil um país soberano em IA?; BELLI, Luca; GASPAR, Walter Britto (Orgs.), **The Quest for AI Sovereignty, Transparency and Accountability**, Rio de Janeiro: FGV Direito Rio, 2023; BELLI *et al*, **Soberania Digital e Inteligência Artificial no Brasil: rumo à autonomia tecnológica**.

¹⁰⁴ LU, Julia, Data exchanges in China, explained · TechNode. Disponível em: <<https://technode.com/2021/08/17/chinas-data-exchanges-explained/>>. Acesso em: 5 dez. 2025.

¹⁰⁵ Relatório Seminário Pilha IA Soberana.



velocidade, pontos de troca de tráfego (IXPs), redes 5G/6G, bem como a segurança do cabeamento submarino, por meio de um marco regulatório homogêneo e coerente, constituem elementos críticos dessa camada. A conectividade significativa, ou seja, acessível, não discriminatória e de alta qualidade, é condição essencial para que as demais camadas funcionem plenamente e para que serviços digitais cheguem à sociedade de forma equânime.

A camada de recursos minerais e energéticos revela dependências frequentemente invisíveis da pilha digital, especialmente no que se refere a materiais necessários para construção de semicondutores, como lítio, grafite e terras raras, ou para operação de *data centers*, como energia elétrica confiável e sustentável. A autonomia tecnológica requer segurança material e energética, dado que *data centers*, *clusters* de IA e cadeias de semicondutores dependem de insumos críticos. Como destacado na Seção 3.5, o Brasil dispõe de vantagens altamente estratégicas nessa camada, mas carece de mecanismos de integração entre política mineral, política energética, política industrial e política digital.

Por fim, a dimensão transversal de capacitação e governança permeia todas as camadas da pilha. A capacitação é indispensável para entender os riscos e aproveitar as oportunidades correlatas a todas as dimensões de todos os elementos da pilha. Paralelamente o tratamento de riscos – seja aqueles inerentes ao desenvolvimento e à operação de tecnologias digitais, sejam os decorrentes de ameaças externas – é essencial para definir controles e protocolos e salvaguardas, bem como para estruturar políticas de desenvolvimento tecnológico e produtivo necessárias para superação de dependências críticas na gestão de tais riscos. Isto inclui formação de profissionais especializados, requalificação de cientistas de outras áreas, mecanismos de auditoria, avaliação de impacto, gestão de riscos algorítmicos e segurança cibernética. Sem essa dimensão transversal, a pilha torna-se insustentável, vulnerável e incapaz de se adaptar valores normativos e constitucionais.¹⁰⁶

Essa arquitetura integrada demonstra que a consideração cuidadosa das demais dimensões da pilha digital brasileira é condição estruturante para o exercício pleno da soberania digital. No Brasil, atualmente, há ao menos três frentes que poderiam ser melhor desenvolvidas e articuladas para promover essa construção da pilha brasileira. O SINAPAD, que além de prover serviços de supercomputação, possui como objetivos a formação de pessoas e o desenvolvimento de produtos e serviços de processamento de alto desempenho, e foi recentemente atualizado pela Portaria MCTI nº 9.445/2025, a iniciativa “Nuvem de Governo”, que é regulada pela Portaria SGD/MGI Nº 5.950, de 26 de outubro de 2023 e o REDATA, cuja Medida Provisória 1318/2025 se encontra em discussão no Congresso.

¹⁰⁶ BELLI, Luca; MEDEIROS, Breno Pauli; COUTO, Natália. Governança da cibersegurança no Brasil: entender o passado, esclarecer o presente e construir o futuro. Disponível em: <<https://cyberbrics.info/wp-content/uploads/2024/06/PP-CTS-FGV-Ciberseguranca.pdf>>. Acesso em: 3 dez. 2024.



5.3 Bolsas de dados e intercâmbio informacional

A soberania digital requer uma arquitetura nacional de dados que viabilize o compartilhamento seguro, auditável e juridicamente protegido de bases públicas e privadas. Na ausência de tal arquitetura, a interoperabilidade e a portabilidade informacional permanecem como ideais meramente teóricos, e a colaboração científico-industrial ao desenvolvimento tecnológico mantém-se limitada.

Para superar essa lacuna, propõe-se a criação de uma Rede Nacional de Dados sob governança federada, potencialmente coordenada pelo Comitê Interministerial para Transformação Digital e operada conjuntamente com os PRODEs¹⁰⁷ estaduais e centros de pesquisa. Tal Rede deveria ser desenvolvida em sinergia com um sistema nacional para desenvolvimento da Inteligência Artificial.

Essa Rede Nacional de Dados deve permitir a integração de bases federais, estaduais e municipais, com padrões de metadados, APIs, esquemas de autenticação e mecanismos de governança. A experiência das plataformas chinesas de intercâmbio de dados oferece um modelo relevante.¹⁰⁸ Nessas plataformas, empresas públicas estaduais operam serviços de curadoria, certificação e comercialização de dados, sob regras que garantem segurança, auditabilidade, rastreabilidade e cumprimento de normas de cibersegurança. Tais estruturas demonstram que o Estado pode ser operador ativo de infraestruturas informacionais, além de definir regras de proteção de dados e padrões de interoperabilidade, sem comprometer inovação ou participação privada.

No contexto brasileiro, os PRODEs podem ser transformados em operadores regionais de intercâmbio de dados, responsáveis pela curadoria de bases estaduais, certificação de qualidade, gestão de contratos de compartilhamento e disponibilização de ambientes seguros de análise.¹⁰⁹ Essa arquitetura permite descentralização e proximidade institucional com governos locais, ao mesmo tempo em que responde a exigências nacionais de uniformização técnica.

Além disso, plataformas federadas de dados em setores específicos como energia, petróleo e gás, clima, agronegócio, medicina ou segurança pública podem ampliar a capacidade de treinamento de modelos nacionais, desde que acompanhadas de controles rigorosos de acesso e anonimização. Bases multimodais e multilíngues, incluindo dados regionais,

¹⁰⁷ Os PRODEs são entidades públicas ou paraestatais criadas pelos governos estaduais brasileiros para gerir, desenvolver e operar soluções de tecnologia da informação e comunicação, voltadas ao atendimento das necessidades da administração pública local. Tradicionalmente, os PRODEs prestam serviços como desenvolvimento de sistemas, hospedagem de dados governamentais, gestão de redes, suporte técnico e implementação de políticas digitais estaduais. Sua função central é prover infraestrutura tecnológica confiável, segura e alinhada às diretrizes públicas.

¹⁰⁸ LU, Julia. Data exchanges in China, explained · TechNode; ARCESATI, Alex He, 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: 13 nov. 2025.

¹⁰⁹ Essa proposta é apresentada em BELLI *et al*, **Soberania Digital e Inteligência Artificial no Brasil: rumo à autonomia tecnológica**.



indígenas e de grupos minoritários, são essenciais para a produção de modelos representativos e inclusivos.

5.4 Centros de excelência, redes de pesquisa e alianças estratégicas

Como apontado ao longo do Seminário Nacional “Pilha de IA: Desafios para Autonomia Tecnológica e Soberania Digital” o Brasil possui ilhas de excelência acadêmica e industrial, mas carece de mecanismos estruturados de coordenação.¹¹⁰ Um ecossistema nacional exige a articulação de centros de supercomputação, universidades, redes de ICTs e empresas por meio de uma governança distribuída, orientada a metas comuns.

Os centros de supercomputação do Sistema Nacional de Processamento de Alto Desempenho (SINAPAD) podem ser alavancados para operar como infraestrutura crítica de pesquisa, com serviços padronizados, ambientes pré-configurados e suporte técnico avançado. Esses centros devem atuar como prestadores de serviços públicos, oferecendo computação sob demanda, consultoria técnica e plataformas educacionais. A governança deve garantir que os recursos sejam alocados de forma transparente e eficiente, com priorização para projetos estratégicos e setores sensíveis.

As universidades e centros de pesquisa devem ser integrados por meio de consórcios formais, responsáveis por pesquisa básica, formação de recursos humanos e desenvolvimento de protótipos. Redes temáticas nacionais dedicadas a assuntos estratégicos para os quais será priorizada a interoperabilidade de dados – como os setores de mineração, energia, agronegócio, segurança pública, defesa ou medicina, destacados na seção precedente – podem garantir coordenação contínua e compartilhamento de infraestrutura para alavancar a riqueza informacional brasileira.

A governança distribuída deve incluir ainda a participação da indústria, por meio de câmaras setoriais e comitês técnico-científicos. A participação empresarial garante aderência às demandas reais do mercado e possibilita que soluções de IA se transformem em produtos, serviços e tecnologias exportáveis. A experiência suíça com o LLM Apertus, ou a da China com o LLM DeepSeek V3 demonstram que modelos abertos podem ser integrados a ecossistemas industriais desde que haja governança capaz de harmonizar interesses e garantir abertura.

No contexto brasileiro, o desenvolvimento autônomo de modelos fundacionais de fronteira (*frontier models*) em IA apresenta elevada complexidade técnica, financeira e institucional. Nesse cenário, mostra-se mais racional e eficiente a constituição de alianças setoriais estratégicas, ancoradas em ativos tecnológicos nacionais já consolidados. Essa abordagem maximiza impacto econômico e social, observa os princípios da eficiência e da economicidade e fortalece capacidades tecnológicas nacionais de forma incremental e sustentável.

Por fim, a experiência internacional demonstra que a soberania tecnológica em inteligência artificial não se alcança mediante iniciativas isoladas, mas através de arranjos institucionais

¹¹⁰ Relatório Seminário Pilha IA Soberana.



coordenados que integram infraestrutura, dados, modelos e talentos. Países líderes como Estados Unidos, China, Japão ou a União Europeia estruturaram suas capacidades em IA mediante alianças estratégicas que articulam laboratórios nacionais, supercomputação, instalações científicas e parcerias público-privadas sob governança unificada no âmbito dos modelos de *AI for Science*.¹¹¹

Como será destacado nas Seções 5.7 e 7.4, o Brasil possui oportunidade singular de estabelecer alianças estratégicas nacionais em IA, instrumentalizada pelo Marco Legal de CT&I, para coordenar o desenvolvimento de um ecossistema tecnologicamente autônomo, ou até de pilhas tecnológicas setoriais digitalmente soberanas. Tal arranjo possibilitaria superar a fragmentação atual – caracterizada por investimentos isolados sem operação sustentável, governança ad hoc de dados e elevado *lock-in* tecnológico – mediante articulação do SINAPAD, do futuro Sistema Nacional de Ciência, Tecnologia e Inovação em IA (SINIA)¹¹², de padronização, e portfólio de missões estratégicas em saúde, clima, agricultura, petróleo e gás, e energia implementadas por meio de alianças setoriais.

Por fim, cabe ressaltar que o Brasil dispõe de ecossistema robusto de empresas estatais e de capital misto que operam na fronteira tecnológica em setores estratégicos como energia, defesa, semicondutores e agronegócio.¹¹³ Essas organizações concentram infraestrutura crítica, quadros técnicos altamente qualificados e capacidade instalada de pesquisa aplicada, constituindo base material relevante para políticas de soberania digital e tecnológica. A criação de alianças estratégicas nos setores nos quais operam tais empresas, junto com universidades, e *startups* apresenta elevada viabilidade institucional e potencial impacto sistêmico, sobretudo na incorporação de IA, robótica avançada e manufatura de alta precisão. A coordenação estatal pode catalisar sinergias intersetoriais com efeitos econômicos, industriais e defensivos significativos.

5.5 Padrões, interoperabilidade e reprodutibilidade científica

A falta de interoperabilidade e padronização é um dos maiores obstáculos para a construção de um ecossistema brasileiro votado à cooperação científica e ao empreendedorismo digital. A heterogeneidade de ambientes de armazenamento e execução, conjuntos de bibliotecas, versões de *frameworks* e métodos de documentação cria barreiras significativas para a colaboração científica, o compartilhamento de modelos e a reprodutibilidade de experimentos.¹¹⁴

¹¹¹ **Artificial Intelligence for Science**, disponível em: <<https://www.worldscientific.com/worldscibooks/10.1142/13123>>. acesso em: 5 jan. 2026.

¹¹² Relatório Seminário Pilha IA Soberana.

¹¹³ Exemplificativamente, é suficiente frisar que a Petrobras lidera aplicações de robótica submarina e IA logística; a Embraer desenvolve robótica agrícola e modelos preditivos; a Embraer é líder em aviação autônoma e IA industrial; o Ceitec desempenha papel relevante em semicondutores estratégicos; e a Nuclep emprega robótica pesada em defesa naval. Tais ativos evidenciam capacidade tecnológica considerável, já instalada e passível de coordenação estratégica.

¹¹⁴ *Ibid.*



Para mitigar esse problema, o ecossistema nacional deve ser estabelecido com base em padrões de interoperabilidade de dados, de documentação, desenvolvimento, armazenamento, versionamento, testes e governança de modelos. Tais requisitos podem ser definidos por decreto e monitorados e atualizados por meio do alavancamento de instituições existentes, nomeadamente o CITDigital, a Secretaria de Ciência e Tecnologia para Transformação Digital, e o Comitê Gestor da Internet (CGI.br), junto com o proposto Sistema Nacional para Desenvolvimento, Regulação e Governança de Inteligência Artificial. A adoção de padrões semelhantes aos utilizados em centros internacionais de computação permitiria que pesquisas conduzidas em diferentes instituições brasileiras fossem replicáveis sem fricção.

A criação de uma Rede Nacional de Dados e o aprimoramento do SINAPAD, como destacado anteriormente, podem proporcionar o ambiente descentralizado ideal para armazenamento de dados, código, documentação e modelos. Este ambiente deveria oferecer versões congeladas de ambientes, pipelines de treinamento e ferramentas de auditoria automatizada, garantindo transparência e confiabilidade. Experiências como o Dataverse e o HuggingFace Hub demonstram a viabilidade de tais ambientes, que podem servir de catalisadores de colaboração científica e transferência tecnológica.

Além disso, a interoperabilidade deve ser garantida também no nível institucional. É necessário que universidades, centros de pesquisa, agências de fomento e órgãos públicos possam compartilhar dados, modelos e resultados de forma segura e padronizada. Isso requer coordenação institucional, além de arranjos normativos que harmonizem requisitos de sigilo, segurança, propriedade intelectual e governança de dados, evitando fragmentação e ineficiência.

5.6 Uma plataforma nacional de comunicação e colaboração profissional baseada em tecnologias *open source* e IA brasileira

Como foi destacado acima, o Estado brasileiro dispõe de instrumentos de compras públicas suficientemente amplos e flexíveis para funcionar como indutores estratégicos de inovação tecnológica autônoma.¹¹⁵ Em vez de se limitar à aquisição de ferramentas proprietárias estrangeiras para comunicação interna, gestão documental e colaboração institucional, a administração pública poderia mobilizar seu poder de compra para estruturar um ecossistema nacional de plataformas profissionais baseadas em tecnologias abertas e soluções de IA desenvolvidas no país. Tal abordagem seria compatível com princípios constitucionais de eficiência, economicidade e supremacia do interesse público, ao mesmo tempo em que fortaleceria a capacidade tecnológica nacional e reduziria dependências estruturais.

¹¹⁵ 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-edb2-40ac-85aa-5c5f4d2196f4/content>>.



A adoção governamental de soluções *open source*, como LibreOffice, Matrix, Jitsi ou Nextcloud, permitiria substituir – e parar de subsidiar – provedores de softwares proprietários e serviços de computação em nuvem estrangeiros amplamente utilizados na administração pública, garantindo auditabilidade, transparência, interoperabilidade e autonomia jurídica.¹¹⁶ Além disso, esses sistemas podem ser customizados para atender às necessidades específicas de órgãos públicos, sem riscos de *lock-in* tecnológico. Em paralelo, a incorporação de modelos brasileiros de IA – como, por exemplo, o Maritaca.ai ou outras iniciativas nacionais emergentes – possibilitaria a criação de assistentes de IA generativa e até agentes de IA e outras aplicações de apoio à tomada de decisão ancoradas em dados públicos e treinadas sob padrões de segurança e ética definidos pelo próprio Estado.¹¹⁷

Cabe ressaltar que a Rede Nacional de Ensino e Pesquisa (RNP) pode ser alavancada como núcleo estruturante de uma plataforma nacional de comunicação e colaboração profissional, baseada em tecnologias *open source* e IA desenvolvida no País. O Sistema RNP já provê conectividade avançada, software para colaboração profissional e serviços de nuvem para a rede acadêmica, demonstrando capacidade técnica e governança consolidada – apesar de sofrer de dependência em nuvem estrangeira.¹¹⁸ Sua adoção em escala pela administração pública federal, com ampliação de *data centers* sob jurisdição nacional, permitiria reduzir dependência de plataformas estrangeiras e fortalecendo a soberania digital.

Essas soluções poderiam operar sobre infraestrutura computacional nacional já existente, como o SINAPAD, o SERPRO ou provedores privados brasileiros capazes de oferecer nuvens sob jurisdição nacional, incluindo estruturas híbridas e federadas. O uso dessa infraestrutura permitiria consolidar um ambiente seguro, soberano e escalável, capaz de suportar cargas de IA generativa, armazenar documentos oficiais e viabilizar fluxos de trabalho interoperáveis entre diferentes órgãos da administração. Ou seja, permitiria alavancar o *open source* e as demais camadas da pilha de IA brasileira para experimentar o estabelecimento de um ecossistema digital autônomo.

Mobilizar o poder de compra estatal para esse fim requer ações coordenadas: definição de requisitos técnicos mínimos baseados em padrões abertos; criação de guias de interoperabilidade; certificação de soluções nacionais; e inserção, nos editais públicos, de critérios que priorizem tecnologias auditáveis, de código aberto e hospedadas em infraestrutura sob jurisdição brasileira. É igualmente necessário articular processos de transição tecnológica, com capacitação de servidores, suporte técnico contínuo e integração gradual com sistemas legados.

Criticamente, tal experimento não deveria ser considerado como um gasto adicional, mas, ao contrário, como uma oportunidade para reduzir significativamente os gastos em software e

¹¹⁶ BELLI, Luca. Compras Públicas como Alavanca da Soberania Digital. Câmara Técnica de Economia Digital (CTED) do CITDigital. 2025.

¹¹⁷ *Ibid.*

¹¹⁸ BR, Núcleo de Informação e Coordenação do Ponto; EVANGELISTA, Rafael de Almeida; RABELLO, Maricy, **Educação em um cenário de plataforma e economia de dados: soberania e infraestrutura**, São Paulo, SP: Núcleo de Informação e Coordenação do Ponto BR, 2023.



infraestruturas estrangeiras enquanto se fortalece a indústria nacional. Ao direcionar contratos públicos para soluções nacionais, o Brasil não apenas reduz dependências externas, mas estimula empresas, universidades e centros de inovação a desenvolver tecnologias competitivas e sustentáveis. Essa estratégia fortaleceria a indústria de software brasileira, criaria demanda estável para modelos de IA nacionais, expandiria o mercado de serviços de nuvem sob jurisdição local e consolidaria um ecossistema digital mais resiliente, transparente e alinhado aos princípios da soberania digital. Iniciativas semelhantes poderiam ser adotadas em outras plataformas e programas de governo como o SEI, gov.br, SUS digital, no eixo de ambientes e dispositivos do programa escolas conectadas etc.

5.7 A construção de um ecossistema digitalmente soberano por meio da CT&I

Como frisado na Seção 1.3, a construção de um ecossistema digitalmente soberano depende, de maneira estruturante, da capacidade de um país de organizar e mobilizar suas políticas de CT&I como instrumentos de autonomia estratégica, desenvolvimento produtivo e inclusão social. Em um contexto de crescente concentração tecnológica global, portanto, a CT&I assume papel central como vetor de redução de dependências, fortalecimento de capacidades nacionais e ampliação da margem de decisão soberana do Estado.

No Brasil, essa agenda vem sendo progressivamente incorporada aos principais instrumentos estratégicos, como a recente proposta de ENCTI 2024–2030, o PBIA, o SINAPAD, bem como iniciativas transversais como o supramencionado REDATA e a Nova Indústria Brasil¹¹⁹ (NIB). Contudo, a efetividade dessas políticas depende de sua articulação coerente, de financiamento sustentado e de ajustes institucionais que permitam a implementação das ambições expressas nos documentos estratégicos.

A ENCTI representa um marco relevante ao reconhecer explicitamente a soberania digital como dimensão estratégica do desenvolvimento nacional. Ao problematizar a dependência tecnológica em áreas como cadeia de valor de IA, semicondutores, computação de alto desempenho, e conectividade, a Estratégia destaca a necessidade de fortalecer capacidades científicas e tecnológicas endógenas. Essa abordagem reforça a compreensão de que ciência e tecnologia não são apenas insumos complementares ao crescimento econômico, mas fatores centrais de produção, capazes de moldar trajetórias de desenvolvimento, competitividade industrial e autonomia não somente tecnológica, mas também econômica e política.

Nesse contexto, o SINAPAD ocupa posição estratégica. Tradicionalmente percebido como provedor de serviços de supercomputação para a comunidade científica, o SINAPAD possui, em seus objetivos institucionais, funções mais amplas e estruturantes, incluindo a formação de recursos humanos especializados e o desenvolvimento de produtos e serviços nacionais de

¹¹⁹ **Nova Indústria Brasil**, Ministério da Fazenda, disponível em: <<https://www.gov.br/fazenda/pt-br/aceso-a-informacao/acoes-e-programas/transformacao-ecologica/programas-em-destaque/nova-industria-brasil/nova-industria-brasil>>. acesso em: 4 jan. 2026.



processamento de alto desempenho.¹²⁰ Essas dimensões são essenciais para a construção de soberania digital, na medida em que ampliam a capacidade do país de desenvolver soluções próprias em áreas intensivas em computação, como modelagem climática, bioinformática, simulações industriais, ciência de materiais e inteligência artificial.

Todavia, o funcionamento do SINAPAD tem sido historicamente prejudicado pela ausência de financiamento sustentado e previsível. A lógica de projetos episódicos e recursos fragmentados compromete a continuidade operacional, a atualização tecnológica e a retenção de talentos. Esse desafio poderia ser mitigado por meio de uma articulação mais estreita entre o SINAPAD e outras iniciativas estratégicas, como a política de nuvem de governo. A incorporação de compras públicas orientadas à inovação, prevendo a aquisição de serviços e produtos de HPC desenvolvidos no país, permitiria criar demanda estável e induzir o fortalecimento de fornecedores nacionais.

Adicionalmente, a articulação com o REDATA poderia contribuir para o financiamento do SINAPAD, desde que contrapartidas associadas aos incentivos concedidos fossem direcionadas ao fortalecimento da infraestrutura pública de processamento. Nesse arranjo, o REDATA deixaria de ser apenas um instrumento de atração de investimentos em data centers e passaria a funcionar como mecanismo indutor de capacidades nacionais, alinhado à agenda de soberania digital.

A NIB, especialmente por meio de sua Missão 4, também apresenta interface direta com essa agenda. Ao reconhecer a centralidade das tecnologias digitais para a reindustrialização e a competitividade do país, a NIB oferece uma oportunidade para alinhar políticas industriais, de CT&I e de transformação digital. No entanto, para que essa convergência se materialize, é fundamental articular explicitamente o SINAPAD, o PBIA, o REDATA e os instrumentos da NIB, evitando a fragmentação de esforços e a sobreposição de incentivos. A ausência dessa articulação tende a reduzir a eficácia das políticas e a ampliar riscos de dependência tecnológica.

A articulação estratégica supramencionada exige a designação clara de uma instância executiva com capacidade de coordenação transversal. Essa função deveria ser atribuída a uma secretaria executiva com mandato explícito para integrar políticas, alinhar prioridades, harmonizar instrumentos de financiamento e acompanhar a implementação das iniciativas relacionadas à soberania digital. Como destacado na Seção 1.3, no âmbito do Ministério de Ciência, Tecnologia e Inovação, a secretaria mais adequada para exercer esse papel é a Secretaria de Ciência, Tecnologia para a Transformação Digital, em razão de seu escopo institucional, de suas competências legais e de sua posição estratégica na interface entre CT&I, transformação digital e políticas industriais. O fortalecimento desse papel coordenador permitiria conferir maior coerência sistêmica às ações em curso, reduzir redundâncias, maximizar sinergias entre programas e assegurar que investimentos públicos em infraestrutura

¹²⁰ Relatório Seminário Pilha IA Soberana.



digital, dados e capacidades computacionais estejam efetivamente orientados aos objetivos de autonomia tecnológica e desenvolvimento nacional.

Além disso, nesse cenário, torna-se evidente a necessidade de criar um programa transversal dedicado à soberania digital no âmbito do FNDCT. Tal programa poderia ser estruturado a partir da realocação ou complementação de recursos do REDATA ou da alavancagem de outros fundos setoriais, como o Fundo de Universalização dos Serviços de Telecomunicações (FUST), o Fundo para o Desenvolvimento Tecnológico das Telecomunicações (FUNTTEL) e os recursos oriundos da cláusula de 1% do petróleo e da energia, prevista na legislação do setor energético. Contudo, cabe frisar que essa estratégia enfrentaria desafios políticos e institucionais relevantes, uma vez que exige negociação com os gestores e beneficiários desses fundos, tradicionalmente resistentes à ampliação de seus escopos originais.

Uma alternativa pragmaticamente mais viável seria a criação de programas de longo prazo voltados a ecossistemas de IA em setores estratégicos específicos, como IA para petróleo e gás, IA para cibersegurança das telecomunicações ou IA para energia. Esses programas poderiam complementar os 12 já existentes, com horizonte temporal ampliado, por exemplo de dez anos, permitindo maior previsibilidade e maturação tecnológica. Essa abordagem setorializada encontraria menor resistência política e pode funcionar como etapa intermediária para a consolidação de uma agenda mais ampla de soberania digital.

Neste contexto, a Secretaria de Ciência, Tecnologia para a Transformação Digital poderia liderar alianças estratégicas nacionais em IA, mobilizando atores setoriais em missões específicas como IA para petróleo e gás, cibersegurança das telecomunicações e sistemas energéticos. Tal coordenação articularia atores complementares: MCTI e CGEE na governança; LNCC, RNP e Centros Nacionais de Processamento de Alto Desempenho (CENAPADs) na operação de infraestrutura; instituições de CT&I como Fiocruz, Embrapa e CNPEM na provisão de dados científicos; e parceiros industriais dependendo dos setores (por exemplo, Petrobras/CENPES, SENAI CIMATEC, Instituto Eldorado, Positivo) em cofinanciamento e transferência tecnológica. Esse modelo federativo, estruturado mediante portal único de transparência, quotas definidas e Acordos de Nível de Serviço (SLAs, no acrônimo inglês) estabelecidos, converteria investimentos públicos em capacidade nacional contínua, reduzindo vulnerabilidades geopolíticas e acelerando descoberta científica através da integração sistêmica entre recursos computacionais, dados estratégicos e instrumentação.

Por fim, cabe reiterar que a coordenação entre os diversos atores envolvidos nessa agenda representa um dos desafios mais críticos. Nesse sentido, o CITDigital deveria desempenhar papel central como instância de articulação, alinhando iniciativas do MCTI, de outros ministérios, das agências de fomento, das instituições de CT&I e do setor produtivo. Sem mecanismos eficazes de coordenação, o risco de fragmentação institucional e de dispersão de recursos permanece elevado, comprometendo a efetividade das políticas de CT&I Digital. A proposta de um Sistema Nacional de Ciência, Tecnologia e Inovação em IA (SINIA), deve ser também considerada por seu potencial de tornar-se o principal arranjo de governança responsável pela implementação da porção da ENCTI relacionada à IA. Assim, ao articular



políticas, programas, infraestrutura, financiamento e regulação, o SINIA pode funcionar como eixo integrador da agenda de IA, assegurando coerência estratégica e alinhamento com os objetivos mais amplos de soberania digital e desenvolvimento nacional.



6 Recomendações Estratégicas de Regulação e Governança

A consolidação da soberania digital no Brasil depende de um conjunto articulado de medidas regulatórias, institucionais e procedimentais capazes de orientar o desenvolvimento tecnológico nacional, garantir segurança jurídica, estimular a inovação e promover a coordenação entre os diversos atores públicos e privados envolvidos nos diferentes elementos do ecossistema digital e nas camadas da pilha de IA.

A regulação deve ser compreendida como uma ferramenta de política pública orientada ao fortalecimento da autonomia tecnológica nacional, à redução de dependências sistêmicas e ao incremento de capacidades endógenas. Nesse sentido, torna-se primordial analisar o arcabouço normativo já existente, diagnosticar lacunas e propor ajustes que permitam organizar o ecossistema digital nacional de modo escalável, seguro, sustentável e alinhado a valores constitucionais e princípios democráticos.

A governança, por sua vez, deve ser pensada como um arranjo institucional que assegure a comunicação, a coordenação e a cooperação estável e contínua entre Estado, academia, setor privado e sociedade civil. A experiência nacional e internacional demonstra que a fragmentação institucional tende a comprometer a eficiência das políticas tecnológicas, ao passo que arranjos multissetoriais e orientados por objetivos e métricas claras e sustentados por instituições estáveis, favorecem o desenvolvimento de ecossistemas robustos.

No Brasil, o aproveitamento do CITDigital e do CGI.br, ambos já em operação, em conexão com os propostos Sistema Nacional para Desenvolvimento, Regulação e Governança de Inteligência Artificial, e a modernização do Sistema Nacional de Processamento de Alto Desempenho representariam passos importantes, mas exigem um esforço adicional para articular agendas comuns, padronizar práticas, ofertar infraestrutura e integrar instrumentos de fomento. A seguir, propõe-se um conjunto de orientações que podem auxiliar na construção de uma política de soberania digital de médio e longo prazo.

6.1 Ajustes regulatórios necessários

Como destacado anteriormente, o ordenamento jurídico brasileiro dispõe de instrumentos relevantes que podem sustentar uma política robusta de soberania digital, incluindo a Lei Geral de Proteção de Dados, o Marco Civil da Internet, a Lei de Governo Digital, várias normas de compras públicas, e regulamentações de segurança cibernética, além do Plano Brasileiro de Inteligência Artificial. No entanto, esses instrumentos foram concebidos de forma fragmentada, em momentos diferentes e com objetivos distintos. É preciso, portanto, harmonizar os dispositivos já existentes a fim de garantir coerência regulatória e direcionamento estratégico.

Para alcançar os objetivos sugeridos no capítulo precedente, é necessário consolidar um marco regulatório brasileiro de dados, estabelecendo não somente os princípios, mas também



os requisitos técnicos que entidades públicas e privadas devem observar no processamento, na interoperabilidade e na portabilidade de dados. Tais requisitos precisam ser diferenciados nos casos de dados pessoais sensíveis e dados confidenciais, bem como no uso de dados para modelos de alto risco e sistemas utilizados em contextos estratégicos, tais como defesa, energia, petróleo e gás, saúde e finanças.

Outro ajuste necessário consiste na criação da já mencionada Rede Nacional de Dados cujos membros deveriam atuar como instituições chave para facilitar a avaliação do cumprimento dos requisitos essenciais ao compartilhamento de dados. Tais ajustes normativos e institucionais são instrumentais para promover pesquisa e reprodutibilidade científica e cooperação científico-industrial, assegurando que o sistema científico nacional consiga operar de maneira integrada e autônoma.

6.2 Governança multissetorial

A elaboração e a implementação de uma visão estratégica nacional de soberania digital requerem um arranjo institucional capaz de garantir coordenação entre atores públicos, privados e acadêmicos. A governança multissetorial não deve ser interpretada como mera participação consultiva, mas como mecanismo estruturante para formulação, acompanhamento e execução de políticas. Neste sentido, o arranjo proposto deve aproveitar e aprimorar o papel das instâncias institucionais existentes, nomeadamente o CITDigital e o CGI.br, para que possam atuar em sinergia com eventuais arranjos futuros, como o Sistema Nacional para Desenvolvimento, Regulação e Governança de Inteligência Artificial.

A estruturação de um arranjo de governança descentralizada pode ser alavancada para permitir a comunicação, a coordenação e a colaboração dos atores sistêmicos, por meio de câmaras técnicas/comitês diretores responsáveis por temas priorizados, como infraestrutura computacional, dados, segurança cibernética, propriedade intelectual, políticas de inovação e integração com setores estratégicos. Para garantir efetividade, a governança deve operar com mandatos claros, competências definidas e responsabilidades compartilhadas.

Além disso, o arranjo de governança descentralizada proposto deveria incluir instâncias permanentes de diálogo com a indústria, incluindo empresas de tecnologia, setores regulados, *startups* e associações empresariais. A academia deve participar ativamente, não apenas por meio de especialistas individuais, mas por meio de consórcios interuniversitários e redes de pesquisa capazes de testar a eficiência e efetividade de normas, padrões, metodologias e boas práticas. A sociedade civil, por sua vez, deve integrar o processo para garantir que direitos fundamentais, inclusão digital e impactos sociais sejam contemplados em todas as etapas da política pública.

Arranjos descentralizados podem ser particularmente eficazes quando apoiados por mecanismos de transparência, procedimentos formais de consulta, definição clara de



responsabilidade, mecanismos de resolução de conflitos e métricas que orientam decisões.¹²¹ Para além de estruturas formais, é indispensável promover fluxos contínuos de informação entre ministérios, agências reguladoras, universidades e centros de pesquisa, assegurando que a política de soberania digital permaneça atualizada frente à rápida evolução tecnológica.

6.3 Alavancar as compras públicas para estimular a indústria nacional

As compras públicas constituem um poderoso instrumento de política industrial e tecnológica, especialmente em setores nos quais o Estado é um grande usuário de serviços e infraestruturas digitais. As experiências dos Estados Unidos e da China demonstram que, quando o setor público atua como cliente âncora, cria-se demanda previsível e de longo prazo capaz de estimular empresas nacionais, ampliar escala de produção e reduzir dependência externa. No Brasil, a legislação de licitações e contratos administrativos permite o uso de margens de preferência, critérios técnicos diferenciados, contratação integrada e encomendas tecnológicas, mas esses instrumentos ainda são subutilizados para estimular o crescimento do ecossistema digital nacional.¹²²

Para promover a soberania digital, as compras públicas devem priorizar soluções desenvolvidas por empresas nacionais, softwares abertos, modelos auditáveis e infraestruturas alinhadas às exigências nacionais de cibersegurança e governança. Recomenda-se a adoção de editais específicos que exijam abertura de código, documentação completa, interoperabilidade com padrões públicos definidos claramente, portabilidade e conformidade com requisitos de cibersegurança. Em setores sensíveis, como saúde, energia, petróleo e gás e defesa, o Estado pode estabelecer cláusulas de soberania, que determinem que dados e modelos críticos sejam processados exclusivamente em infraestrutura sob jurisdição nacional.

Sugere-se, ainda, a criação de um programa nacional de encomendas tecnológicas em IA, voltado à produção de modelos multimodais, bibliotecas de otimização, ferramentas de segurança e *frameworks* de MLOps, como design e *packaging* de semicondutores com financiamento compartilhado entre governo e empresas.¹²³ Para startups e pequenas empresas inovadoras, recomenda-se a adoção de compras públicas por fases, que permitam testes, pilotos e escalonamento gradual das soluções. Dessa forma, as compras públicas não apenas estimulam o mercado interno, mas também contribuem para a construção de uma pilha tecnológica nacional robusta.

¹²¹ CALCATERRA, Craig; KAAL, Wulf A., *Decentralized Governance*, 2021.

¹²² RAUEN, André Tortato. *COMPRAS PÚBLICAS PARA INOVAÇÃO NO BRASIL: O PODER DA DEMANDA PÚBLICA*; BELLI L. *Compras Públicas como Alavanca da Soberania Digital*. Câmara Técnica de Economia Digital (CTED) do CITDigital. 2025.

¹²³ Relatório Seminário Pilha IA Soberana.



6.4 Framework de compliance e certificação em segurança e proteção de dados

A consolidação da soberania digital brasileira demanda um sistema de *compliance* que vá além das estruturas existentes no Brasil em matéria de proteção de dados e segurança cibernética. É necessário estabelecer um arcabouço normativo e procedimental capaz de garantir que infraestruturas, serviços em nuvem, modelos de IA e plataformas de dados operem sob jurisdição, controle e governança nacional.

Para esse fim, deve ser criado um Framework Brasileiro de Soberania Digital, inspirado nos princípios estruturantes observados no *Cloud Sovereignty Framework* europeu, mas ajustado às realidades administrativas, regulatórias e industriais do Brasil. Como será destacado na conclusão deste texto, sugere-se que um estudo futuro analise os critérios e métricas necessários para que cada entidade pública ou privada possa avaliar seu próprio nível de dependência e vulnerabilidade tecnológica.

Esse framework deve articular três dimensões normativas principais: soberania jurídica, soberania técnica e soberania operacional. A soberania jurídica refere-se à exigência de que dados considerados sensíveis, confidenciais ou estratégicos sejam armazenados e auditados exclusivamente sob legislação brasileira, garantindo que a jurisdição nacional prevaleça sobre normas estrangeiras potencialmente conflitantes.

A soberania técnica implica que modelos, algoritmos, infraestruturas e plataformas devem incorporar requisitos de auditabilidade, portabilidade, interoperabilidade e documentação completas, permitindo escrutínio público e redução de dependências sistêmicas.

Já a soberania operacional estabelece padrões para controle de acesso, governança compartilhada, monitoramento contínuo, gestão de riscos, redundância e garantias contratuais que evitem interrupções ou captura tecnológica por fornecedores externos.

O *framework* proposto pode ser estruturado em quatro camadas complementares. A primeira camada envolve requisitos legais e regulatórios vinculantes, que estabeleçam direitos, obrigações e responsabilidades para fornecedores, operadores e entes públicos que utilizem IA e serviços de infraestrutura crítica. Essa camada deve harmonizar normas setoriais, diretrizes de proteção de dados pessoais e princípios de segurança cibernética, com base nos controles estabelecidos no Programa de Privacidade e Segurança da Informação (PPSI), criando um núcleo jurídico uniforme aplicável a todos os sistemas classificados como estratégicos. A segunda camada abrange padrões técnicos mínimos para armazenamento, processamento, criptografia, redundância física, auditoria e documentação, incluindo especificações para modelos de IA de alto risco e aplicações em setores sensíveis.

A terceira camada refere-se a requisitos de governança e transparência, contemplando documentação de ciclo de vida de modelos, logs de acesso, controle de versões, trilhas de auditoria, rastreabilidade de dados, gestão de incidentes e mecanismos de participação institucional. Essa camada deve promover alinhamento entre as práticas de entidades públicas, centros de pesquisa e empresas, assegurando padrões uniformes de governança algorítmica. A quarta camada envolve certificação e conformidade, por meio de laboratórios



independentes, acreditados e integrados à Rede Nacional de Dados e ao SINAPAD – e, eventualmente, ao Sistema Nacional para Desenvolvimento, Regulação e Governança de Inteligência Artificial – responsáveis por testar e verificar o atendimento aos requisitos jurídicos, técnicos e operacionais.

A certificação deve ser escalonável, com níveis progressivos de exigência conforme o risco e a criticidade das aplicações. Serviços de nuvem para órgãos públicos podem ser certificados quanto à residência e à soberania de dados, verificando a inexistência de vínculos contratuais ou técnicos que permitam acesso por jurisdições estrangeiras. Modelos de IA podem ser testados quanto a robustez, equidade, transparência e rastreabilidade. Infraestruturas críticas podem ser avaliadas quanto a mitigação de riscos sistêmicos, planos de contingência, independência tecnológica e interoperabilidade com padrões nacionais.

Essa estrutura visa permitir ao Brasil avançar na direção de uma soberania digital efetiva, garantindo que o Estado e a sociedade tenham autonomia para desenvolver, operar e fiscalizar sistemas essenciais, reduzindo dependências estratégicas e promovendo inovação responsável. A adoção desse *framework* fortalece a confiança institucional, qualifica o ecossistema digital e estabelece bases sólidas para políticas de desenvolvimento tecnológico e produtivo, e de governança capazes de embutir efetivamente o disposto normativo em tecnologias.



7 Política De Desenvolvimento Tecnológico e produtivo para a Soberania Digital

A construção de uma política robusta para a inteligência artificial no Brasil requer a articulação entre infraestrutura, formação técnica, governança, mecanismos de financiamento e estímulos diretos à produção de modelos, software e hardware nacionais que possam oferecer alternativas sólidas aos sistemas atualmente dominantes. Como destacado nas seções precedentes, ecossistemas tecnológicos soberanos dependem da capacidade de um Estado em coordenar investimentos, incentivar pesquisa, estimular mercados, reduzir dependências externas e estabelecer parcerias estratégicas com o setor privado e com a academia.

No contexto brasileiro, a política digital não pode ser reduzida a incentivos pontuais ou a iniciativas isoladas. Ela deve constituir-se como política de Estado, com visão de longo prazo, fortemente ancorada na demanda pública, na digitalização do setor industrial e na reindustrialização do setor eletrônico, bem como na formação de competências e na criação da Rede Nacional de Dados, acompanhada pelo aprimoramento da infraestrutura nacional de computação. Essa política deve contemplar mecanismos de fomento contínuo, que sustentem desde a pesquisa fundamental até a aplicação comercial.

A seguir, desenvolvem-se algumas recomendações estruturadas em cinco eixos: *i)* fortalecimento da infraestrutura nacional; *ii)* estímulo ao desenvolvimento de software e hardware; *iii)* incentivo ao *open source*; *iv)* integração com setores estratégicos; e, *v)* parcerias público-privadas e instrumentos financeiros.

7.1 Fortalecimento da infraestrutura tecnológica fundamental

O fortalecimento da infraestrutura tecnológica é o eixo fundante da soberania digital brasileira. A capacidade de armazenar dados, treinar modelos, realizar inferência em larga escala e garantir resiliência cibernética depende de conectividade significativa, uma rede energética performante, supercomputadores, *clusters* de GPUs e arquiteturas seguras para processamento de dados. Como frisado em seções precedentes, o diagnóstico nacional revela que o Brasil ainda carece de capacidade computacional compatível com as exigências contemporâneas da IA de fronteira.¹²⁴ Embora iniciativas como o Sistema Nacional de Processamento de Alto Desempenho (SINAPAD), as redes acadêmicas e alguns *data centers* estaduais constituam bases relevantes, a infraestrutura permanece fragmentada, heterogênea e aquém da escala necessária.

O PBIA representa um avanço fundamental ao reconhecer a infraestrutura computacional como elemento estratégico para o desenvolvimento da IA e para a soberania digital. Todavia, a efetividade dessa agenda depende de maior previsibilidade e sustentabilidade das fontes de financiamento destinadas à infraestrutura nacional de processamento, em particular no contexto do fortalecimento e da expansão do novo SINAPAD. Assim, a ausência de uma

¹²⁴ *Ibid.*



estratégia integrada de financiamento e coordenação compromete o aproveitamento pleno do potencial do SINAPAD e das iniciativas listadas no PBIA, limitando sua capacidade de alcançar escala necessária para sustentar, de forma contínua e competitiva, as demandas crescentes da pesquisa científica, da inovação tecnológica e das aplicações avançadas de IA.

O fortalecimento dessa infraestrutura exige investimentos continuados e uma estratégia federada, capaz de integrar recursos federais, estaduais, acadêmicos e privados. Duas prioridades devem orientar tal estratégia. Primeiramente, orientar incentivos fiscais, orçamentários e creditícios para construção e modernização de data centers baseados em capital e gestão nacional, aquisição de supercomputadores e integração de redes acadêmicas de alta velocidade. Deve contemplar ainda mecanismos de encomendas tecnológicas para desenvolvimento de soluções nacionais de orquestração, virtualização, segurança e gestão de clusters de IA. Como será enfatizado nas próximas seções, a adoção de padrões abertos, o estímulo a arquiteturas soberanas como RISC-V e a ampliação de capacidades técnicas do país em semicondutores também são componentes essenciais, criando condições futuras para uma autonomia crescente em hardware.

Em segundo lugar, a proibição das práticas de *zero rating* e a plena implementação do artigo 9º do Marco Civil da Internet devem ser tratadas como prioridades estruturantes para a soberania digital brasileira, tomando como referência o sucesso da experiência da Índia, precedentemente ilustrada. Ao assegurar a neutralidade de rede e impedir práticas discriminatórias no tráfego, o país cria condições para que a infraestrutura tecnológica nacional seja efetivamente alavancada por meio de conectividade significativa, permitindo que qualquer pessoa acesse e compartilhe, de forma não discriminatória, qualquer serviço, aplicação ou conteúdo – desde que legais e ciberseguros – independentemente do hardware utilizado. Somente em um ambiente em que o fluxo de dados não é artificialmente direcionado para plataformas dominantes será possível estimular inovação nacional, ampliar a concorrência com base na qualidade e favorecer o surgimento de soluções tecnológicas alinhadas às necessidades brasileiras.

7.2 Estímulo ao desenvolvimento de modelos, software e hardware

A soberania lógica, referente à capacidade de produzir algoritmos, frameworks, bibliotecas, sistemas operacionais e modelos pré-treinados, é tão fundamental quanto a soberania infraestrutural. No Brasil, a produção científica em IA é expressiva, mas a capacidade de transformar pesquisa em infraestrutura lógica de larga escala ainda é limitada. Um dos maiores déficits nacionais é a dependência de modelos fechados e de software e bibliotecas proprietárias, dificultando auditoria, segurança e controle sobre sistemas críticos.¹²⁵

A política de CT&I deve promover o desenvolvimento de modelos nacionais pré-treinados, com ênfase em abertura, diversidade linguística, respeito à legislação pátria, representatividade

¹²⁵ *Ibid.*



cultural e aplicações estratégicas. A partir dos avanços trazidos pelo PBIA, recomenda-se o lançamento de programas de grande escala, envolvendo consórcios entre universidades, empresas públicas, empresas privadas e centros de supercomputação, para produzir modelos de linguagem geral e modelos setoriais, como os de saúde, energia, clima e agricultura.

No entanto, cabe reiterar que, na ausência de conectividade significativa, os esforços voltados ao aprimoramento da capacidade algorítmica do país serão provavelmente voltados ao fracasso, sendo as modalidades de acesso à internet essenciais para favorecer a adoção tecnológica.

No campo do software, recomenda-se o estímulo a bibliotecas e *frameworks* nacionais, especialmente nas camadas intermediárias da pilha, como MLOps, ferramentas de otimização, sistemas de execução distribuída e plataformas de inferência. Esses elementos reduzem dependências e fortalecem capacidades internas, permitindo que empresas nacionais integrem soluções personalizadas e soberanas.

Quanto ao hardware, embora a produção doméstica de GPUs seja de elevada complexidade tecnológica e industrial, o Brasil pode avançar em etapas críticas da cadeia, como design, encapsulamento e teste de chips, além de participar do ecossistema global de RISC-V. A política de desenvolvimento tecnológico e produtivo deve incluir investimentos em laboratórios de microeletrônica, apoio a *startups fabless* e parcerias com países que dominam tecnologias abertas, como a Índia e a China. A longo prazo, a consolidação de uma cadeia nacional de hardware aberto pode contribuir de forma decisiva para a redução de dependências estruturais e para o fortalecimento da soberania tecnológica.

7.3 Incentivo ao *open source* como vetor de autonomia

O *open source* representa um dos mais importantes vetores de autonomia tecnológica, inclusive no campo da IA. Modelos, bibliotecas e plataformas abertas permitem a inspeção pública, a auditabilidade, a independência de fornecedores e a capacidade de adaptação às necessidades locais. A experiência comparada mostra que países que investem em *open source* alcançam maior autonomia e reduzem dependências estratégicas. A China, por exemplo, consolidou ecossistemas robustos de aprendizado profundo e *frameworks* abertos, que servem como base para sua autonomia tecnológica. A Suíça, com o projeto Apertus, demonstra que modelos abertos podem ser tão eficientes quanto modelos fechados, com a vantagem adicional da transparência.

O Brasil pode impulsionar o *open source* por meio de três estratégias. A primeira é o financiamento público de projetos abertos de IA, incluindo modelos nacionais, bibliotecas, bancos de dados e sistemas de execução distribuída. Esses projetos devem ser desenvolvidos em repositórios públicos, com documentação completa, licenças permissivas e governança aberta. A segunda estratégia é a adoção prioritária de software aberto pela administração pública, mediante editais que exijam transparência, auditabilidade e reutilização de código. A terceira estratégia é a inclusão de disciplinas práticas e atividades de extensão em cursos



superiores voltadas para o desenvolvimento/avaliação de softwares e hardwares abertos e ciberseguros (uso da educação para resolver problemas práticos). A quarta é o fomento a comunidades de desenvolvedores, universidades, startups e organizações sociais voltadas ao uso e produção de *open source*. Essa rede fortalece a capacidade nacional de inovação e reduz custos, ao mesmo tempo em que protege a soberania lógica brasileira.

O *open source*, contudo, deve ser acompanhado de políticas sólidas de cibersegurança, governança e *compliance*, evitando riscos decorrentes de dependência de comunidades externas, da exploração de vulnerabilidades desconhecidas ou de falhas de manutenção. O *framework* de soberania proposto anteriormente pode contribuir para mitigar esses riscos, definindo critérios e controles voltados a assegurar que soluções abertas utilizadas pelo Estado ou por empresas estratégicas estejam alinhadas a padrões de segurança e conformidade.

7.4 Desenvolvimento de ecossistemas de inovação e integração com setores estratégicos da economia

Para que a política de soberania digital produza impactos estruturantes, ela deve ser integrada a setores estratégicos da economia brasileira, tais como energia, petróleo e gás, saúde, finanças, agroindústria, mobilidade e defesa. Esses setores possuem grande capacidade de investimento, exigem tecnologias avançadas e podem atuar como alavancas para o desenvolvimento tecnológico nacional. A transformação digital e, particularmente, a integração entre IA e setores estratégicos são especialmente relevantes e não devem ocorrer de forma pontual, mas por meio de programas articulados e alianças setoriais implementadas por meio de missões estratégicas que promovam pesquisa aplicada, compartilhem infraestrutura e gerem oportunidades de inovação.

No setor energético e no de petróleo e gás, o uso de IA pode melhorar a eficiência operacional, reduzir custos, aumentar a segurança e promover a sustentabilidade. A Petrobrás já é um dos maiores investidores em infraestrutura digital do país e, junto com outras empresas do setor elétrico e grandes consumidores energéticos, pode atuar como clientes âncora para soluções nacionais de IA, apoiando o treinamento de modelos de previsão, detecção de anomalias e otimização de processos. Para isso, é necessário estabelecer consórcios entre empresas, universidades e centros de supercomputação, compartilhando dados, infraestrutura e financiamento.

Na área da saúde, o uso de IA em diagnóstico, gestão e pesquisa depende de bases de dados sensíveis e de infraestrutura segura. O Brasil pode criar plataformas federadas de dados de saúde, respeitando a LGPD e normas de segurança da informação, para treinamento de modelos nacionais capazes de atender às especificidades epidemiológicas e culturais do país. A produção de modelos abertos de saúde pública pode reduzir custos, ampliar o acesso aos tratamentos mais necessários para a população brasileira e fortalecer a autonomia sanitária.

O setor financeiro, por sua vez, já apresenta grande maturidade tecnológica e capacidade de investimento. O Banco Central, a Febraban e empresas do setor podem financiar modelos



nacionais de detecção de fraude, crédito responsável e previsão de risco sistêmico. Na agroindústria, o uso de IA pode melhorar produtividade, sustentabilidade e resiliência climática, permitindo que o Brasil desenvolva soluções proprietárias e competitivas globalmente.

É sabido que alguns setores possuem forte enraizamento territorial, a exemplo do setor de petróleo. É preciso aproveitar e cultivar especializações locais em favor da soberania digital. No Rio de Janeiro, por exemplo, a presença de infraestruturas de supercomputação financiadas pela Petrobras, conjugada à atuação de ICTs especializadas, configura ecossistema de inovação cuja potencialidade requer articulação institucional mediante alianças estratégicas entre União, estados e municípios. Vale avaliar que outras capacidades poderiam ser desenvolvidas por esse ecossistema a partir das competências já existentes.

Além disso, faz-se imperativa a exploração de novos encadeamentos produtivos inter-regionais a partir desse ecossistema. Questiona-se, exemplificativamente, como articular o polo de microeletrônica de Campinas às demandas tecnológicas do Rio de Janeiro, e que formas de cooperação institucional permitiriam integrar as competências em IA para descoberta científica entre esses dois centros de excelência acadêmica. Paralelamente, cabe discutir mecanismos para interligar esses polos e Brasília às capacidades em cibersegurança sendo desenvolvidas em Recife, construindo arquitetura federativa que capitalize as vocações regionais complementares. A exemplo da experiência chinesa mencionada na Seção 4.2, a constituição de polos de excelência em determinadas localidades desempenha um papel instrumental para desenvolver/atrair talentos, investimentos e massa crítica para superar desafios complexos e criar um sistema virtuoso de desenvolvimento.

7.5 Mecanismos público-privados e instrumentos financeiros

A política de desenvolvimento de IA exige financiamento contínuo, previsível e coordenado. Os atuais instrumentos de fomento, embora relevantes, ainda são fragmentados e insuficientes diante da escala necessária. É imperativo criar mecanismos que articulem fomento público, investimento privado, instrumentos de crédito e encomendas tecnológicas.

Recomenda-se o estabelecimento e a coordenação de fundos setoriais específicos para apoio a autonomia tecnológica. Esses fundos, se bem articulados, podem financiar de modo efetivo desde pesquisa fundamental até projetos industriais, incluindo treinamento de modelos, construção de infraestrutura e desenvolvimento e adoção de software e hardware aberto.

O Brasil pode também adotar instrumentos de financiamento baseados em desempenho, como contratos de impacto tecnológico, que remuneram empresas de acordo com metas de inovação, soberania e segurança. Encomendas tecnológicas dirigidas, especialmente para modelos abertos, sistemas críticos e *frameworks* de IA, devem compor o núcleo da política de soberania digital. Além disso, é necessário criar incentivos fiscais para empresas que investem em IA soberana, incluindo dedução de investimentos em P&D, créditos tributários e redução de encargos sobre contratos de pesquisa.



Por fim, é fundamental desenvolver mecanismos de parceria público-privada que permitam que universidades, centros de supercomputação e institutos tecnológicos operem como prestadores de serviços de IA, gerando receitas próprias e ampliando sua sustentabilidade financeira.



8 Cooperação Internacional para a Soberania Digital: Padrões, Regimes Jurídicos, Ciência e Indústria

A construção da soberania digital brasileira não implica isolamento, mas, ao contrário, participação ativa e estratégica em regimes internacionais de governança tecnológica. A autonomia tecnológica deve ser considerada como uma função da capacidade interna combinada com a atuação diplomática externa capaz de influenciar normas multilaterais, regimes de padronização e arranjos cooperativos de pesquisa e desenvolvimento. No contexto das pilhas digitais, cujas camadas lógicas, informacionais e de riscos ultrapassam fronteiras nacionais, a cooperação internacional torna-se um elemento estruturante. Ela deve ocorrer simultaneamente em quatro frentes interdependentes.

A primeira frente é a definição de padrões técnicos comuns. Infraestruturas digitais dependem de interoperabilidade, protocolos abertos, formatos padronizados de dados, mecanismos de segurança e regras compartilhadas entre países e blocos econômicos. A participação brasileira em organismos intergovernamentais como a ITU ou em organismos técnicos como ISO, IEEE e IETF, bem como em redes regionais ou temáticas de padronização, é fundamental para assegurar que padrões internacionais reflitam necessidades nacionais e do Sul Global, e não apenas interesses das grandes potências e corporações globais. Especialmente, a elaboração de padrões para modelos de IA, métricas de confiabilidade, interoperabilidade de dados, requisitos de cibersegurança e certificações técnicas deve ser tratada como instrumento de soberania, pois padrões globais definem não apenas especificações tecnológicas, mas também preferências regulatórias e posições de poder na economia digital.

A segunda frente é a necessidade de costurar parcerias internacionais para influenciar a definição de regimes internacionais que interessam as demais camadas da pilha, com base em princípios jurídicos, normas substantivas e mecanismos eficazes de resolução de controvérsias. Pilhas digitais implicam fluxos transfronteiriços de dados, uso de computação em nuvem internacional, dependência de cadeias globais de semicondutores e riscos comuns de cibersegurança. Tais elementos exigem *frameworks*, tratados, princípios e acordos que regulem proteção de dados, transferência internacional de informações, riscos (sistêmicos) determinado pelos próprios sistemas de IA, direitos de propriedade intelectual, e salvaguardas geopolíticas. O Brasil deve atuar para que tais regimes tenham mecanismos de solução de disputas que não reproduzam assimetrias econômicas ou jurídicas, incorporando princípios de autonomia tecnológica, autodeterminação informativa, transparência, proporcionalidade, proteção de direitos humanos e salvaguarda do devido processo.

A terceira frente é a cooperação científica internacional. A pesquisa em IA e infraestrutura digital beneficia-se de projetos conjuntos, laboratórios multinacionais, redes de pesquisa, intercâmbio de pesquisadores e compartilhamento responsável de dados e modelos. Parcerias com universidades latino-americanas, europeias, africanas e asiáticas permitem ao Brasil reduzir dependências tecnológicas, ao mesmo tempo em que ampliam sua capacidade de



desenvolver e eventualmente exportar software, hardware e modelos próprios. A cooperação científica também fortalece boas práticas de ciência aberta, reprodutibilidade, auditoria e desenvolvimento responsável, criando ambientes regulatórios e institucionais alinhados a padrões globais de excelência científica.

A quarta frente é a cooperação comercial e industrial. A autonomia tecnológica depende de integração em cadeias produtivas internacionais de semicondutores, equipamentos de telecomunicações, hardware avançado, serviços de nuvem, componentes críticos e modelos de IA. O Brasil deve articular-se com parceiros estratégicos para atrair investimentos, desenvolver clusters industriais, participar de redes globais de inovação e estabelecer acordos que reduzam vulnerabilidades materiais na camada de recursos minerais e energéticos. Cooperação bilateral e multilateral pode incluir codesenvolvimento de tecnologias, transferência de conhecimento, *joint ventures*, parcerias regionais e acordos setoriais, especialmente por meio da exploração de parcerias estratégicas com países do bloco BRICS e do Mercosul, ampliando a capacidade do Brasil de competir e cooperar na economia digital.

Em conjunto, essas quatro frentes revelam que a cooperação internacional não é alternativa à soberania: ao contrário, é uma dimensão necessária da atuação soberana. Uma estratégia nacional de autonomia digital deve combinar fortalecimento interno com presença ativa nos regimes internacionais, de modo a assegurar que o ecossistema digital brasileiro não seja isolado, mas permaneça integrado ao mundo, mediante regras compartilhadas que preservem a autonomia, a segurança e o interesse público nacional.

8.1. Uma inserção qualificada na governança internacional

Para o Brasil, quatro eixos de cooperação internacional revelam-se particularmente estratégicos: *i)* a cooperação multilateral no âmbito do sistema das Nações Unidas; *ii)* a cooperação regional e plurilateral, incluindo BRICS, Mercosul e mecanismos UE–Mercosul; *iii)* a cooperação bilateral dirigida a setores críticos como semicondutores, infraestruturas públicas digitais e modelos de IA; e, *iv)* a cooperação técnica direta em organismos internacionais de padronização como ISO, IEEE, IETF, W3C e outros fóruns que definem as bases normativas e operacionais das infraestruturas digitais globais.

Esses quatro movimentos precisam ser articulados de forma coordenada pelo governo brasileiro, com apoio estratégico do corpo diplomático, alavancando os arranjos existentes, como por exemplo a sólida participação do CGI.br, da ANATEL ou do MCTI em fóruns internacionais dedicados à padronização e à governança da internet, como a Uniao Internacional das Telecomunicações, ou mesmo do aparato de diplomacia cibernética do Ministério das Relações Exteriores, ativamente envolvido em fóruns da ONU como o *UN Group of Government Experts* (UNGGE) e o *Group of Governmental Experts* (GGE).¹²⁶ Adicionalmente,

¹²⁶ 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.



o Ministério das Relações Exteriores, por meio do recém-criado Escritório do Embaixador de Tecnologia, também pode desempenhar papel essencial no monitoramento de negociações, na antecipação de tendências, na identificação de riscos regulatórios e na articulação de posições nacionais.

Contudo, a diplomacia deve operar de forma integrada aos órgãos que coordenam o tema internamente, para que conjuntamente se mobilize a comunidade técnica, as universidades, os centros de pesquisa, as agências reguladoras e o setor privado, em torno dos fóruns de padronização, onde decisões aparentemente técnicas moldam dinâmicas políticas, econômicas e estratégicas. A combinação desses eixos fortalece a capacidade do Brasil de influenciar normas internacionais, proteger interesses nacionais e construir, camada por camada, uma pilha digital soberana.

8.2. Cooperação no âmbito do sistema das Nações Unidas

A arquitetura institucional da ONU oferece um conjunto de mecanismos multilaterais particularmente relevantes para a construção da soberania digital brasileira, pois combina fóruns normativos, técnicos, científicos e de desenvolvimento econômico. A União Internacional de Telecomunicações (UIT) constitui o principal organismo responsável pela definição de padrões globais de telecomunicações, espectro, redes móveis e interoperabilidade técnica. A participação qualificada do Brasil na UIT é essencial para influenciar padrões que moldam diretamente as camadas de infraestrutura de conectividade e de infraestrutura computacional da pilha digital brasileira, assegurando que normas técnicas internacionais não provoquem assimetrias que impossibilitem o desenvolvimento de soluções locais.

A *UN Trade and Development* (UNCTAD), por sua vez, fornece arcabouço analítico e regulatório sobre economia digital, fluxos de dados, comércio eletrônico e cadeias globais de valor. Ao engajar-se de forma ativa nesses debates, o Brasil pode fortalecer posições normativas relacionadas à autonomia informacional, à tributação de dados e ao desenvolvimento industrial em tecnologias estratégicas. A UNESCO desempenha papel central na dimensão ética, cultural e educacional da inteligência artificial, e sua Recomendação sobre a Ética da IA fornece parâmetros relevantes para a governança de riscos e para políticas de capacitação transversal.

O Fórum de Governança da Internet (IGF), embora não normativo, constitui espaço estratégico para construção de consenso, identificação, de tendências e soluções a problemas compartilhados, circulação de conhecimento técnico e fortalecimento da participação multissetorial, permitindo ao Brasil articular suas prioridades com atores globais e regionais.¹²⁷ Esses organismos, considerados em conjunto, formam um ecossistema de governança que possibilita ao país projetar seus interesses e alinhar sua pilha digital às dinâmicas internacionais.

¹²⁷ *Ibid.*



8.3. Cooperação em clubes e mecanismos regionais de governança: BRICS, Mercosul e diálogos UE–Mercosul

Arranjos regionais ou plurilaterais são instrumentos centrais para o exercício de soberania digital compartilhada, especialmente em temas que exigem escala, complementaridade e convergência regulatória. O BRICS constitui plataforma estratégica para o Brasil, pois reúne países com políticas industriais robustas em semicondutores, IA, redes 5G/6G e governança de dados. Iniciativas como o BRICS *Institute of Future Networks*, o *New Development Bank* e grupos de trabalho sobre economia digital e segurança das TIC podem apoiar projetos de interconexão regional, pesquisa científica conjunta e desenvolvimento de padrões técnicos alternativos. No nível industrial, há potencial para cooperação em design de chips, cadeias de suprimento de minerais estratégicos, sistemas de pagamentos digitais, e desenvolvimento de modelos abertos multilíngues.

O Mercosul pode atuar como espaço de harmonização regulatória em privacidade, proteção de dados, segurança cibernética e infraestrutura de conectividade regional. A construção de políticas digitais regionais facilita a circulação de dados, fortalece redes de pesquisa e permite que países vizinhos compartilhem recursos computacionais e capacidade técnica. O diálogo UE–Mercosul, embora complexo, oferece oportunidade para cooperação em padrões técnicos, governança de dados e IA, regulação de plataformas e infraestrutura crítica. A experiência europeia em proteção de dados, certificação e interoperabilidade é particularmente útil para o fortalecimento de marcos regulatórios brasileiros, desde que adaptada às realidades regionais e sem induzir dependências tecnológicas excessivas. Em conjunto, esses arranjos regionais permitem que o Brasil construa coalizões estratégicas e amplie seu poder de barganha nos regimes globais.

8.4. Cooperação bilateral estratégica: semicondutores, IA e infraestrutura crítica

A soberania digital brasileira também depende de alianças bilaterais dirigidas a setores-chave da pilha, especialmente semicondutores, hardware avançado, computação em nuvem sob jurisdição nacional, conectividade segura e modelos de IA. Na indústria de semicondutores, a cooperação bilateral é fundamental porque a cadeia produtiva é altamente especializada e concentrada em poucos países. Parcerias com China, Taiwan, Coreia do Sul, Índia, Alemanha e Estados Unidos podem incluir transferência de conhecimento, codesenvolvimento de tecnologias, capacitação técnica e participação do Brasil em etapas específicas da cadeia, como encapsulamento, testes, caracterização, design ou manufatura de nicho. Esse tipo de cooperação reforça a camada de recursos minerais e energéticos ao integrar o país a cadeias globais estratégicas.

No campo da IA, acordos bilaterais podem fomentar laboratórios conjuntos, intercâmbio de pesquisadores, compartilhamento responsável de dados anonimizados e codesenvolvimento



de modelos abertos. Em infraestrutura crítica, parcerias com países com expertise em redes de alta capacidade e energia limpa podem fortalecer as camadas de infraestrutura computacional e conectividade, assegurando resiliência e autonomia. Cooperação bilateral estruturada deve ser orientada por princípios de soberania, transparência, reciprocidade e proteção de dados, evitando acordos que gerem dependências assimétricas ou delegação excessiva de funções essenciais a fornecedores estrangeiros.

8.5. A cooperação técnica em organismos internacionais de padronização

A participação ativa em organismos de padronização técnica é uma das ferramentas mais eficazes para ampliar a autonomia digital de um país. Nesses espaços, definem-se protocolos, requisitos de segurança, modelos de interoperabilidade, arquiteturas de rede, padrões de conectividade e parâmetros normativos e operacionais que estruturam a infraestrutura global.

Na ISO e na IEC, discutem-se normas sobre segurança da informação, governança de dados, IA e sistemas críticos. No IEEE, desenvolvem-se padrões para hardware, redes, computação distribuída, robótica e sistemas de energia. No IETF e no W3C, são construídos os protocolos fundamentais que regem o funcionamento da internet e da web, desde endereçamento e transporte até interfaces web e criptografia. Cada decisão tomada nesses organismos afeta diretamente a capacidade do Brasil de projetar e operar sistemas digitais estratégicos em condições de igualdade.

Cabe frisar que o Brasil ocupa posição de destaque no âmbito da *RISC-V International*, tendo ingressado como membro premium da aliança em fevereiro de 2024 e tendo integrado o Conselho Diretivo da entidade¹²⁸, o que lhe assegura representação direta e capacidade de influenciar o desenvolvimento dessa tecnologia aberta de arquitetura de processadores. A adesão brasileira, com a única representação governamental no Conselho da entidade, vinculada ao MCTI, constitui movimento estratégico para a formulação de políticas públicas em CT&I, particularmente no tocante ao desenvolvimento soberano de semicondutores. Tal participação qualificada permite ao país atuar proativamente na definição de padrões tecnológicos abertos e na governança de ecossistema que se apresenta como alternativa viável à dependência de arquiteturas proprietárias. A presença brasileira no conselho da *RISC-V International* representa, portanto, oportunidade concreta de inserção em rede global de inovação tecnológica, com potencial para catalisar o desenvolvimento de capacidades nacionais em microeletrônica mediante acesso a padrões abertos, conhecimento técnico compartilhado e articulação com atores internacionais relevantes.

Porém, apesar dos destaques mencionados acima, a presença brasileira em organismos internacionais de padronização ainda é limitada, muitas vezes restrita a esforços individuais de universidades e pesquisadores. A ampliação dessa participação exige estrutura institucional,

¹²⁸ EM 12/03/2024 14H35, Publicado, **Brasil se torna membro da Aliança RISC-V International**, Ministério da Ciência, Tecnologia e Inovação, disponível em: <<https://www.gov.br/mcti/pt-br/acompanhe-o-mcti/noticias/2024/03/brasil-se-torna-membro-da-alianca-risc-v-international>>. acesso em: 5 jan. 2026.



financiamento contínuo, articulação diplomática e, sobretudo, coordenação técnica nacional. A participação não deve ser reativa ou pontual: precisa ser estratégica, orientada por prioridades nacionais (cibersegurança, IA, computação em nuvem sob jurisdição nacional, 5G/6G, interoperabilidade de dados públicos etc.) e conectada às camadas da pilha digital. Ao engajar-se de forma consistente nesses organismos, o Brasil contribui para moldar padrões que atendam às suas necessidades e evita que o país se torne mero importador de normas originadas em contextos geopolíticos distintos e muitas vezes incompatíveis com suas realidades sociais, econômicas e regulatórias.

Nesta perspectiva, é importante lembrar que a Ação 54 do PBIA almeja colmatar esta lacuna, permitindo a inserção estrategicamente estruturada do Brasil no debate internacional sobre padronização técnica relativa à IA, ao almejar a criação de uma rede de apoio à participação qualificada do país em fóruns e processos multilaterais relevantes.¹²⁹ Essa ação busca estruturar e articular uma rede de pesquisadores, especialistas e técnicos capaz de ampliar, qualificar e conferir maior consistência à atuação brasileira nos debates internacionais sobre IA, incluindo temas como governança, padrões técnicos, ética, regulação e cooperação científica. Essa iniciativa é particularmente relevante diante do vácuo historicamente deixado pelo poder público e por empresas nacionais nos fóruns nacionais e internacionais de padronização, espaço que tem sido ocupado, em grande medida, por filiais de empresas estrangeiras. Nessas instâncias, tais filiais tendem a incorporar e promover os interesses estratégicos de suas matrizes, influenciando a definição de normas e padrões técnicos nacionais de forma potencialmente desalinhada das prioridades de desenvolvimento e soberania tecnológica do país.

As entregas previstas para 2026 no que diz respeito à Ação 54 reforçam o caráter estruturante de tal medida, destacando-se, de um lado, o apoio ao estabelecimento da Rede Internacional de Colaboração em IA generativa soberana, voltada à cooperação entre países e instituições comprometidos com modelos abertos e com a autonomia tecnológica; e, de outro, a contratação de um estudo abrangente sobre riscos, oportunidades e soluções seguras para o compartilhamento de dados nacionais em iniciativas de cooperação internacional destinadas ao desenvolvimento de modelos de IA generativa aberta. Essas entregas são instrumentais para assegurar que a participação do Brasil em iniciativas internacionais de IA ocorra de forma coordenada, tecnicamente qualificada e alinhada aos objetivos de soberania digital, proteção do interesse público e fortalecimento de capacidades científicas e tecnológicas endógenas.

Por fim, cabe lembrar que o CGI.br ocupa posição singular para articular e coordenar a participação brasileira em vários organismos internacionais de padronização. Sua natureza multissetorial – integrando governo, setor privado, academia e sociedade civil – é especialmente adequada aos desafios contemporâneos da definição de padrões tecnológicos,

¹²⁹ MINISTÉRIO DA CIÊNCIA, TECNOLOGIA E INOVAÇÕES, **Plano Brasileiro de Inteligência Artificial (PBIA) 2024-2028**, Laboratório Nacional de Computação Científica - LNCC, disponível em: <<https://www.gov.br/lncc/pt-br/assuntos/noticias/ultimas-noticias-1/plano-brasileiro-de-inteligencia-artificial-pbia-2024-2028>>. acesso em: 7 maio 2025.



que não são apenas técnicos, mas também jurídicos, econômicos e políticos. O CGI.br possui legitimidade institucional e acúmulo histórico em governança da internet, o que lhe permite formar pontes entre comunidades técnicas brasileiras e processos globais de padronização, sobretudo no IETF e no W3C, onde sua atuação já é reconhecida.

O CGI.br pode desempenhar papel ainda mais estruturante ao criar mecanismos permanentes de interlocução entre Ministérios afetos ao tema da padronização, Itamaraty, agências reguladoras, academia e setor produtivo, identificando temas prioritários e articulando posições nacionais consistentes para organismos como ISO, IEC, IEEE e ITU-T. Além disso, pode apoiar financeiramente a participação de pesquisadores e especialistas brasileiros em reuniões internacionais, promover grupos de trabalho nacionais sobre padrões estratégicos e organizar processos públicos de consulta e consolidação de entendimento técnico.

Assim, a coordenação da participação nacional em fóruns de padronização técnica reforça a capacidade do Brasil de influenciar a definição de protocolos que moldam as camadas da pilha digital, reduz assimetrias com países tecnologicamente mais robustos e garante que o país participe de forma ativa e qualificada da governança digital global.



9 Caminhos para Implementação

A implementação de uma abordagem nacional de soberania digital exige não apenas formulação estratégica e definição programática, mas também mecanismos operacionais, métricas confiáveis, cronogramas realistas e estratégias de mitigação de riscos. As experiências internacionais mencionadas a título exemplificativo no capítulo 4 demonstram que o sucesso de políticas tecnológicas depende de instrumentos institucionais e cooperação multissetorial capazes de transformar diretrizes abstratas em ações concretas, contínuas e verificáveis. Nesta perspectiva, pode-se argumentar que o Brasil já acumulou diagnósticos e debates suficientes: o principal desafio, neste momento, situa-se na capacidade de execução e de coordenação.

O presente bloco apresenta quatro diretrizes essenciais para transformar a agenda de soberania digital em prática: *i)* a definição de prioridades e métricas voltadas a medir como e quando tais prioridades seja alcançada; *ii)* o sequenciamento estratégico de políticas e investimentos; *iii)* a identificação de riscos; e, *iv)* a construção de mecanismos permanentes de monitoramento e mitigação de riscos. Trata-se, portanto, de uma agenda orientada não apenas ao planejamento, mas sobretudo à governança e *accountability*.

9.1 Priorização estratégica e métricas de impacto

A implementação efetiva de uma política nacional para soberania digital requer definição clara de prioridades, alinhada a indicadores claramente verificáveis e auditáveis. A ausência de métricas pode transformar a política em conjunto disperso de aspirações e iniciativas desconexas, sem capacidade de orientar concretamente investimentos, corrigir desvios ou avaliar resultados. Neste sentido, a identificação de prioridades deve considerar cinco dimensões: infraestrutura computacional e de conectividade, dados, modelos e software, aplicações estratégicas e formação de pessoas e governança. Essas dimensões refletem as camadas identificadas no capítulo 5 e as priorizam, com base no diagnóstico efetuado no capítulo 3 e nas análises compartilhadas ao longo do Seminário Nacional “Pilha de IA: Desafios para Autonomia Tecnológica e Soberania Digital”¹³⁰.

O primeiro passo é definir quais infraestruturas são consideradas estratégicas e qual sua participação relativa na política de soberania digital. Métricas como capacidade computacional instalada, crescimento anual da infraestrutura pública, número de clusters de GPU operando sob jurisdição brasileira e percentual de projetos estratégicos atendidos pela infraestrutura nacional podem orientar a evolução dessa política. No que diz respeito à conectividade, devem-se considerar métricas que avaliem não apenas a expansão quantitativa das redes – como densidade de cobertura 5G, penetração de fibra óptica ou disponibilidade de *backhaul* – mas, sobretudo, indicadores qualitativos de conectividade significativa (medidos por

¹³⁰ Relatório Seminário Pilha IA Soberana.



parâmetros como velocidade sustentada, estabilidade, latência, existência e volume de franquias de dados e ausência de práticas discriminatórias como o *zero rating*¹³¹) e de participação de produtos e serviços nacionais na cesta de consumo digital significativa. Somente métricas que captem essas dimensões qualitativas permitirão identificar gargalos reais de acesso, orientar investimentos públicos e garantir que a infraestrutura nacional suporte, de forma plena e equitativa, o desenvolvimento e uso de tecnologias digitais avançadas.

Para dados, as métricas devem incluir volume de bases públicas estruturadas, número de bolsas de dados (ou seja, plataformas interoperáveis) estabelecidas, a qualidade dos metadados e a quantidade de acordos de compartilhamento celebrados. Para modelos e software, as métricas devem incluir o número de modelos pré-treinados nacionais, a diversidade linguística e cultural dos *datasets*, a realização de auditorias independentes, o número de bibliotecas abertas desenvolvidas por instituições nacionais, número de projetos de *open source* iniciados e mantidos de forma contínua, e o grau de dependência de *frameworks* estrangeiros. Para aplicações estratégicas, métricas devem refletir adoção de IA em setores críticos, impacto socioeconômico, redução de custos operacionais e eficiência de serviços públicos. Finalmente, para formação profissional, métricas devem acompanhar o número de cursos técnicos, mestrados profissionais, redes de capacitação contínua e participação de regiões historicamente sub-representadas, especialmente Norte e Nordeste.

A definição dessas métricas exige uma abordagem jurídico-institucional clara, que preveja a responsabilidade de cada órgão na produção e validação dos dados necessários. Recomenda-se que o CITDigital, MCTI, CGEE e o CGI.br e, quando for criado, o SINIA e o Sistema Nacional para Desenvolvimento, Regulação e Governança de Inteligência Artificial sejam encarregados de organizar a consolidação anual desses indicadores, permitindo o acompanhamento público da evolução da política e a correção tempestiva de desvios.

9.2 Sequenciamento de políticas e investimentos por meio de alianças setoriais

Não parece possível que a implementação de uma abordagem abrangente de soberania digital possa ocorrer de forma dispersa ou simultânea em todas as frentes. Portanto, é necessário estabelecer sequenciamento estratégico, priorizando ações e alianças estratégicas setoriais que criem o alicerce necessário para as etapas subsequentes. O sequenciamento proposto deve ser implementado no âmbito de alianças estratégicas setoriais, capitalizando ativos já consolidados em setores críticos como petróleo e gás, agroindústria, saúde, finanças e defesa, mediante coordenação federativa que integre infraestrutura existente, competências institucionais e demandas específicas de cada domínio. Considerando-se que infraestrutura e dados constituem os alicerces sobre os quais modelos, softwares e aplicações se

¹³¹ NIC.BR, Conectividade significativa: propostas para medição e o retrato da população no Brasil.



desenvolvem, o primeiro bloco de implementação deve concentrar investimentos prioritariamente nesses elementos estruturantes.

O sequenciamento proposto pode ser dividido em três fases complementares. Na fase inicial, ou fundacional, a prioridade deve ser garantir a disponibilidade de infraestrutura robusta e reconfigurar os PRODEs e centros do SINAPAD em operadores federados da computação pública. Paralelamente, devem ser criados padrões unificados de compartilhamento e governança de dados, estabelecendo desde o início requisitos de segurança, auditoria e soberania jurisdicional. Nesta etapa, as alianças setoriais devem mapear infraestruturas existentes, como os supercomputadores financiados pela Petrobras no Rio de Janeiro ou sistemas em instituições de saúde, e integrá-las à arquitetura federada nacional.

Na fase intermediária, o foco deve ser o desenvolvimento da camada lógica: frameworks, bibliotecas, MLOps, modelos pré-treinados nacionais e ferramentas abertas. Essa fase exige coordenação estreita entre universidades, centros de supercomputação, centros de pesquisa setoriais (como CENPES, Fiocruz e instituições financeiras públicas) e empresas, bem como mecanismos de fomento contínuo. Encomendas tecnológicas devem priorizar modelos abertos treinados em infraestrutura pública, com dados setoriais curados, assegurando transparência, auditabilidade e adequação às especificidades de cada domínio estratégico.

Na fase final, ou de consolidação, devem ser priorizadas aplicações setoriais e integração com cadeias produtivas estratégicas. É nesse momento que setores estratégicos devem receber incentivos específicos para adoção de IA soberana, com suporte técnico especializado, financiamento direcionado e integração com modelos e dados nacionais desenvolvidos nas fases anteriores. As alianças setoriais atuam como vetores de difusão tecnológica, garantindo que soluções desenvolvidas em infraestrutura pública sejam efetivamente incorporadas aos processos produtivos e operacionais. A consolidação exige ainda mecanismos permanentes de avaliação de impacto, conformidade regulatória, segurança cibernética, e atualização tecnológica contínua, assegurando sustentabilidade e relevância de longo prazo do ecossistema nacional de IA.

Esse sequenciamento garante que políticas e investimentos não se sobreponham de forma incoerente e que todas as camadas da pilha se desenvolvam de maneira ordenada e eficiente.

9.3 Riscos, obstáculos e mitigação

A implementação de uma política nacional soberana envolve riscos técnicos, jurídicos, econômicos, operacionais e geopolíticos. Identificar esses riscos e estabelecer mecanismos de mitigação é fundamental para evitar interrupções de política pública, desperdício de recursos e dependências tecnológicas involuntárias.

O primeiro risco é a exacerbação do *lock-in* devido à dependência persistente de fornecedores estrangeiros em camadas críticas da pilha, especialmente no nível de hardware, serviços de nuvem, e bibliotecas básicas. A mitigação exige políticas de substituição gradual, incentivos



para produção local, adoção de padrões abertos e contratação pública com cláusulas de soberania.

O segundo risco é a fragmentação federativa e institucional. O Brasil possui múltiplos órgãos com competências sobre tecnologia, proteção de dados, inovação e cibersegurança – área na qual as consequências nefastas deste risco são particularmente evidentes¹³². A ausência de coordenação pode gerar iniciativas duplicadas, incoerentes e conflitantes, determinando vulnerabilidades sistêmicas. O CITDigital – eventualmente junto ao Sistema Nacional para Desenvolvimento, Regulação e Governança de Inteligência Artificial, quando for estabelecido – poderia assumir o papel de coordenador técnico e político, articulando a definição de instrumentos jurídicos claros para harmonização de políticas.

O terceiro risco é a falta de sustentabilidade financeira. Infraestruturas de IA exigem recursos públicos contínuos, e o modelo atual de financiamento é instável e dependente de ciclos políticos. A mitigação passa pela criação de fundos específicos, linhas de crédito dedicadas, mecanismos de parceria público-privada e modelos de autossustentação baseados em prestação de serviços por centros de computação pública.

O quarto risco é o déficit de capacitação técnica. Sem profissionais especializados, centros de supercomputação, computação quântica e plataformas de IA não conseguem operar plenamente. Apesar do Brasil ser um produtor de talento, capacidade altamente especializadas são necessárias para operar certos tipos de componentes infraestruturais, como engenheiros de HPC/IA, administradores de clusters GPU e especialistas em operações de data centers de alto desempenho. A mitigação depende de políticas educacionais, formação profissional contínua e incentivos para fixação de talentos em instituições públicas e regiões menos favorecidas.

O quinto risco é o da baixa reprodutibilidade científica. A atual falta de padronização técnica nacional dificulta replicação e validação de experimentos. A mitigação exige estratégias e ferramentas nacionais de reprodutibilidade, padrões de versionamento e documentação obrigatória para projetos financiados com recursos públicos.

Por fim, há riscos políticos, geopolíticos e de segurança cibernética. A proibição do *zero rating* seja talvez o melhor exemplo dos riscos políticos e geopolíticos que as dependências determinam. Embora proibir o *zero rating* seja instrumental para garantir que a inovação nacional possa competir em condições equitativas e ser amplamente distribuída – como demonstra a experiência indiana – tal proibição envolve custos políticos e geopolíticos significativos. A forte dependência brasileira de plataformas patrocinadas, em especial das redes sociais do grupo Meta, cria um cenário em que qualquer medida que elimine benefícios artificiais a essas aplicações tende a enfrentar resistência intensa. Governos que busquem proibir o *zero rating* de redes sociais poderão ser rapidamente alvo de críticas de atores

¹³² BELLI, Luca; MEDEIROS, Breno Pauli; COUTO, Natália. **Governança da cibersegurança no Brasil: entender o passado, esclarecer o presente e construir o futuro**, Disponível em: <<https://cyberbrics.info/wp-content/uploads/2024/06/PP-CTS-FGV-Ciberseguranca.pdf>>. Acesso em: 3 dez. 2024.



políticos domésticos e de pressões internacionais, incluindo potenciais reações negativas da administração norte-americana. Essa dinâmica ilustra que medidas necessárias para a soberania digital frequentemente desafiam estruturas de poder consolidadas e exigem coordenação diplomática, comunicação pública clara e resiliência institucional.

Por fim, a dependência de hardware estrangeiro pode expor o país a vulnerabilidades, interrupções de fornecimento e espionagem. A mitigação exige certificação nacional de hardware, inspeção técnica e desenvolvimento gradual de cadeias produtivas locais, com foco em tecnologias abertas como RISC-V.

9.4 Conjunto de indicadores e monitoramento

A implementação da política de soberania digital deve ser acompanhada por mecanismos permanentes de monitoramento, para favorecer transparência e *accountability*. Propõe-se a criação de um Conjunto de Indicadores de Soberania Digital¹³³, voltado a permitir a coleta, análise e publicação periódica de informações sobre desenvolvimento, dependências e vulnerabilidades de infraestruturas, bases e plataformas de dados, modelos e software, e formação profissional. Tal Conjunto desempenharia um valor complementar ao *Framework* Brasileiro de Soberania Digital, apresentado na seção 6.4: enquanto o conjunto permitiria a avaliação de nível de desenvolvimento, dependências e vulnerabilidades, o *Framework* definiria os critérios e controles que devem ser aplicados.

Portanto, desenvolvimento, dependência e vulnerabilidade deveriam ser considerados como as dimensões complementares nas quais devem ser organizados indicadores claros. Na dimensão do desenvolvimento, os indicadores devem capturar a capacidade nacional de produzir, manter e evoluir tecnologias críticas. Isso inclui métricas como capacidade computacional pública instalada, *uptime* e eficiência energética de centros de supercomputação, latência e desempenho das redes acadêmicas, grau de interoperabilidade de bases de dados públicas, diversidade e atualização das fontes de dados, número de modelos abertos produzidos no país, volume de aplicações estratégicas desenvolvidas localmente e oferta qualificada de profissionais de IA distribuída de forma equilibrada regionalmente.

Na dimensão da dependência, os indicadores devem medir o grau de exposição do país a tecnologias, plataformas e infraestruturas estrangeiras. Exemplos incluem percentual de dados governamentais armazenados fora da jurisdição nacional, grau de dependência de nuvens públicas comerciais, proporção de softwares proprietários utilizados na administração pública, participação de plataformas estrangeiras no tráfego nacional, peso de modelos de IA

¹³³ Como indicado na seção 10.1, recomenda-se que os Indicadores de Soberania Digital sejam desenvolvidos por meio de estudos futuros específicos e complementares a este texto para discussão. Embora já existam exemplos dispersos de métricas voltadas a infraestrutura, dados, modelos e capacitação, nenhum esforço atual adotou uma abordagem verdadeiramente abrangente, integrada e apta a refletir a complexidade multidimensional da soberania digital. Veja-se por exemplo: <https://digitaldependence.eu/en/>



fechados em aplicações críticas e dependência de fornecedores externos para manutenção, suporte e auditoria de sistemas essenciais.

Por fim, a dimensão da vulnerabilidade deve avaliar riscos estruturais associados a essas dependências, bem como fragilidades internas. Indicadores relevantes incluem exposição a pontos únicos de falha, exposição a *enforcement* abusivo de propriedade intelectual em tecnologia proprietária, frequência e severidade de incidentes de segurança, grau de resiliência cibernética de infraestruturas críticas, distribuição de clusters computacionais, capacidade de resposta a interrupções ou sanções internacionais e concentração de dados sensíveis em arquiteturas centralizadas. Somadas, essas três dimensões permitem diagnosticar não apenas o nível de maturidade tecnológica do país, mas sobretudo sua autonomia efetiva e sua capacidade de resistir a choques externos ou a manipulações decorrentes da interdependência assimétrica.

O MCTI deve exercer papel central na coordenação e facilitação do monitoramento periódico – trimestral ou semestral – do Conjunto de Indicadores de Soberania Digital. A implementação de tal monitoramento deve envolver, idealmente, a participação de múltiplos atores e auditorias independentes, assegurando transparência e controle social. Universidades, centros de pesquisa, empresas e sociedade civil devem ter acesso aos dados, propondo melhorias e pressionando por correções de rota. Esse processo confere legitimidade à política pública, reduz riscos de captura e promove alinhamento entre atores diversos.

Por fim, recomenda-se que relatórios anuais com base no Conjunto de Indicadores de Soberania Digital sejam atualizados periodicamente e que os próprios indicadores sejam revisados periodicamente, permitindo ajustes dinâmicos às mudanças tecnológicas, econômicas, regulatórias e geopolíticas.



10 Conclusões

Este texto ressalta que a consolidação da soberania digital brasileira constitui um desafio jurídico, tecnológico e institucional de grande complexidade, que exige visão estratégica de longo prazo, capacidade de coordenação intergovernamental e compromisso com o desenvolvimento científico e industrial do país. O conjunto de análises desenvolvidas ao longo deste trabalho demonstra que soberania digital não é um estado fixo a ser alcançado, mas um processo contínuo, dinâmico e multifacetado. Trata-se de capacidade estratégica de um Estado de definir, controlar e operacionalizar suas políticas públicas, sua infraestrutura crítica, seus sistemas informacionais e seus modelos de inteligência artificial sem dependência insustentável de atores estrangeiros, sejam eles empresas, governos ou plataformas globais.

O diagnóstico apresentado indica que o Brasil dispõe de importantes ativos institucionais, humanos e científicos: uma base legislativa avançada em matéria de proteção de dados, um ecossistema acadêmico competitivo internacionalmente, centros de supercomputação em expansão, setores estratégico com grande potencial de crescimento digital, capacidade industrial potencialmente reativável na área eletrônica e experiência acumulada em definição e implementação de políticas industriais complexas, como energia e saúde. No entanto, esses ativos coexistem com vulnerabilidades persistentes: dependência quase total de *hardware* (e *software*) estrangeiro, déficit em bibliotecas de *software* e modelos nacionais, ausência de plataformas federadas de dados, fragmentação institucional, insuficiência de financiamento contínuo, disparidades regionais em formação de pessoal e baixa adoção de cultura tecnológica soberana por órgãos públicos.

A comparação internacional deixa claro que não existe um único modelo de soberania digital. A abordagem estadunidense demonstra a força de políticas de demanda, nas quais o Estado atua como cliente âncora e orienta a indústria local por meio de compras públicas estratégicas. A abordagem chinesa evidencia os efeitos de políticas industriais integradas, combinando infraestrutura, regulação, estímulos econômicos e apoio estatal direto ao desenvolvimento de *hardware* e *software* nacionais. A abordagem europeia mostra a necessidade, porém insuficiência de arcabouços regulatórios e mecanismos de governança coerentes. A experiência do Uruguai, da China e, mais recentemente da Suíça e da Finlândia, demonstram o enorme potencial do *open source*, inclusive para países de tamanho reduzido. A experiência do México demonstra que o valor do retorno no investimento computacional depende, em larga medida, do pensamento ecossistêmico que acompanha tal investimento, mais do que o tamanho do investimento mesmo. Cada uma dessas abordagens oferece elementos úteis para o Brasil, mas nenhuma delas pode ser transplantada integralmente; o país deve construir sua própria estratégia, adaptada às condições locais.

Com base nesse diagnóstico, o texto para discussão apresentou recomendações estruturadas em múltiplos eixos. Em primeiro lugar, ajustes regulatórios são essenciais para harmonizar o conjunto disperso de normas existentes e estabelecer um marco claro para infraestrutura



crítica, dados sensíveis, modelos de alto risco e plataformas públicas de IA. A criação de padrões específicos para facilitar compartilhamento de dados e modelos, acompanhada de mecanismos de auditoria e transparência, pode estimular a cooperação e reduzir vulnerabilidades. Em segundo lugar, é indispensável consolidar uma governança multissetorial, capaz de integrar ministérios, agências reguladoras, universidades, centros de pesquisa, empresas e sociedade civil em um arranjo estável e eficiente. O CIT Digital – junto com o Sistema Nacional para Desenvolvimento, Regulação e Governança de Inteligência Artificial, se e quando for criado – pode assumir papel central nessa coordenação, articulando câmaras técnicas e assegurando alinhamento entre políticas públicas, pesquisas e demandas industriais.

Em terceiro lugar, as compras públicas precisam ser mobilizadas como instrumento de política industrial. A legislação brasileira oferece múltiplos instrumentos para isso, como margens de preferência, encomendas tecnológicas, contratação integrada e regimes diferenciados de contratação, mas sua aplicação às áreas de IA ainda é precária. O Estado deve utilizar sua capacidade de compra para orientar a indústria nacional, incentivar software aberto, exigir transparência e auditabilidade e priorizar infraestruturas e modelos operados sob jurisdição brasileira. Em quarto lugar, é necessária a criação de um Conjunto de Indicadores de Soberania Digital bem como de um Framework de compliance, inspirado no modelo europeu do Cloud Sovereignty Framework, mas ajustado ao ordenamento jurídico nacional. O Conjunto permitiria a avaliação de nível de desenvolvimento, dependências e vulnerabilidades, enquanto o Framework deve estabelecer requisitos legais, técnicos, operacionais e de governança para certificação de serviços em nuvem, modelos de IA e infraestruturas críticas.

No âmbito da política de desenvolvimento tecnológico e produtivo, este texto para discussão destacou que a soberania lógica é tão importante quanto a soberania infraestrutural. O Brasil deve investir em desenvolvimento de modelos abertos, bibliotecas e frameworks nacionais, ferramentas de MLOps e algoritmos adaptados a necessidades locais. A produção de modelos nacionais pré-treinados, especialmente multilíngues e multiculturais, é fundamental para autonomia e inclusão. O país também deve fortalecer sua capacidade em hardware, participando de cadeias globais de semicondutores e ampliando sua inserção no ecossistema RISC-V. A política industrial deve ainda integrar setores estratégicos, como saúde, energia, petróleo e gás, defesa, finanças e agroindústria, que podem atuar como âncoras e contribuir para sustentabilidade financeira e tecnológica do ecossistema.

A construção de um ecossistema digital nacional tecnologicamente autônomo requer, ainda, plataformas integradas de dados, centros de excelência e redes de pesquisa interinstitucionais. Plataformas de intercâmbio de dados sob governança federada, organizadas no âmbito de uma Rede Nacional de Dados e coordenadas pelo CIT Digital, podem promover acesso seguro e eficiente a bases públicas e privadas. Centros de supercomputação integrados em rede, com serviços padronizados e ambientes pré-configurados, podem reduzir barreiras de entrada e democratizar acesso à infraestrutura. Redes de pesquisa distribuídas,



envolvendo universidades e empresas, podem garantir produção científica de excelência, reprodutibilidade e transferência tecnológica.

A execução dessas políticas depende de mecanismos permanentes de financiamento, sequenciamento estratégico e sistemas de monitoramento. A criação de fundos temáticos, linhas especiais de crédito, fundos de venture público-privado e modelos de autossustentação para centros de supercomputação são essenciais para garantir continuidade. O sequenciamento proposto divide a implementação em fases fundacionais, intermediárias e de consolidação, permitindo que infraestrutura, dados, modelos e aplicações se desenvolvam de forma coerente. O Conjunto de Indicadores de Soberania Digital e seu monitoramento, devem permitir avaliação contínua de desempenho, identificação de gargalos e ajustes dinâmicos conforme evolução tecnológica e institucional.

Em síntese, a soberania digital brasileira dependerá da capacidade do Estado e da sociedade de organizar recursos, pessoas e instituições para construção de um ecossistema tecnológico integrado, seguro, inclusivo e competitivo. Não se trata de isolamento tecnológico, mas de autonomia estratégica: capacidade de escolher, produzir, auditar, governar e adaptar tecnologias essenciais ao interesse público e ao desenvolvimento nacional. O Brasil tem potencial para consolidar uma agenda própria de IA soberana, desde que políticas públicas, instituições científicas, setor produtivo e sociedade trabalhem de maneira coordenada, contínua e orientada à construção de capacidades nacionais.

A estratégia aqui delineada oferece um caminho estruturalmente viável para esse objetivo, articulando regulação, governança, política industrial, infraestrutura e ciência aberta em um modelo coerente e alinhado com os desafios contemporâneos de autonomia tecnológica. A próxima e última seção deste texto, expõe recomendações finais para estudos futuros, voltadas ao desenvolvimento de métricas nacionais de soberania digital, ao aprimoramento de modelos de governança e ao mapeamento sistemático das arenas internacionais onde se decide o futuro tecnológico global.

10.1 Recomendações para estudos futuros

Além das ações imediatas, é essencial investir em estudos estruturantes que orientarão políticas públicas de médio e longo prazo. Um dos temas prioritários é o desenvolvimento de indicadores e métricas para avaliar a soberania digital. A literatura evidencia que não existe indicador único capaz de capturar dimensões como autonomia informacional, controle sobre infraestrutura crítica, resiliência cibernética, capacidade industrial, dependência de fornecedores estrangeiros e governança algorítmica. Portanto, parece urgente que seja desenvolvido um Conjunto de Indicadores de Soberania Digital voltado a avaliar o nível de desenvolvimento, dependência e vulnerabilidade tecnológica.

Outro eixo de estudo futuro diz respeito à análise comparada de modelos de governança de soberania digital. Países como Estados Unidos, China, Índia, Suíça, Finlândia, México e Uruguai oferecem estratégias e arranjos institucionais radicalmente distintos que combinam Estado,



mercado, comunidade técnica e academia em graus variáveis. A compreensão aprofundada dessas estruturas, de seus mecanismos decisórios e de seus instrumentos de coordenação e como eles garantem estabilidade pode orientar o desenho de uma governança brasileira mais eficaz, que preserve direitos, incentive inovação e reduza dependências sistêmicas.

Também se recomenda o mapeamento abrangente dos fóruns internacionais relevantes para cada camada da pilha digital: organismos de padronização como ISO, IEEE, ITU-T, IETF e W3C; fóruns normativos e multilaterais como as agências da ONU, e arranjos plurilaterais como BRICS, Mercosul, e G20 e parcerias estratégicas bilaterais. Esse mapeamento deve incluir análise de agendas, atores dominantes, processos decisórios, oportunidades para influência brasileira e estratégias de participação efetiva, articuladas pelo Itamaraty, especialmente pelo Escritório do Embaixador de Tecnologia.

Em conjunto, esses estudos fornecerão a base intelectual, empírica e institucional para uma política nacional de soberania digital robusta, capaz de orientar investimentos, regular tecnologias críticas, fortalecer o ecossistema científico e industrial e assegurar que o Brasil exerça controle legítimo e democrático sobre as infraestruturas que sustentam seu futuro tecnológico.



Referências Bibliográficas

ARCESATI, Alex He, 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: 13 nov. 2025.

ARCESATI, Rebecca; MEINHARDT, Caroline. China's Open-Source Tech Development.

ASSOCIAÇÃO BRASILEIRA DAS EMPRESAS DE SOFTWARE. **Mercado Brasileiro De Software: Panorama E Tendências 2008**. [s.l.]: Abes, 2024.

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>>.

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. Compras Públicas como Alavanca da Soberania Digital. Câmara Técnica de Economia Digital (CTED) do CITDigital. 2025.

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

BELLI, Luca. **Community Networks: Building Digital Sovereignty and Environmental Sustainability**. Rio de Janeiro, RJ: Publicações Direito Rio, 2023.

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. 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; 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. 23, n. 52, 2025.

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; GASPAR, Walter B. *The Quest for AI Sovereignty, Transparency and Accountability.* 2023.

BELLI, Luca; GASPAR, Walter B; COUTO, Natalia; *et al.* **Soberania Digital e Inteligência Artificial no Brasil: rumo à autonomia tecnológica.** RIO DE JANEIRO, RJ: Lumen Juris, 2026.

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 B.; KREMER, Bianca; *et al.* **Redes sociais e LGPD.** [s.l.: s.n.], 2025. Disponível em: <<https://hdl.handle.net/10438/37854>>. Acesso em: 10 dez. 2025.

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. **L'État digital: numérisation de l'administration publique et administration publique du numérique.** Boulogne-Billancourt: Berger-Levrault, 2022. (Au fil du débat).

BELLI, Luca; JIANG, Min. **Digital Sovereignty in the BRICS Countries: How the Global South and Emerging Power Alliances Are Reshaping Digital Governance.** Cambridge University Press; 2025. 2024.

BELLI, Luca; MEDEIROS, Breno Pauli; COUTO, Natália. **Governança da cibersegurança no Brasil: entender o passado, esclarecer o presente e construir o futuro,** Disponível em: <<https://cyberbrics.info/wp-content/uploads/2024/06/PP-CTS-FGV-Ciberseguranca.pdf>>. Acesso em: 3 dez. 2024.

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.** Rio de Janeiro, RJ: Editora Lumen Juris, 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; ZINGALES, Nicolo; BAKONYI, Erica. **LGPD: lei que pega ou lei que não pega?** JOTA Jornalismo. Disponível em: <<https://www.jota.info/opiniao-e-analise/colunas/direitos-tecnologias/lgpd-lei-que-pegou-lei-que-nao-pegou>>. Acesso em: 9 dez. 2025.

BRATTON, Benjamin H. **The stack: on software and sovereignty.** Cambridge, Mass. London: MIT press, 2015. (Software studies).

BRASIL. Ministério da Ciência, Tecnologia e Inovação. *Programas estruturantes e mobilizadores.* Disponível em: <https://www.gov.br/mcti/pt-br/acompanhe-o->



[mcti/fndct/paginas/planejamento/programas-estruturantes-e-mobilizadores/programas-estruturantes-e-mobilizadores](https://mcti.fndct/paginas/planejamento/programas-estruturantes-e-mobilizadores/programas-estruturantes-e-mobilizadores). Acesso em: 4 jan. 2026.

BRIA, Francesca; TIMMERS, Paul; GERNONE, Fausto. EuroStack – **A European Alternative for Digital Sovereignty**. p. 127 p., 2025.

CALCATERRA, Craig; KAAL, Wulf A. **Decentralized Governance**. 2021. Disponível em: <<https://papers.ssrn.com/abstract=3782214>>. Acesso em: 11 dez. 2025.

CHANDER, Anupam. Facebookistan. **North Carolina Law Review**, v. 90, n. 5, p. 1807, 2012.

COULDRY, Nick; MEJIAS, Ulises A. **Data colonialism: rethinking big data's relation to the contemporary subject**. 2018. Disponível em: <https://eprints.lse.ac.uk/89511/1/Couldry_Data-colonialism_Accepted.pdf>.

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.

COVERI, Andrea; COZZA, Claudio; GUARASCIO, Dario. **Big Tech and the US Digital-Military-Industrial Complex**. Disponível em: <<https://www.intereconomics.eu/contents/year/2025/number/2/article/big-tech-and-the-us-digital-military-industrial-complex.html>>. Acesso em: 5 jan. 2026.

DATAETHICS. **Finland Wins On Digital Sovereignty In New Index** · Dataetisk Tænkehandletank. Disponível em: <<https://dataethics.eu/finland-wins-on-digital-sovereignty-in-new-index/>>. Acesso em: 10 dez. 2025.

DRAGHI, Mario. The future of European competitiveness: Part A: a competitiveness strategy for Europe. Luxembourg: Publications Office of the European Union, 2025.
DRAPER, Hannah; BELL, Luca; MEIRA, Marina; *et al.* **A Consumer-centric Approach to DPIs for sustainable financial inclusion**. Brasil: T20 Brasil 2024, 2024. (Inclusive Digital Transformation).

EM 10/06/2025 19H49, Publicado em 10/06/2025 17h18 Atualizado. **Gestão, Serpro e Dataprev lançam serviços de nuvem de governo para órgãos federais**. Ministério da Gestão e da Inovação em Serviços Públicos. Disponível em: <<https://www.gov.br/gestao/pt-br/assuntos/noticias/2025/maio/gestao-serpro-e-dataprev-lancam-servicos-de-nuvem-de-governo-para-orgaos-federais>>. Acesso em: 4 jan. 2026.

EM 12/03/2024 14H35, Publicado. **Brasil se torna membro da Aliança RISC-V International**. Ministério da Ciência, Tecnologia e Inovação. Disponível em: <<https://www.gov.br/mcti/pt-br/acompanhe-o-mcti/noticias/2024/03/brasil-se-torna-membro-da-alianca-risc-v-international>>. Acesso em: 5 jan. 2026.

EM 18/12/2025 08H09, Publicado. **Participe da Consulta Pública da Estratégia Nacional de Ciência, Tecnologia e Inovação (ENCTI) 2024-2034**. Centro Brasileiro de Pesquisas Físicas -



CBPF. Disponível em: <<https://www.gov.br/cbpf/pt-br/assuntos/noticias/participe-da-consulta-publica-da-estrategia-nacional-de-ciencia-tecnologia-e-inovacao-entci-2024-2034>>. Acesso em: 4 jan. 2026.

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.

FARRELL, Henry; NEWMAN, Abraham L. Weaponized Interdependence: How Global Economic Networks Shape State Coercion. **International Security**, v. 44, n. 1, p. 42–79, 2019.

FLORIDI, Luciano. The Fight for Digital Sovereignty: What It Is, and Why It Matters, Especially for the EU. **Philosophy & Technology**, v. 33, n. 3, p. 369–378, 2020.

GOMES, Ana Bárbara; DUARTE, Felipe; ROCILLO, Paloma. **Inclusión digital como política pública Brasil y América del Sur en perspectiva**. [s.l.]: IRIS, [s.d.]. Disponível em: <<https://irisbh.com.br/wp-content/uploads/2020/05/Inclusion-digital-como-politica-publica-IRIS.pdf>>. GONZÁLEZ, Fernanda. **Coatlicue, así es la supercomputadora que convertirá a México en líder de procesamiento de datos en LATAM**. WIRED. Disponível em: <<https://es.wired.com/articulos/coatlicue-asi-es-la-supercomputadora-que-convertira-a-mexico-en-lider-de-procesamiento-de-datos-en-latam>>. Acesso em: 10 dez. 2025.

GU, Hongfei. Data, Big Tech, and the New Concept of Sovereignty. **Journal of Chinese Political Science**, v. 29, n. 4, p. 591–612, 2024.

IBRAHIM, Sara. Fact and fiction about the Swiss AI model Apertus. Disponível em: <<https://www.swissinfo.ch/eng/swiss-ai/fact-and-fiction-about-the-swiss-ai-model-apertus/90110034>>. Acesso em: 4 jan. 2026.

INTERNATIONAL, Cullen. **[INFOGRAPHIC] Top 10 European antitrust fines on Big Tech**. Disponível em: <<https://www.cullen-international.com/news/2025/09/-INFOGRAPHIC--Top-10-European-antitrust-fines-on-Big-Tech.html>>. Acesso em: 11 dez. 2025.

JIANG, Min; BELL, 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.

KAK, Amba; MYERS WEST, Sarah; WHITTAKER, Meredith. **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: 10 dez. 2025.

KOCHER, Paul; GENKIN, Daniel; GRUSS, Daniel; *et al.* Spectre Attacks: Exploiting Speculative Execution. 2018. Disponível em: <<http://arxiv.org/abs/1801.01203>>. Acesso em: 11 dez. 2025.

KUMAR, Purushottam; KUMAR, Dr Prakash. Vendor Lock-In Situation and Threats in Cloud Computing. v. 7, n. 9, 2022.

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.

LIANOS, Ioannis; IVANOV, Alexey. Digital Era Competition BRICS Report. 2019. Disponível em: <<https://papers.ssrn.com/abstract=3901413>>. Acesso em: 5 dez. 2025.

LU, Julia. Data exchanges in China, explained · TechNode. Disponível em: <<https://technode.com/2021/08/17/chinas-data-exchanges-explained/>>. Acesso em: 5 dez. 2025.

MACKINNON, Rebecca. **Consent of the Networked: The Worldwide Struggle For Internet Freedom**. USA: Basic Books, Inc., 2012.

MCMAHON, M. *et al.* (2021), “Scale, market power and competition in a digital world: Is bigger better?”, *OECD Science, Technology and Industry Working Papers*, No. 2021/01, OECD Publishing, Paris;

MALLIK, Amitav. **Technology and security in the 21st century: a demand-side perspective**. Oxford: Oxford Univ. Press, 2005. (SIPRI research report, 20).

MAZZUCATO, Mariana. Mission-oriented innovation policies: challenges and opportunities. **Industrial and Corporate Change**, v. 27, n. 5, p. 803–815, 2018.

MAZZUCATO, Mariana; PENNA, Caetano C. R. **Mission-Oriented Finance for Innovation: New Ideas for Investment-Led Growth**. [s.l.]: Bloomsbury Publishing PLC, 2015.

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.

MERA, Alejandro; FENG, Bo; LU, Long; *et al.* DICE: Automatic Emulation of DMA Input Channels for Dynamic Firmware Analysis. 2021. Disponível em: <<http://arxiv.org/abs/2007.01502>>. Acesso em: 11 dez. 2025.

MINISTÉRIO DA CIÊNCIA, TECNOLOGIA E INOVAÇÕES. **Plano Brasileiro de Inteligência Artificial (PBIA) 2024-2028**. Laboratório Nacional de Computação Científica - LNCC.



Disponível em: <<https://www.gov.br/lncc/pt-br/assuntos/noticias/ultimas-noticias-1/plano-brasileiro-de-inteligencia-artificial-pbia-2024-2028>>. Acesso em: 7 maio 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.

NACIONAL, Imprensa. **DESPACHO DO PRESIDENTE DA REPÚBLICA - DOU - Imprensa Nacional**. Disponível em: <<https://www.in.gov.br/en/web/dou/-/despacho-do-presidente-da-republica-673947267>>. Acesso em: 10 dez. 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.

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.

PARSHEERA, Smriti. Net neutrality in India: From rules to enforcement. *In*: BELL, 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.

POHLE, Julia; THIEL, Thorsten. **Digital sovereignty**. Disponível em: <<https://policyreview.info/concepts/digital-sovereignty>>. Acesso em: 11 mar. 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>>.

REPÚBLICA, Presidencia de la. **Presidenta Claudia Sheinbaum presenta “Coatlicue”, la supercomputadora del pueblo de México y la más poderosa de América Latina**. gob.mx. Disponível em: <<http://www.gob.mx/presidencia/prensa/presidenta-claudia-sheinbaum-presenta-coatlicue-la-supercomputadora-del-pueblo-de-mexico-y-la-mas-poderosa-de-america-latina>>. Acesso em: 10 dez. 2025.

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.

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.

UNIÃO, Tribunal de Contas da. **Auditoria aponta falhas na aplicação da LGPD por organizações federais – Notícias**. Portal TCU. Disponível em: <<https://portal.tcu.gov.br/imprensa/noticias/auditoria-aponta-falhas-na-aplicacao-da-lgpd-por-organizacoes-federais>>. Acesso em: 11 dez. 2025.

UNITED STATES OF AMERICA. **Foreign Intelligence Surveillance Act**. Disponível em: <<https://www.intel.gov/foreign-intelligence-surveillance-act>>. Acesso em: 11 dez. 2025.

URUGUAY. **Information and Communication Technology**. Disponível em: <<https://www.trade.gov/country-commercial-guides/uruguay-information-and-communication-technology>>. Acesso em: 10 dez. 2025.

URUGUAY DIGITAL, Uruguay Digital, disponível em: <<https://www.gub.uy/uruguay-digital/home>>. acesso em: 10 dez. 2025.

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.

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.

WU, Tim. **The Age of Extraction: How Tech Platforms Conquered the Economy and Threaten Our Future Prosperity**. [s.l.]: Knopf, 2025.

WU, Tim. The Curse of Bigness: Antitrust in the New Gilded Age. **Faculty Books**, 2018. Disponível em: <<https://scholarship.law.columbia.edu/books/63>>.

ZINGALES, Nicolo; AZEVEDO, Paula Farani de. **A aplicação do direito antitruste em ecossistemas digitais: desafios e propostas**. [s.l.]: FGV Direito Rio, 2022. Disponível em: <<https://hdl.handle.net/10438/32889>>. Acesso em: 11 dez. 2025.

Apertus. Swiss AI. Disponível em: <<https://www.swiss-ai.org/apertus>>. Acesso em: 10 dez. 2025.

Apertus: A fully open, transparent, multilingual language model. Disponível em: <<https://www.swisscom.ch/en/about/news/2025/09/02-apertus.html>>. Acesso em: 4 jan. 2026.

Apertus: a fully open, transparent, multilingual language model | ETH Zurich. Disponível em: <<https://ethz.ch/en/news-and-events/eth-news/news/2025/09/press-release-apertus-a>>.



[fully-open-transparent-multilingual-language-model.html?utm_source=chatgpt.com](https://openai.com/research/fully-open-transparent-multilingual-language-model.html?utm_source=chatgpt.com)>.

Acesso em: 10 dez. 2025.

Artificial Intelligence for Science. Disponível em: <https://www.worldscientific.com/worldscibooks/10.1142/13123>>. Acesso em: 5 jan. 2026.

BELLI, Luca. **Compras Públicas como Alavanca da Soberania Digital.** Câmara Técnica de Economia Digital (CTED) do CITDigital. 2025.

Big Tech fines tracker. Proton. Disponível em: <https://proton.me/tech-fines-tracker/>>. Acesso em: 11 dez. 2025.

Community networks - the Internet by the people, for the people.1.1.

Data for development. Geneva: United Nations, 2024.

Fuga de cérebros: o que o Brasil faz para evitar saída de cientistas? – ABC – Academia Brasileira de Ciências. Disponível em: https://www.abc.org.br/2025/09/01/fuga-de-cerebros-o-que-o-brasil-faz-para-evitar-saida-de-cientistas/?utm_source=chatgpt.com>. Acesso em: 10 dez. 2025.

IA Generativa e LGPD: transparência, desafios regulatórios e caminhos para a conformidade. Disponível em: <https://repositorio.fgv.br/items/ddb2b6b5-d069-42d3-88c8-ac10b9ee3908>>. Acesso em: 10 dez. 2025.

Inside Elon Musk's Government Contracts. Built In. Disponível em: <https://builtin.com/articles/elon-musk-government-contracts>>. Acesso em: 5 jan. 2026.

Market features in AI infrastructure: Competition in artificial intelligence infrastructure. OECD. Disponível em: https://www.oecd.org/en/publications/competition-in-artificial-intelligence-infrastructure_623d1874-en/full-report/component-6.html>. Acesso em: 10 dez. 2025.

Nova Indústria Brasil. Ministério da Fazenda. Disponível em: <https://www.gov.br/fazenda/pt-br/aceso-a-informacao/acoes-e-programas/transformacao-ecologica/programas-em-destaque/nova-industria-brasil/nova-industria-brasil>>. Acesso em: 4 jan. 2026.

Open Source Special Edition MIT Technology Review Brasil 2021.

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: 4 jan. 2026.

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.

Plano Brasil Digital 2030.

Programas Estruturantes e Mobilizadores. Ministério da Ciência, Tecnologia e Inovação. Disponível em: <https://www.gov.br/mcti/pt-br/acompanhe-o>



mcti/fndct/paginas/planejamento/programas-estruturantes-e-mobilizadores/programas-estruturantes-e-mobilizadores>. Acesso em: 4 jan. 2026.

Relatório Seminário Pilha IA Soberana.

Scale, market power and competition in a digital world: Is bigger better? [s.l.: s.n.], 2021. (OECD Science, Technology and Industry Working Papers). Disponível em: <https://www.oecd.org/en/publications/scale-market-power-and-competition-in-a-digital-world_c1cff861-en.html>. Acesso em: 5 dez. 2025.

Towards AI Regulation in Brazil: Past Policies, Future Paths, and Present Uncertainties.

Uruguay Digital. Uruguay Digital. Disponível em: <<https://www.gub.uy/uruguay-digital/home>>. Acesso em: 10 dez. 2025.

View - UIS Data Browser. Disponível em: <<https://uis-data-browser-frontend-9qoly6dvy-ixt1.vercel.app/view>>. Acesso em: 4 jan. 2026.

Zero Rating. Zero Rating. Disponível em: <<https://zerorating.wordpress.com/publications/>>. Acesso em: 10 dez. 2025.