

ARTIGO PARA DISCUSSÃO
#003 / 2025



SOBERANIA DIGITAL E INTELIGÊNCIA ARTIFICIAL NO BRASIL

Luca Belli, Filipe Medon, Walter B. Gaspar, Natalia
Couto, Breno Pauli Medeiros

09.2025

SUMÁRIO

RESUMO EXECUTIVO	2
1. INTRODUÇÃO	2
1.1. Da soberania digital à soberania em IA.....	5
1.2. Os vários tons da soberania digital.....	7
1.3. As bases constitucionais da soberania tecnológica no Brasil	8
1.4. Soberania em IA é soberania sobre dados	11
1.5. O Brasil não é condenado a ser uma colônia digital	17
2. UMA ABORDAGEM EM “CAMADAS” À SOBERANIA EM IA	18
3. CONSEQUÊNCIAS DA FALTA DE SOBERANIA DIGITAL	22
3.1 Dependência da nuvem estrangeira:	23
3.2 Plataformas digitais patrocinadas como concentradoras de dados pessoais, intermediadoras da economia, e mediadoras da esfera pública.....	24
3.3 Exposição a interrupções em cadeias de suprimento	28
4. CAMINHOS E SOLUÇÕES	31
4.1 Governança da Soberania Digital	31
4.2 Principais atores na governança da soberania digital no Brasil.....	33
4.3 Instrumentos de coordenação para a soberania digital.....	37
REFERÊNCIAS	42

RESUMO EXECUTIVO

Ao longo dos últimos anos, o assunto da soberania digital emergiu como um dos temas mais debatidos nos círculos das políticas digitais. A soberania digital é um conceito central no debate contemporâneo sobre a autonomia tecnológica dos Estados. A soberania digital deve ser compreendida como “a capacidade de entender o funcionamento das tecnologias digitais, conseguir desenvolvê-las e regulá-las efetivamente, exercendo, portanto, autodeterminação, poder e controle sobre ativos digitais tais como dados, softwares, hardwares e redes eletrônicas.” (Belli, 2023; 2024; 2025; Jiang & Belli, 2024).

Desde 2020, o projeto CyberBRICS do Centro de Tecnologia e Sociedade da FGV Direito Rio vem analisando as estratégias, regulações e iniciativas sobre soberania digital dos países do bloco BRICS ao longo de três fases dedicadas à cibersegurança, transformação digital e governança de IA no BRICS. Este paper apresenta alguns dos principais achados das nossas pesquisas, para estimular um debate informado sobre o assunto, considerando que, como acontece com frequência quando um tema vira popular, muitos novos “especialistas” emergem, e o debate pode se tornar confuso.

Este trabalho é estruturado em quatro seções: a primeira analisa os conceitos de soberania digital, soberania de dados e soberania em IA; a segunda parte oferece uma abordagem em camadas à soberania em IA; a terceira ilustra alguns dos riscos que podem se realizar na situação de falta de soberania digital; por fim, a quarta seção destaca quais podem ser alguns caminhos e soluções potenciais para organizar a soberania digital no país.

1. INTRODUÇÃO

Ao longo dos últimos anos, o assunto da soberania digital emergiu como um dos temas mais debatidos nos círculos das políticas digitais. Desde 2020, o projeto CyberBRICS do Centro de Tecnologia e Sociedade da FGV Direito Rio¹ vem analisando as estratégias, regulações e iniciativas sobre soberania digital

¹ CENTRO DE TECNOLOGIA E SOCIEDADE (CTS-FGV). *Centro de Tecnologia e Sociedade*. Brasília: FGV Direito Rio, s.d. Disponível em: <https://direitorio.fgv.br/pesquisa/centro-de-tecnologia-e-sociedade>. Acesso em: 25 ago. 2025.

dos países do bloco BRICS ao longo de três fases dedicadas à cibersegurança², transformação digital³ e governança de IA no BRICS⁴.

A pesquisa elaborada no âmbito do projeto CyberBRICS oferece um insight particularmente valioso para os debates brasileiros sobre soberania digital, por três razões diferentes. Primeiramente, é literalmente a única pesquisa que existe no Brasil e no mundo que analisa quais estratégias, políticas industriais, e regulações foram adotadas por um grupo de países em desenvolvimento que se transformaram em lideranças tecnológicas globais ao longo das últimas décadas. Neste sentido, apesar de estar cientes das peculiaridades dos sistemas políticos de alguns países do bloco BRICS e das legítimas críticas que podem surgir sobre tais sistemas, nos parece particularmente valioso analisar e tentar entender como países em desenvolvimento conseguiram construir sua soberania digital, ao invés de tentar copiar “soluções” propostas, com resultados muito questionáveis, por países europeus, cujo nível de soberania digital continua sendo extremamente limitado, apesar de amplo desenvolvimento econômico e maturidade institucional de tais países⁵.

Em segundo lugar, como será evidente para o leitor deste trabalho, nossa pesquisa baseia-se numa abordagem sistêmica, evitando se concentrar somente num setor regulado ou dimensão única (por exemplo, regulação de dados pessoais, acesso à Internet, cibersegurança, etc.), mas adotando a visão sistêmica que acreditamos seja necessária para analisar e conectar tais dimensões, identificando as interseções de tais setores que consideramos

² BELLI, Luca (ed.). *CyberBRICS: Cybersecurity Regulations in the BRICS Countries*. Cham: Springer, 2021. DOI: <https://doi.org/10.1007/978-3-030-56405-6>. ISBN (eBook): 978-3-030-56405-6.

³ COMPUTER LAW & SECURITY REVIEW. *Special Issue: Digital Transformation in the BRICS Countries*. Vol. 54, set. 2024. Disponível em: <https://www.sciencedirect.com/special-issue/10VRL9GGMQG>. Acesso em: 25 ago. 2025.

⁴ BELLI, Luca. *BRICS countries and AI sovereignty: Introduction to Thematic Section. The African Journal of Information and Communication (AJIC)*, v. 34, 2024, p. 1–6. DOI: <https://doi.org/10.23962/ajic.i34.20864>. Disponível em: <https://ajic.wits.ac.za/article/view/20864>. Acesso em: 25 ago. 2025.

⁵ O fracasso da UE na construção de soberania digital na última década e, especialmente, desde a primeira administração Trump, foi amplamente debatido ao longo da conferência “Towards European Digital Independence: Building the Eurostack”, organizada no próprio Parlamento Europeu. <https://digitalindependencieu.wordpress.com/agenda/> Cabe ressaltar que a dependência tecnológica europeia foi instaurada apesar dos países membros da EU disporem de capacidades intelectuais, financeiras, tecnológicas e institucionais extremamente elevadas. Assim, parece evidente que a experiência europeia precisa ser estudada principalmente como exemplo de fracasso em termos de soberania digital, como evidenciado por vários relatórios elaborados pelos participantes da conferência <https://eurostack.eu/>

como elementos indissociáveis de um ecossistema digital (ou de sistemas de IA). Entendemos perfeitamente a dificuldade de se adotar tal abordagem sistêmica, especialmente devido à enorme setorialização e consequente compartimentação, da regulação, das políticas públicas e do próprio ensino sobre o funcionamento das tecnologias digitais que compõem sistemas de IA.

Porém, nos parece essencial ter uma abordagem sistêmica para compreender o funcionamento e lidar efetivamente com – literalmente – **sistemas** de IA ou **sistemas** digitais. Nesta perspectiva, nossa pesquisa almeja analisar as diferentes estratégias regulatórias que podem ser usadas para regular tecnologias digitais e sistemas de IA além da lei, alavancando ferramentas econômicas (como investimentos e tributação) ou a própria estrutura dos hardwares e softwares que compõem tais sistemas, ou seja regulando por meio da “arquitetura” e enxergando o “poder estrutural” da tecnologia digital, ou ainda por meio de hábitos criados artificialmente para regular o comportamento do usuário⁶.

Neste contexto, a soberania digital se torna um conceito central no debate contemporâneo sobre a autonomia tecnológica dos Estados. A soberania digital deve ser compreendida como “a capacidade de entender o funcionamento das tecnologias digitais, conseguir desenvolvê-las e regulá-las efetivamente, exercendo, portanto, autodeterminação, poder e controle sobre ativos digitais tais como dados, softwares, hardwares e redes eletrônicas.” (Belli, 2023; 2024; 2025; Jiang & Belli, 2024). A partir desta definição podemos estruturar três pilares fundamentais: **autodeterminação, autonomia tecnológica e cibersegurança**. Esses pilares asseguram que países, entidades e até pessoas possam entender, desenvolver, gerir e proteger suas infraestruturas digitais de forma independente, evitando vulnerabilidades decorrentes da dependência excessiva de atores estrangeiros (Jiang & Belli, 2024).

⁶ Tais dimensões são estudadas no âmbito do direito e tecnologia há mais de vinte cinco anos e pelos cientistas políticos há quase quarenta anos. Sobre o poder estrutural, ver Susan Strange, *States and Markets* (1st edn, Continuum 1988); Luca Belli. *Structural Power as a Critical Element of Digital Platforms’ Private Sovereignty*. In Edoardo Celeste, Amélie Heldt and Clara Iglesias Keller (Eds). *Constitutionalising Social Media*. (Hart 2022). Sobre as diferentes modalidades de regulação das tecnologias digitais, ver Lawrence Lessig ‘The Law of the Horse: What Cyberlaw Might Teach’ [1999] *Harvard Law Review* 501; L. Lessig, *Code: And Other Laws of Cyberspace Version 2.0*, (Basic Books 2006); L. Belli *De la Gouvernance à la régulation de l’Internet* (Berger-Levrault 2016).

Além dos pilares, Belli (2023; 2024) destaca três dimensões para a efetivação da soberania digital: **pesquisa, desenvolvimento⁷ e regulação**. Tais dimensões são intimamente conectadas e, como destacaremos na Seção 4 deste trabalho, precisam ser articuladas por meio de mecanismos de governança multissetorial voltados ao estabelecimento de uma sinergia entre objetivos públicos, fomento de tais objetivos, pesquisa sobre como alcançar tais objetivos por meio de inovação, desenvolvimento de soluções, e consequente transformação de tais soluções em produtos e serviços escaláveis, e fiscalização da regulação setorial.

Este paper apresenta alguns dos principais achados das nossas pesquisas, para estimular um debate informado sobre o assunto, considerando que, como acontece com frequência quando um tema vira popular, muitos novos “especialistas” emergem, e o debate pode se tornar confuso. Todos os trabalhos utilizados para preparar este documento foram revisados por pares, seguindo processos de revisão “duplamente cega” impostos pelas editoras internacionais que publicaram as pesquisas elaboradas no âmbito do Projeto CyberBRICS⁸ ao longo dos últimos anos.

1.1. Da soberania digital à soberania em IA

A soberania em IA é uma espécie do genus soberania digital. Como destacamos em nosso estudo sobre *“Digital Sovereignty in the BRICS Countries : How the Global South and Emerging Power Alliances Are Reshaping Digital Governance”*⁹, embora a soberania digital tenha atraído uma atenção crescente tanto dos decisores políticos como dos acadêmicos, este conceito continua a ser fluido, polissêmico e multifacetado, não tendo ainda encontrado uma definição universalmente aceita. Neste contexto, o objetivo

⁷ Cabe ressaltar que pesquisa e desenvolvimento, apesar de conceitos distintos, são frequentemente tratados em conjunto - P&D -, sendo a pesquisa voltada para a expansão das fronteiras do conhecimento ou seu aprofundamento e o desenvolvimento, para a realização de etapas iniciais ou avançadas no processo de criação de novos produtos, serviços etc. Assim, devem ser enxertadas como parte de um mesmo processo contínuo, iterativo, complexo, desenvolvido de forma sistêmica, de inovação, que possa ser, por meio de várias etapas, levar a introdução de novos produtos e serviços no mercado ou para o proveito da sociedade.

⁸ <https://cyberbrics.info/>

⁹ JIANG, Min; BELL, Luca (orgs.). *Digital Sovereignty in the BRICS Countries*. Cambridge: Cambridge University Press, 2025. ISBN 9781009531139. DOI: <https://doi.org/10.1017/9781009531085>. Disponível em: <https://www.cambridge.org/core/books/digital-sovereignty-in-the-brics-countries/27E9FD7E4579C76C8D4BA52F7670B431>. Acesso em: 25 ago. 2025.

deste trabalho é oferecer as ferramentas necessárias para esclarecer o debate, desde as bases conceituais da soberania digital até as implementações práticas e operacionais do conceito.

A noção westfaliana de soberania é entendida como a prerrogativa dos Estados-Nação do pleno gozo da integridade territorial, igualdade legal e não interferência em assuntos internacionais junto com o monopólio do uso legítimo da força e autoridade suprema sobre seu território. Porém tal noção implica uma centralidade estadual desafiada pelo papel essencial que tecnologias digitais com alcance transnacional – especialmente sistemas de IA – acabaram desempenhando no que diz respeito ao funcionamento de nossas sociedades, economias e democracias.

Neste contexto, nossa definição de trabalho de soberania digital¹⁰ tem sido “a capacidade de entender o funcionamento das tecnologias digitais, conseguir desenvolvê-las e regulá-las efetivamente, exercendo, portanto, autodeterminação, poder e controle sobre ativos digitais tais como dados, softwares, hardwares e redes eletrônicas.” Com base nesta definição, a soberania em IA pode ser definida como “a capacidade de entender, desenvolver e regular sistemas de IA, mantendo assim a autodeterminação, agência e controle sobre tais sistemas”¹¹.

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

¹⁰ JIANG, Min; BELLI, Luca. *Introdução: Contestando a soberania digital: Desembarçando um conceito complexo e multifacetado*. In: JIANG, Min; BELLI, Luca (orgs.). *Digital Sovereignty in the BRICS Countries*. Cambridge: Cambridge University Press, 2025. p. 1–16. ISBN 9781009531139. DOI: <https://doi.org/10.1017/9781009531085>. Disponível em: <https://www.cambridge.org/core/books/digital-sovereignty-in-the-brics-countries/introduction/88A1164945DC955023BB812CA88FEABC>. Acesso em: 25 ago. 2025.

¹¹ JIANG, Min; BELLI, Luca. *Introdução: Contestando a soberania digital: Desembarçando um conceito complexo e multifacetado*. In: JIANG, Min; BELLI, Luca (orgs.). *Digital Sovereignty in the BRICS Countries*. Cambridge: Cambridge University Press, 2025. p. 1–16. ISBN 9781009531139. DOI: <https://doi.org/10.1017/9781009531085>. Disponível em: <https://www.cambridge.org/core/books/digital-sovereignty-in-the-brics-countries/introduction/88A1164945DC955023BB812CA88FEABC>. Acesso em: 25 ago. 2025.

1.2. Os vários tons da soberania digital

O discurso sobre soberania digital começa oficialmente em 2011, com a proposição da Organização de Cooperação de Xangai, uma organização intergovernamental liderada por China e Rússia que, em 2011, elaborou um Código Internacional de Conduta para Segurança da Informação, atualizado em 2015, mencionando explicitamente o tema da “soberania na Internet” e associando a tal tema uma conotação autoritária. É claro que existem manifestações autoritárias da soberania (não somente digital) mas associar soberania digital inevitavelmente ao autoritarismo significa ignorar não somente a evolução do conceito, mas uma amplíssima gama de exemplos de “boa soberania digital”¹².

Um de tais exemplos é parte de nosso cotidiano: o Pix. Antes do Pix, a única opção disponível para processar pagamentos eletrônicos instantâneos em tempo integral no Brasil era utilizar as redes das gigantes estadunidenses Visa e Mastercard, que cobram uma taxa de 3% a 5% em cada transação, além de centralizar a coleta de dados de todos os seus usuários¹³.

O papel chave das duas empresas antes do Pix significava que a soberania brasileira sobre pagamentos digitais era de fato delegada a dois atores estrangeiros que monopolizavam renda, o controle sobre os dados coletados e, com base neles, a capacidade de desenvolver e competir em IA. Esses pontos são a principal razão pela qual o desenvolvimento de infraestruturas públicas digitais¹⁴ como o Pix é enormemente relevante do ponto de vista de uma boa soberania digital.

Poucos sabem que o Pix é diretamente inspirado do UPI, análogo sistema introduzido pela Reserve Bank of India em 2016 como uma rede de pagamento instantâneo baseada em uma API aberta operada pela National Payments

¹² BELLI, Luca. *Building Good Digital Sovereignty through Digital Public Infrastructures and Digital Commons in India and Brazil*. CyberBRICS, 11 set. 2023. Disponível em: <https://cyberbrics.info/building-good-digital-sovereignty-through-digital-public-infrastructures-and-digital-commons-in-india-and-brazil/>. Acesso em: 25 ago. 2025.

¹³ CHRISTL, Wolfie; KOPP, Katharina; RIECHERT, Patrick Urs. *How Companies Use Personal Data Against People: Automated Disadvantage, Personalized Persuasion, and the Societal Ramifications of the Commercial Use of Personal Information*. Cracked Labs, outubro de 2017. Disponível em: <https://crackedlabs.org/en/data-against-people>. Acesso em: 25 ago. 2025.

¹⁴ T20 BRASIL. *Task Force 05. A Consumer-Centric Digital Public Infrastructure: A Critical Approach to Financial Inclusion and Consumer Welfare*. Brasília, 2023. Disponível em: https://www.t20brasil.org/media/documentos/arquivos/TF05_ST_02_A_Consumer-centric66d5d363d0a6f.pdf. Acesso em: 25 ago. 2025.

Corporation of India. Ainda menos sabem que o UPI é inspirado pelo sistema Russo Mir, desenvolvido logo depois da invasão da Crimeia, em 2014, que resultou na primeira rodada de sanções – entre as quais a proibição do uso das redes Visa e Mastercard.

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

Quando o presidente estadunidense começou a adotar ordens executivas como armas econômicas, proibindo o uso de software estadunidense pela chinesa Huawei¹⁵ e tentando bloquear o TikTok, a maioria dos países europeus começaram a perceber os riscos da dependência tecnológica. Pela primeira vez nos últimos 30 anos as lideranças europeias se deram conta de sua extrema vulnerabilidade por falta de autonomia tecnológica. Porém, é assustador constatar que nos últimos cinco anos eles não foram capazes sequer de elaborar um esboço de plano para criar autonomia tecnológica, sendo hoje totalmente desamparados face a sua situação de colônia digital. Neste sentido, nos parece que a experiência europeia não ofereça boas práticas de soberania digital que possam ser replicada e, ao contrário, deveria ser estudada como um exemplo de falta de soberania digital.

1.3. As bases constitucionais da soberania tecnológica no Brasil

A evolução do debate sobre soberania digital na direção da garantia da autonomia tecnológica é particularmente relevante, não somente porque tal aspiração é mais que legítima, mas particularmente porque, diferentemente da

¹⁵ JIANG, Min. *U.S. Ban on Huawei: Superpowers' Insecurities and Nightmares*. *CyberBRICS*, 3 jun. 2019. Disponível em: <https://cyberbrics.info/u-s-ban-on-huawei-superpowers-insecurities-and-nightmares/>. Acesso em: 25 ago. 2025.

Europa, no Brasil a autonomia tecnológica é um objetivo constitucionalmente protegido¹⁶.

Pouquíssimas pessoas na própria vida chegam a ler até o artigo 219 da Constituição Federal. Quem fizer parte desse seleto grupo pode entender que, no Brasil, a soberania digital e soberania em IA encontram amparo constitucional diretamente na autonomia tecnológica. Assim, nos termos da Constituição:

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

Para se alcançar tal autonomia no que diz respeito à IA é necessário se adotar estratégias, políticas e mecanismos de governança e regulação aptos a entender e gerenciar as (inter)dependências e as potenciais vulnerabilidades existentes entre os diferentes elementos que dão suporte ao funcionamento dos sistemas de IA. Tais elementos podem ser considerados como “Facilitadores Essenciais da Soberania em IA”¹⁷ e são: dados, capacidade algorítmica, capacidade computacional, conectividade significativa, energia elétrica, recursos humanos capacitados, cibersegurança e um marco legislativo capaz de regular os riscos da IA de maneira efetiva.

Como demonstra nossa pesquisa¹⁸, estes facilitadores estão interligados e é essencial entender esta conexão para regular de maneira eficiente e efetiva.

¹⁶ BELLI, Luca; GALDINO DE MAGALHÃES SANTOS, Larissa. *Editorial: Toward a BRICS stack? Leveraging digital transformation to construct digital sovereignty in the BRICS countries*. *Computer Law & Security Review*, [S.l.], v. 55, p. 106064, 2024. DOI: 10.1016/j.clsr.2024.106064. Disponível em: <https://www.sciencedirect.com/science/article/pii/S0267364924001304>. Acesso em: 25 ago. 2025.

¹⁷ 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, R.; SCHERTEL MENDES, L.; BIONI, B.; DA MOTA ALVES, F. *Inteligência Artificial e Regulação*. Gen-Jurídico. 2024. Disponível em: <https://cyberbrics.info/soberania-em-inteligencia-artificial-o-que-e-o-quais-facilitadores-essenciais-podem-tornar-o-brasil-um-pais-soberano-em-ia/>. Acesso em: 25 ago. 2025.

¹⁸ BELLI, Luca; GASPAR W.B. *The Quest for AI Sovereignty, Transparency and Accountability*. CyberBRICS, 2025. Disponível em: <https://cyberbrics.info/pre-print-the-quest-for-ai-sovereignty-transparency-and-accountability/>. Acesso em: 25 ago. 2025.

Para entender a necessidade de visão holística e as vulnerabilidades sistêmicas que podem surgir na falta de tal visão, é suficiente pensar que os enormes investimentos em capacidade algorítmica e computacional propostos pelo Plano Brasileiro de IA¹⁹ serão relativamente inúteis para os cidadãos brasileiros, se a maioria da população do País – 78% segundo os dados do Cetic.br²⁰ – continuar sem conectividade significativa, tendo acesso ilimitado somente a redes sociais patrocinadas, enquanto o acesso a todo o restante da internet tem um custo se aproximando a 15% de um salário mínimo.

Como destacaremos na seção 3.2, neste contexto, a enorme maioria dos “usuários de internet” no Brasil são de fato meros usuários de redes sociais, que estão entre os pouquíssimos aplicativos subsidiados nas franquias dos planos de internet móvel, concentrando a coleta de dados pessoais e a capacidade de inovação em IA - bem como de perfilamento populacional - que deriva do tratamento de tais dados. Assim, cabe se perguntar quais consumidores poderão acessar modelos de IA brasileira em supercomputadores brasileiros se para acessar tal inovação continua sendo necessário dispor de um plano de conectividade que somente 22% pode suportar, enquanto redes sociais patrocinadas já estão oferecendo acessos a suas próprias IA “de graça”, criando o hábito – ou a adição – ao uso desta IA nos cérebros dos usuários?

Outros países, como a Índia, proibiam as práticas de “patrocínio de aplicativos” ou “zero rating”²¹ mencionadas acima, ou seja, os modelos de conectividade

¹⁹ BRASIL. *Plano Brasileiro de IA terá supercomputador e investimento de R\$ 23 bilhões em quatro anos*. Ministério da Ciência, Tecnologia e Inovação, 2024. Disponível em: <https://www.gov.br/mcti/pt-br/acompanhe-o-mcti/noticias/2024/07/plano-brasileiro-de-ia-tera-supercomputador-e-investimento-de-r-23-bilhoes-em-quatro-anos>. Acesso em: 25 ago. 2025.

²⁰ CASTELLO, Graziela (coord.). *Conectividade significativa: propostas para medição e o retrato da população no Brasil*. São Paulo: Núcleo de Informação e Coordenação do Ponto BR (NIC.br), 2024. Disponível em: <https://cetic.br/pt/publicacao/conectividade-significativa-propostas-para-medicao-e-o-retrato-da-populacao-no-brasil/>. Acesso em: 25 ago. 2025.

²¹ Há pelo menos uma década, pesquisadores alertam sobre o potencial das práticas de zero rating para aumento de concentração de poder, mercado e dados nos ecossistemas digitais, bem como a incompatibilidade desta prática com o Marco Civil da Internet. BELLI, L. Neutralidade de rede e ordem econômica. Observatorio do marco Civil da Internet. 2017. <https://www.omci.org.br/jurisprudencia/207/neutralidade-de-rede-e-ordem-economica/>; BELLI, L. Neutralidade da rede, zero-rating e o Marco Civil da Internet. Em: Governança e regulações da internet na América Latina. Rio de Janeiro: FGV Direito Rio, 2018b. p. 175–204; IDEC; INSTITUTO LOCOMOTIVA. Acesso à internet móvel pelas classes CDE. São Paulo: IDEC e Instituto Locomotiva, nov. 2021. Disponível em: https://idec.org.br/sites/default/files/pesquisa_locomotiva_relatorio.pdf. Uma coleção de estudos sobre a prática pode se encontrar em www.zerorating.info Acesso em: 25 ago. 2025.

limitados aos aplicativos patrocinados (entre os quais havia principalmente redes sociais estadunidenses), consagrando a neutralidade da rede. Essa decisão, apesar de ser frequentemente subestimada, talvez esta tenha sido a medida que mais fez pela soberania digital da Índia²². A maioria dos observadores naquela época perceberam a iniciativa indiana como uma grande vitória para a liberdade expressão, e para promoção dos direitos dos consumidores, mas na verdade um dos principais impactos da adoção dessa política foi a preservação do potencial do ecossistema digital nacional, da concorrência e da inovação local, ou seja, o fortalecimento da soberania no sentido de autodeterminação e autonomia tecnológica.

Proibindo o patrocínio de somente alguns aplicativos dominantes – o que acontece na maioria dos países do mundo – os indianos evitaram que os dados da população fossem concentrados somente por algumas plataformas dominantes e permitiram que as startups indianas fossem acessíveis em pé de igualdade para todos os usuários. Essas startups agora são gigantes e a Índia está vivendo uma *belle époque* da inovação²³, passando a ser o terceiro lugar com mais startups do mundo²⁴. Os indianos entenderam extremamente bem o valor da soberania digital.

1.4. Soberania em IA é soberania sobre dados

Continuamos a proclamar que os dados são o petróleo do Século XXI, mas de fato entregamos uma concessão gratuita para explorar essa riqueza *ad infinitum*, e desenvolver IA com tais dados, para as mesmas pouquíssimas empresas estrangeiras que não somente sabemos ser implicadas em atividade de espionagem reveladas desde 2013 por Edward Snowden, mas

²² BELLI, L. BRICS Countries to Build Digital Sovereignty. Em: BELLI, L. (Ed.). CyberBRICS: Cybersecurity Regulations in the BRICS Countries. Cham: Springer International Publishing, 2021. p. 271–280; BELLI ET AL. Cibersegurança: uma visão sistêmica rumo a uma proposta de Marco Regulatório para um Brasil digitalmente soberano. FGV Direito Rio. 2023.

²³ PARSHEERA, S. Net neutrality in India: From rules to enforcement. Em: BELLI, L.; PAHWA, N.; MANZAR, O. (Eds.). The value of internet openness in times of crisis: Official outcome of the UN IGF coalitions on net neutrality and on community connectivity. Rio de Janeiro: FGV Direito Rio, 2020. p. 61–68.

²⁴ CHOUDHURY, S. P.; SHARMA, S.; JAIN, S. Three Waves: Tracking the Evolution of India's Startups. Knowledge at Wharton, 5 nov. 2019. Disponível em: <<https://knowledge.wharton.upenn.edu/article/three-waves-tracking-evolution-indias-startups/>>. Acesso em: 3 ago. 2025; SORENSEN, D. Unicorn Hunting 2022: Top Countries & Industries for Unicorn Companies. Disponível em: <<https://tipalti.com/unicorn-hunting-2022/>>. Acesso em: 3 ago. 2025.

que recentemente manifestaram total submissão à nova administração Trump,²⁵ e se beneficiam de tributação extremamente vantajosa e limitada²⁶.

Este cenário é bem distante de uma situação de soberania e ainda mais da cibersegurança que o País precisa²⁷. Ao contrário, políticas de soberania digital são essenciais para (re)construir autodeterminação, cibersegurança e controle sobre ativos digitais ao invés de ser controlados por meio de sistemas de IA e tecnologias estrangeiras das quais nos tornamos perigosamente dependentes²⁸. Neste sentido, é necessário frisar que soberania em IA não podem prescindir de soberania sobre dados²⁹.

Com base na nossa pesquisa em soberania digital³⁰, podemos definir a soberania de dados na aptidão para compreender o funcionamento de tecnologias que processam dados, saber desenvolver tais tecnologias e regulá-las efetivamente, rompendo com modelos extrativistas que reproduzem lógicas coloniais na extração de dados pessoais e outras informações valiosas por meio de tecnologia digital.

Portanto, ser soberano sobre dados, não significa simplesmente adotar leis de proteção de dados: a soberania depende da habilidade para desenvolver tecnologias baseadas em dados e para implementar efetivamente as normas que as regulam, e ambas as habilidades podem ser realizadas concretamente somente quando existir a compreensão do funcionamento das tecnologias que

²⁵ MAGEE, T. Big tech's support for Trump isn't a moral about-face – it's business - Raconteur. Disponível em: <<https://www.raconteur.net/technology/tech-tribute-trump-oped>>. Acesso em: 25 ago. 2025.

²⁶ Uma análise detalhada da atual ineficiência do regime tributário pátrio no que diz respeito à tributação de modelos extrativistas de dados pessoais se encontra em BELLI, Luca FOSSATI, Gustavo; MCCLASKEY, Layla; e ZINGALES Nicolo. Proteção de dados, tributação de dados e equidade de dados: equilíbrio entre valores, riscos e obrigações. Artigo para Discussão Apresentado na Computers, Privacy and Data Protection Conference Latin America (CPDP LatAm) 2025, 2025.. Disponível em: <https://cpdp.lat/pt-br/publicacoes/>.

²⁷ BELLI, L. et al. Cibersegurança: uma visão sistêmica rumo a uma proposta de Marco Regulatório para um Brasil digitalmente soberano. repositorio.fgv.br, 14 jun. 2023.

²⁸ BELLI, Luca; JIANG, Min. Conclusion: Digital Sovereignty in the BRICS: Structuring Self-Determination, Cybersecurity, and Control. In: JIANG, Min; BELLI, Luca (Ed.). Digital Sovereignty in the BRICS Countries: How the Global South and Emerging Power Alliances Are Reshaping Digital Governance. Cambridge: Cambridge University Press, 2025. p. 214–238.

²⁹ BELLI, Luca; GASPAR, Water 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. 46, p. 105–123, 2024. Disponível em: <https://www.sciencedirect.com/science/article/pii/S0267364924000839>. Acesso em: 25 ago. 2025.

³⁰ JIANG, Min ; BELLI, Luca. Digital Sovereignty in the BRICS Countries. [s.l.]: Cambridge University Press, 2024.

coletam e processam dados. Porém, tal ideal ainda está distante da realidade da maioria global. Fortalecer esse domínio é crucial tanto para a proteção individual de dados quanto para a promoção de autonomia tecnológica nacional, porém, como destacaremos em seguida, é somente uma dimensão da soberania sobre dados.

Conforme destacado recentemente pela jurisprudência do Tribunal Interamericano de Direitos Humanos, no caso CAJAR v. Colômbia, a autodeterminação informativa é um direito fundamental autônomo³¹ e o Estado deve desempenhar papel ativo no auxílio aos titulares, através de mecanismos que permitam o pleno gozo de direitos. Reconhece-se, inspirado em teóricos como Stefano Rodotà e Donna Haraway, que dados pessoais constituem extensões eletrônicas do corpo e, portanto, controle sobre como dados pessoais são tratados é essencial para a dignidade do indivíduo. Porém, é importante frisar que a autodeterminação informativa, consagrada no artigo 2 da Lei Geral de Proteção de Dados (LGPD), transcende a proteção individual e deve ser considerada também na sua dimensão coletiva.

É justamente a consideração de tal dimensão coletiva da autodeterminação informativa³² que nos permite reconhecer a centralidade dos dados para o desenvolvimento nacional, e exige que a governança de dados reconheça o valor econômico dos dados, de forma a promover o interesse público, o desenvolvimento nacional, e assegurar democracia e a cibersegurança das infraestruturas digitais. Nessa perspectiva, dados são um fator de produção³³, equiparável a trabalho, capital e terra, e a regulação de dados deve servir ao

³¹ BELLI, Luca; BRIAN, Ana; MENDOZA, Jonathan; PALAZZI, Pablo Andrés; REMOLINA, Nelson. Transferência internacional de dados pessoais na América Latina. Rio de Janeiro: FGV Direito Rio — Centro de Tecnologia e Sociedade, nov. 2024. Disponível em: <<https://repositorio.fgv.br/items/98aaa2e4-7279-4649-8dae-836ca8a65bae>>. Acesso em: 26 ago. 2025.

³² 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. 46, p. 105–123, 2024. Disponível em: <https://www.sciencedirect.com/science/article/pii/S0267364924000839>. Acesso em: 25 ago. 2025.

³³ Esse entendimento representa a base estruturante da concepção chinesa de dados, como destacaremos na seção 1.6. Neste sentido, após a promulgação da Estratégia Nacional de Big Data em 2015, durante o 18º Congresso do Partido Comunista Chinês, o governo da China instituiu, a partir do 19º Comitê Central, em 2019, um arcabouço regulatório e de política industrial fundamentado na concepção dos dados como fator de produção. Ver The Fourth Plenary Session of the 19th Central Committee of the Communist Party of China. (19 de outubro 2019) https://www.gov.cn/zhengce/2019-11/05/content_5449023.htm acessado em 19 de agosto 2025.

interesse público, consolidando a democracia, protegendo infraestruturas digitais e promovendo desenvolvimento nacional.

Para alcançar esta finalidade, não basta criar normas ou agências especializadas na proteção de dados pessoais. É necessário facilitar a pesquisa e o desenvolvimento das infraestruturas de hardware e software que possam permitir ao ecossistema nacional de dados florescer e ser aproveitado pelos atores públicos e privados nacionais, garantindo o respeito da legislação nacional. Neste sentido, o uso de infraestruturas de coleta e troca de dados como os *data exchanges* estabelecidos na China ou os *data spaces* vislumbrados pela União Europeia, parecem ser uma estratégia promissora para estimular a valorização e uso de dados nacionais, especialmente em setores como agropecuária, transportes etc. onde amplas bases de dados já são produzidas e não necessariamente exploradas.³⁴

Além disso, a tributação precisa ser enxergada como estratégia regulatória³⁵ voltadas a facilitar o exercício da autodeterminação informativa no sentido individual e coletivo. Como observamos em recente pesquisa, não existem no Brasil políticas tributárias que atuem como instrumentos regulatórios, capazes de incentivar boas práticas de governança, proteção de dados e segurança da informação, bem como de desestimular modelos de negócio baseados na extração ilimitada e na concentração de dados.³⁶ Neste sentido, parece necessário vincular a tributação desses modelos extrativistas à promoção da justiça social e à efetividade do direito fundamental à proteção de dados.

Por fim, além de precisar ser enxergada como a base infraestrutural do desenvolvimento nacional, a tecnologia pode se tornar um poderoso aliado do direito, por exemplo por meio de infraestruturas públicas digitais (DPIs no acrônimo inglês) e protocolos técnicos para registro do consentimento e comunicação de requisições, como já feito de forma embrionária pelo *Data*

³⁴ Os *data exchanges* serão explorados brevemente na seção 1.6. Os *data spaces* europeus não serão analisados porque, apesar de terem sido anunciados, de fato ainda não existem na prática, tendo somente experiências experimentais que dificilmente podem ser replicadas ou usadas como exemplos.

³⁵ CPDP LatAm. Publicações. CPDP LatAm 2025. Disponível em: <https://cpdp.lat/pt-br/publicacoes/>.

³⁶ BELLI, Luca FOSSATI, Gustavo; MCCLASKEY, Layla; e ZINGALES Nicolo. Proteção de dados, tributação de dados e equidade de dados: equilíbrio entre valores, riscos e obrigações. cit supra n (26).

Empowerment and Protection Architecture (DEPA)³⁷ da Índia. Por meio das DPIs, o estado recupera um protagonismo atrelado ao desenvolvimento de infraestrutura digital confiável³⁸ e interoperável, decisivo para construir bases concretas da soberania digital³⁹, mitigando as assimetrias e promovendo a responsabilização efetiva contra abusos e usos indevidos dos dados.

Assim, a adoção de protocolos padronizados⁴⁰ merece atenção para facilitar a aplicação de direitos como portabilidade e exclusão, respeitando a diversidade tecnológica e regulatória dos países da maioria global.

1.6. Soberania de dados: a experiência da China

A experiência chinesa em matéria de governança de dados é particularmente interessante porque constitui um dos exemplos mais consistentes de articulação entre regulação jurídica (por meio da sanção) e política industrial (por meio da facilitação) voltada à definir limites e proporcionar as ferramentas necessárias para aproveitar dados na economia digital. Desde outubro de 2019, o Comitê Central do Partido Comunista da China reconheceu, com decisão adotada no 4º Plenário do 19º, que os dados como um novo fator de produção, ao lado de terra, trabalho e capital, desencadeando uma abordagem sistêmica aos dados. Este novo fator de produção passou a ser compreendido não apenas como insumo econômico, mas como recurso estratégico, indissociável da segurança nacional, da soberania tecnológica e do desenvolvimento socioeconômico.⁴¹

³⁷ BELLI, Luca; GASPAR, Walter B.; SINGH JASWANT, Shilpa. Data sovereignty and data transfers as fundamental elements of digital transformation: Lessons from the BRICS countries. *International Data Privacy Law*, v. 13, n. 1, p. 1–?, 2024. Disponível em: <https://academic.oup.com/idpl/article-abstract/13/1/1/6809023>.

³⁸ MISRA, Manu; PANDAY, Jyoti; ZINGALES, Nicolo. Applying the CII Framework to DPIs considerations, challenges and opportunities. Rio de Janeiro: FGV Direito Rio – Centro de Tecnologia e Sociedade (CTS), dez. 2024. Disponível em: <https://repositorio.fgv.br/items/c8ebc2dc-7062-4d94-8497-ecc4bd1ec637>.

³⁹ BELLI, Luca. Building Good Digital Sovereignty through Digital Public Infrastructures. Think20 India, 2023. Disponível em: <https://t20ind.org/research/building-good-digital-sovereignty-through-digital-public-infrastructures/>. Acesso em: 26 ago. 2025.

⁴⁰ CATALDO, Bruna; GALDINO, Larissa; ZINGALES, Nicolo; PARSHERA, Smriti. Standardized payment interfaces as Digital Public Infrastructure. FGV Direito Rio, 2024. Disponível em: <https://hdl.handle.net/10438/36194>. Acesso em: 26 ago. 2025.

⁴¹ WANG W.W.. Contextualizing Personal Information: Privacy's Post-Neoliberal Constitutionalism and Its Heterogeneous Imperfections in China. *Computer Law & Security Review*. Volume 55, November 2024. <https://cyberbrics.info/contextualizing-personal-information-privacys-post-neoliberal-constitutionalism-and-its-heterogeneous-imperfections-in-china/> ; WANG W.W. (2023). China's digital transformation: Data-empowered state capitalism and social governmentality. *The African Journal of Information and Communication* (AJIC), 31, 1-13.

Do ponto de vista normativo, a República Popular da China adota instrumentos clássicos de regulação pela lei, fundados no poder sancionatório do Estado. Nesse sentido, destacam-se três diplomas fundamentais: a Lei de Cibersegurança, promulgada em 2017; a Lei de Segurança de Dados, de 2021; e a Lei de Proteção de Informações Pessoais, igualmente de 2021.⁴² A aplicação desses diplomas é concentrada na *Cyberspace Administration of China* (CAC), autoridade administrativa com ampla capacidade regulatória, responsável pela fiscalização e pela imposição de sanções.

Ao lado desse aparato sancionatório, observa-se a presença de uma política industrial de caráter facilitador, cujo objetivo é estruturar o ecossistema nacional de dados como espaço de inovação e de desenvolvimento econômico.⁴³ Entre os principais instrumentos empregados, destacam-se os investimentos públicos maciço em pesquisa e desenvolvimento; o estabelecimento de plataformas de intercâmbio de dados (*data exchanges*) desde 2015, que chegaram a gerar faturamentos bilionários para as empresas públicas que os gerenciam em cidades como Guiyang, Xangai, Pequim e Shenzhen⁴⁴; e a utilização de contratos administrativos e encomendas tecnológicas para estimular empresas nacionais do setor de tecnologia da informação. Tais medidas visam não apenas fomentar a circulação de dados como ativo econômico, mas também assegurar que essa circulação ocorra em ambiente controlado, certificado – especialmente em termos de qualidade, cibersegurança e direitos de exploração de dados, elementos explicitamente controlados pelos *data exchanges* – e auditável, compatível com os imperativos da segurança nacional e da proteção de direitos individuais.

A sinergia entre regulação pela sanção e política industrial pela facilitação confere ao modelo chinês elevada efetividade regulatória e reforça a soberania de dados do país. O Estado chinês, ao mesmo tempo em que estabelece normas jurídicas e instrumentos de fiscalização efetivos, cria condições materiais e institucionais para o desenvolvimento das tecnologias digitais no plano doméstico e, de maneira particularmente importante, a tributação dos

⁴² *Idem*.

⁴³ MA A. 'Regulation in pursuit of artificial intelligence (AI) sovereignty: China's mix of restrictive and facilitative modalities' (2024) 34 *African Journal of Information and Communication* 120; BELLI, Luca (2022) "New Data Architectures in Brazil, China, and India: From Copycats to Innovators, towards a post-Western Model of Data Governance," *Indian Journal of Law and Technology*: Vol. 18: Iss. 2, Article 3. <https://repository.nls.ac.in/ijlt/vol18/iss2/3>

⁴⁴ HE A., ARCESATI R. Data Marketplaces and Governance: Lessons from China. Governance Frameworks to Unleash the Value of Data. CIGI. 12 November 2024.

ativos de dados. Esse arranjo normativo e político assegura que a regulação dos dados não se limite a um exercício repressivo, sancionando o descumprimento da lei, como poderia ser pensado para um típico observador ocidental, mas constitua também um mecanismo de coordenação estratégica para facilitar o desenvolvimento tecnológico, em consonância com os objetivos nacionais de segurança, inovação e competitividade.

1.5. O Brasil não é condenado a ser uma colônia digital

Como explica nossa pesquisa, o Brasil foi até um precursor da soberania digital⁴⁵, com as políticas da primeira administração Lula sobre software livre. Por anos, o País foi referência mundial, oferecendo uma visão de software como ferramenta libertadora, em vez de um instrumento de extração de dados e de colonização digital.

Porém, o erro brasileiro foi pensar que software livre deveria somente ser adotado ao invés de estimular sua produção para que um ecossistema de tecnologias *open source* pudesse crescer e até ser exportado. A lição foi aprendida por outros países do BRICS. Os indianos entenderam o valor de se produzir infraestruturas públicas digitais⁴⁶ por meio de software livre, e os chineses entenderam muito bem o quanto é estratégico promover IA em código aberto para fortalecer sua soberania, como nos lembra o recente exemplo do DeepSeek.

Portanto, cabe ressaltar que a definição de um arcabouço regulatório, de políticas industriais e de uma governança capaz de fortalecer a soberania em IA não significa se isolar e instaurar uma autarquia digital⁴⁷. Ao contrário, pode - e, na opinião de quem escreve, deve - significar ter uma abordagem desenvolvimentista capaz de promover pesquisa, desenvolvimento e inovação e organizar tais iniciativas de maneira ecossistêmica, por meio de parcerias e cooperações, empoderando a população.

⁴⁵JIANG, Min; BELLI, Luca (orgs.). *Digital Sovereignty in the BRICS Countries*. Cambridge: Cambridge University Press, 2025.

⁴⁶ HARIHARAN, Venkatesh; NATARAJAN, Sarayu. Digital sovereignty and payments: a case study of the National Payments Corporation of India. In: JIANG, Min; BELLI, Luca (Ed.). *Digital Sovereignty in the BRICS Countries: How the Global South and Emerging Power Alliances Are Reshaping Digital Governance*. Cambridge: Cambridge University Press, 2025. p. 105–123. DOI: <https://doi.org/10.1017/9781009531085.008>.

⁴⁷ BELLI, Luca. Views: AI sovereignty and Brazil's role in the global debate. MediaNama, 14 jun. 2024. Disponível em: <https://www.medianama.com/2024/06/223-views-ai-sovereignty-brazil-global-debate/>. Acesso em: 25 ago. 2025.

As próximas seções analisam quais elementos deveriam ser considerados para se estruturar uma visão sistêmica da soberania digital e, particularmente, da soberania em IA, e consequentemente deveriam ser embutidos numa nova abordagem estratégica e regulatória de tais assuntos.

2. UMA ABORDAGEM EM “CAMADAS” À SOBERANIA EM IA

Ao reconhecer no modo de produção da economia digital a emergência de um novo paradigma tecnoeconômico fundado no valor de ativos intangíveis, especialmente os dados e o controle sobre o conhecimento; e assumir que uma inserção não dependente nesse novo paradigma é necessária para a estruturação de uma estratégia de desenvolvimento autônoma⁴⁸; uma visão soberana sobre a digitalização passa por ações que ampliam e reforçam o espaço de política pública à disposição do Estado na condução de assuntos relacionados ao uso, ao desenvolvimento e à regulação de tecnologias digitais⁴⁹.

A capacidade dos países de escolher e seguir um caminho de desenvolvimento é condicionada por uma gama de fatores domésticos e internacionais, incluindo restrições estabelecidas no âmbito de organizações internacionais, forma de inserção de sua indústria doméstica em cadeias globais de valor e em sistemas corporativos de inovação e restrições impostas a partir das escolhas de política pública, especialmente aquelas relativas ao comércio e à segurança nacional, de outras nações⁵⁰.

No campo das políticas digitais, estes fatores se consubstanciam em escolhas de arquitetura e investimentos de grandes empresas de tecnologia sediadas

⁴⁸ ORSI, Fabienne; CORIAT, Benjamin. The New Role and Status of Intellectual Property Rights in Contemporary Capitalism. *Competition & Change*, v. 10, n. 2, p. 162–179, jun. 2006;

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

PEREZ, Carlota. Microelectronics, long waves and world structural change: New perspectives for developing countries. *World development*, v. 13, n. 3, p. 441–463, 1985.

⁴⁹ JACKSON, Rosanna. The purpose of policy space for developing and developed countries in a changing global economic system. *Research in Globalization*, v. 3, p. 100039, 1 dez. 2021.

⁵⁰ JACKSON, Rosanna. The purpose of policy space for developing and developed countries in a changing global economic system. *Research in Globalization*, v. 3, p. 100039, 1 dez. 2021;

RIKAP, Cecilia. *Capitalism, Power and Innovation; Intellectual Monopoly Capitalism Uncovered*. London & New York: Routledge, 2021.

em países centrais, controladoras de complexas redes globais de produção de valor; restrições e diretrizes estabelecidas por organizações internacionais, como aquelas relativas à propriedade intelectual, proteção do meio ambiente e ao regime fiscal de fluxos globais de valor, bem como a sua capacidade de atuação; e a securitização de elementos da economia digital, como o controle sobre matérias-primas, restrições de negociação de determinadas tecnologias de interesse nacional, controle do fluxo migratório de profissionais especializados, dentre outros.

Tudo isso tem sido evidenciado recentemente pela disputa econômica e tecnológica entre Estados Unidos e China, em que o controle sobre determinadas tecnologias estratégicas e condicionantes da dominância de mercados de tecnologias digitais de empresas das respectivas nações tem sido ponto nevrálgico de discussões em torno de temas de segurança nacional, dependência tecnológica e política industrial⁵¹.

A partir da perspectiva de um país como o Brasil, o conceito de soberania digital pode ser detalhado em componentes que sejam essenciais para fazer frente a dinâmicas globais que impactam seu espaço de política digital e de desenvolvimento. É possível compreender a soberania digital como uma “pilha” composta por múltiplas camadas interdependentes (Belli, 2023; 2024), que precisam ser desenvolvidas de forma coordenada:

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

⁵¹ DIGWATCH TEAM. US bans chips, quantum and AI investment in China | Digital Watch Observatory. DigWatch, 11 ago. 2023. Disponível em: <<https://dig.watch/updates/us-bans-chips-quantum-and-ai-investment-in-china>>. Acesso em: 20 maio. 2024; GUZMAN, Chad de. A Timeline of the U.S.-China Trade War During Trump's Second Term. Disponível em: <<https://time.com/7292207/us-china-trade-war-trump-tariffs-timeline/>>. Acesso em: 15 ago. 2025.

de IA sejam acessíveis, utilizáveis e compartilháveis com a maior parte possível da população.

5. **Recursos energéticos e minerais:** disponibilidade de energia limpa, segura e sustentável, além de minerais críticos (como lítio, nióbio e terras raras), essenciais para a fabricação de chips, semicondutores e dispositivos digitais.
6. **Recursos humanos:** formação, retenção e valorização de talentos em ciência da computação, engenharia, segurança da informação e áreas correlatas, bem como áreas do conhecimento necessárias para um entendimento interdisciplinar, crítico e ético da soberania digital.
7. **Riscos de cibersegurança:** mitigação de vulnerabilidades técnicas, regulação sistêmica - acompanhada por uma estrutura de governança que a coordene e execute - e proteção contra ameaças digitais.
8. **Resiliência à interferência estrangeira em processos regulatórios internos:** capacidade de entender e enfrentar a interferência desproporcional e assimétrica de empresas e governos estrangeiros na formulação de políticas públicas, processos decisórios e processos legislativos, por meio, sobretudo, da manipulação de narrativas capazes de inviabilizar o desenvolvimento de infraestruturas soberanas.

Cada componente da “pilha” está inserido em um complexo contexto institucional formado por entidades públicas e privadas e variados conjuntos normativos. Lançar uma visão sistêmica (Cassiolato, 2008) sobre a soberania digital, que entenda o funcionamento e as interações de todos os elementos da pilha, requer reconhecer a interrelação dinâmica entre os subsistemas de:

- Políticas públicas: incluindo os atores que participam da sua composição, implementação e avaliação. Isto inclui entidades do Poder Público, especialmente o Executivo por meio de seus Ministérios (e.g., MCTI, MDIC etc.), bem como organizações de representação setorial da indústria (e.g., CNI, Assesspro, Brasscom etc.), empresas públicas (e.g., Serpro, Dataprev, CEITEC etc.) e privadas (e.g., Google, Microsoft, IBM etc.), representantes de interesses diversos na sociedade, como organizações da sociedade civil (e.g., IDEC, NIC.br etc.), e entidades híbridas de gestão de políticas públicas (e.g., EMBRAPPII, Softex).
- Financiamento: incluindo atores públicos e privados que atuem no financiamento de ações pertinentes, especialmente pesquisa, desenvolvimento e inovação (PD&I). Atores estatais como FINEP e as fundações de amparo à pesquisa estarão mais proximamente envolvidos em etapas de pesquisa e desenvolvimento, provendo financiamento paciente e de longo prazo⁵², enquanto financiadores como bancos de desenvolvimento (BNDES, bancos de

⁵² MAZZUCATO, Mariana. The Entrepreneurial State. London: Penguin, 2018.

desenvolvimento estaduais) e arranjos privados de investimento atuarão em etapas de inovação de menor incerteza.

- Construção de capacidades: envolvendo organizações que atuam na formação de profissionais e incorporação do progresso técnico, como universidades públicas e privadas, institutos de pesquisa, redes de formação profissional (e.g., organizações do Sistema S).
- Pesquisa e desenvolvimento: incluindo instituições científicas e tecnológicas que atuem em pesquisa básica e aplicada, como universidades, fundações e unidades de pesquisa situadas em empresas públicas e privadas.
- Evoluções do contexto geopolítico: obrigações derivadas de tratados e outros instrumentos internacionais (e.g., obrigações relativas à propriedade intelectual derivadas do acordo TRIPS), políticas implementadas por outros países, especialmente aqueles que contêm nós importantes de sistemas globais de inovação em tecnologias digitais.
- Evoluções do contexto social, político, econômico e cultural: incluindo regulações relevantes, como projetos em andamento de regulação de plataformas e normas relativas à proteção de dados pessoais e segurança da informação em geral e em âmbito setorial; e o tratamento de questões relativas à soberania digital brasileira como parte de uma estratégia nacional de desenvolvimento a longo prazo.
- Evoluções na demanda: referente à formação de mercados domésticos para tecnologias desenvolvidas no país, incluindo o uso do poder de compra do Estado como força motriz do desenvolvimento tecnológico, bem como a canais de informação e retroalimentação entre atores do mercado de modo a informar trajetórias tecnológicas que se adequem às necessidades da indústria e da sociedade brasileira.

Do ponto de vista organizacional, há a necessidade de coordenação entre os atores do sistema, especialmente na execução de políticas públicas, sob a lente da soberania digital. Ou seja, que as políticas públicas relativas a cada componente da pilha de soberania digital estejam conectadas sob o objetivo estratégico da promoção da soberania digital do país. Da mesma forma, é preciso conectar e coordenar os diversos atores dos subsistemas mencionados acima neste sentido.

Na prática, isto se traduz na adoção de arranjos de governança que facilitem entendimentos compartilhados a respeito dos objetivos de política pública. Por exemplo, na adoção de uma estratégia e plano de ação relativos à Inteligência Artificial no país, é de crucial importância o seu entrecruzamento a esforços pretéritos e prospectivos de planejamento estatal, de modo que a condução

da IA no país se alinhe a documentos como o recente E-Digital 2022-2026, o Plano Nacional de Internet das Coisas, as prioridades para projetos de ciência, tecnologia e inovação do MCTI, a Estratégia Nacional de Governo Digital 2024-2027 e o plano de neindustrialização “Nova Indústria Brasil”.

Algumas ações deste último documento em missões específicas revelam algum grau de cruzamento entre prioridades de políticas públicas no sentido da promoção da soberania digital, com particular atenção à IA. Por exemplo, a consideração de demandas por tecnologias baseadas em IA do Complexo Econômico-Industrial da Saúde brasileiro e a utilização de diversas linhas de financiamento do programa Mais Inovação Brasil relacionadas a transportes, agroindústria, saúde e infraestrutura para promoção de digitalização, desenvolvimento e adoção de soluções de IA na indústria nacional⁵³.

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

3. CONSEQUÊNCIAS DA FALTA DE SOBERANIA DIGITAL

A ausência de uma configuração institucional, política e regulatória capaz de entender as dimensões da soberania digital expõe países a riscos que abrangem desde a perda de ganhos financeiros, até o eventual comprometimento de sua autonomia estratégica em dados, softwares, recursos energéticos e minerais, resultando em um esvaziamento da soberania nacional.

Isto é, ao passo que as diferentes camadas da pilha de soberania digital são desafiadas não somente de forma pontual, mas também de forma sistêmica, desenvolve-se um ciclo vicioso em que a ausência de soberania digital fragiliza fundamentos da autonomia nacional. A história recente evidenciou exemplos

⁵³ Costa; Gaspar; Johansson, 2026, em preparação para publicação

ilustrativos destes riscos concretos que vem se tornando recorrentes na sociedade brasileira e em países do sul global.

3.1 Dependência da nuvem estrangeira:

Serviços públicos e privados (como saúde, educação e finanças) tornam-se vulneráveis a falhas ou decisões unilaterais de provedores e empresas. A gestão de empresas estrangeiras sobre dados nacionais coloca usuários à mercê da lógica decisória de administradores estrangeiros, que por sua vez, obedecem a lógica de mercados competitivos. Neste sentido, eventuais decisões acerca do armazenamento e transferência de dados não necessariamente estarão em consonância com o arcabouço legal local como a LGPD (ou da GDPR, no caso de usuários europeus).

Para além de decisões mercantis, os riscos que a privacidade dos usuários já enfrentava vem sendo acelerada pela adesão de modelos de IA. Um exemplo é a popularização de sistemas de armazenamento de fotos e vídeos na nuvem, que foi acompanhada de sistemas de IA capazes de editar fotos e/ou de organizar as coleções de fotos, identificando pessoas ou locais ao longo do tempo, recorrendo a um mapeamento efetivo da biometria de usuários ao redor do mundo, que acabam aderindo a estes modelos de negócio de forma compulsória conforme são embutidos em atualizações de sistemas operacionais de smartphones.⁵⁴

Somam-se a estes riscos, a possibilidade de erros técnicos que afetam toda a cadeia de suprimentos que está utilizando serviços estrangeiros. Neste caso, o recente exemplo da CrowdStrike é latente. A empresa, referência no mercado de cibersegurança, ganhou evidência ao lançar uma atualização compulsória sem testá-la propriamente. O resultado foi o comprometimento de sistemas críticos de infraestrutura e de empresas, ocasionando um apagão cibernético global.⁵⁵

⁵⁴ DAVE, Paresh. This Website Shows How Much Google's AI Can Glean From Your Photos. **Wired**, 2 dez. 2024.

LANDYMORE, Frank. **Meta Is Being Incredibly Sketchy About Training Its AI on Your Private Photos**. Disponível em: <<https://futurism.com/meta-sketchy-training-ai-private-photos>>. Acesso em: 27 ago. 2025.

⁵⁵ BBC NEWS BRASIL. **CrowdStrike: por que empresa de segurança foi responsável por apagão cibernético global**. Disponível em: <<https://www.bbc.com/portuguese/articles/cjr4l9ndd4do>>. Acesso em: 27 ago. 2025.

Além disso, ocorrências como as revelações de Edward Snowden em 2013 demonstraram como dados são utilizados para fins políticos e estratégicos sob o viés da segurança nacional, ao evidenciarem práticas de monitoramento e espionagem de cidadãos, empresas e líderes mundiais. Na ocasião, o fato de as principais Big Techs terem seus servidores localizados no território norte americano, foi o fator fundamental que permitiu a legalidade do acesso da National Security Agency norte americana aos dados de usuários ao redor do mundo.⁵⁶

Como resultado, a ausência de alternativas autônomas e soberanas favorece a disponibilidade de dados de usuários nacionais para empresas estrangeiras que exploram estes dados conforme os seus interesses econômicos, estratégicos e/ou sujeitos às pressões dos governos de origem destas empresas.

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

Como frisamos, os dados pessoais são considerados o “recurso mais valioso do mundo” há mais de duas décadas e, para coletá-los, alguns provedores de aplicativos chegam a patrocinar taxas de acesso aos seus próprios aplicativos. Claramente, para o seletivo grupo de provedores com capacidade econômica necessária, vale a pena patrocinar taxas de acesso aos próprios aplicativos para conseguir concentrar artificialmente a atenção e consequentemente, a coleta de dados do usuário em seus aplicativos patrocinados.

Modelos de patrocínio de aplicativo ou “zero rating” surgiram no contexto de uma verdadeira “Corrida por Dados”,⁵⁷ onde os participantes do mercado lutam

CISA. **Widespread IT Outage Due to CrowdStrike Update** | CISA. Disponível em: <<https://www.cisa.gov/news-events/alerts/2024/07/19/widespread-it-outage-due-crowdstrike-update>>. Acesso em: 11 set. 2024.

⁵⁶ BELLI, Luca; GASPARI, Water B.; SINGH JASWANT, Shilpa. 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.

DEVANNY, Joe; MARTIN, Ciaran; STEVENS, Tim. On the strategic consequences of digital espionage. **Journal of Cyber Policy**, v. 6, n. 3, p. 429–450, 2 set. 2021.

MEDEIROS, Breno Pauli *et al.* O uso do ciberespaço pela administração pública na pandemia da COVID-19: diagnósticos e vulnerabilidades. **Revista de Administração Pública**, v. 54, p. 650–662, 28 ago. 2020.

⁵⁷ BELLI, L. (15 December 2017). The scramble for data and the need for network self-determination. openDemocracy.

para capturar a atenção dos usuários e, conseqüentemente, seus dados pessoais. Neste contexto, para os provedores mais abastados – tipicamente redes sociais dominantes como as aplicações do grupo Meta – vale a pena patrocinar taxas de acesso aos próprios aplicativos. Assim, os provedores de aplicativos buscam cada vez mais criar verdadeiras “adições”⁵⁸ dos próprios usuários para seus serviços, por meio de configurações de aplicativos viciantes e estratégias de mercados voltadas a manter o engajamento, partindo do pressuposto de que o aplicativo mais bem-sucedido não é aquele com os melhores recursos, mas aquele que consegue “agarrar” os usuários por mais tempo.⁵⁹ Assim, o patrocínio de aplicativos visa cada vez mais criar ou aumentar a dependência psicológica do usuário.

Particularmente, quando o acesso subsidiado a alguns aplicativos é combinado com a imposição de limites de dados muito limitados, os usuários da Internet podem ter um forte incentivo para acessar apenas aplicativos patrocinados que são apresentados e percebidos como “de graça” enquanto o acesso ao resto da Internet demora, comparativamente, extremamente caro. Este raciocínio pode ser especialmente relevante para os usuários menos abastados, que são a grande maioria dos usuários na maioria dos países, especialmente em países de renda média e baixa como o Brasil.⁶⁰ Ao patrocinar uma seleção limitada de aplicativos enquanto prevê um pagamento pelo acesso aberto à Internet, há um risco tangível de conversão da Internet, como uma rede de propósito geral, em uma rede de propósito pré-definido onde os usuários se tornam consumidores passivos, cuja atenção pode ser direcionada para serviços pré-selecionados, em vez de serem prosumidores ou seja usuários capazes também de produzir inovação e compartilhá-la livremente, para competir com os serviços já existentes.

De fato, 94,5% dos usuários de Internet móvel no país utilizam sua conexão principalmente por meio de aplicativos de mensagens instantâneas e redes sociais: é legítimo questionar se esse uso exorbitante das redes sociais

⁵⁸EYAL, N. (2014). *Hooked: How to Build Habit-Forming Products*.

⁵⁹HARRIS, T. (18 May 2016). *How Technology is Hijacking Your Mind—from a Magician and Google Design Ethicist*.

⁶⁰No Brasil, aproximadamente 80% da população faz parte das chamadas classes C, D e E, que representam os indivíduos menos ricos, de acordo com estatísticas oficiais. Embora os números mais recentes disponíveis tenham sido alterados – negativamente – pela recente pandemia de Covid-19, dados muito recentes nos permitem afirmar que 63% da população combinada das classes C, D e E autoimpõem restrições no uso da internet, para evitar o consumo da franquia mensal de dados. Veja IDEC e Instituto Locomotiva (novembro de 2021). *Barreiras e Limitações no acesso à internet e hábitos de uso e navegação na rede nas classes C, D e E*. https://idec.org.br/sites/default/files/pesquisa_locomotiva_relatorio.pdf

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

Em uma economia orientada por dados, limitar e direcionar a navegação dos usuários para pouquíssimos serviços – ou até eliminar esta necessidade ao fornecer diretamente respostas elaboradas por IA generativa – torna-se muito mais lucrativo do que deixar os indivíduos explorarem livremente a rede como desejarem e construírem novos serviços inovadores e concorrentes. O Brasil é um exemplo revelador de como a adoção generalizada de ofertas de *zero rating* tende a reduzir significativamente a abertura da internet, visto que esses planos de internet móvel direcionam e, *de fato*, restringem a experiência da internet móvel a um número limitado de aplicativos subsidiados.⁶¹ No Brasil, apenas as redes sociais dominantes – notadamente as de propriedade da Meta, como Facebook, WhatsApp e Instagram, e um número muito limitado de aplicativos que, geralmente, são integrados verticalmente com operadoras de telefonia móvel – estão incluídas em planos de zero rating.

Essa perspectiva adquire particular relevância no cenário atual, em que chatbots de IA generativa estão sendo instalados automaticamente em redes sociais patrocinadas (tipicamente o Meta.ai nas redes sociais do grupo) para fornecer respostas diretas a qualquer consulta do usuário, a fim de direcionar a atenção do internauta para o conteúdo gerado por IA, em vez de direcioná-la à página da web usada para produzir a resposta gerada por IA.

Assim, essa prática concentra a atenção e a coleta de dados de toda a população conectada nas mãos de um número muito limitado de provedores, todos partes do mesmo grupo econômico, que extraem e exportam ativos de dados extremamente valiosos – e não são tributados – ao passo que os usuários treinam seus próprios serviços. Parece importante destacar que tais práticas podem ter um enorme impacto na concorrência, na capacidade de inovar, bem como na circulação de (des)informação no país. Neste cenário,

⁶¹Para uma visão geral dos planos de classificação zero mais difundidos no mundo, consulte www.zerorating.info

cabe frisar que a concentração de debates políticos, econômicos e sociais em plataformas patrocinadas cria riscos à integridade do processo democrático e à autonomia informacional do país.⁶²

Contudo, a dependência político-social para com plataformas estrangeiras evidencia um risco imediato de manipulação da opinião pública que já foi comprovado em ocorrências recentes como o caso Cambridge Analytica em 2018. Na ocasião, a empresa britânica Cambridge Analytica fornecia serviços que eram estruturados ao redor da criação de perfis psicológicos de usuários do Facebook, a partir dos quais eram direcionadas propagandas e notícias, não necessariamente verídicas, para estes usuários. A empresa então vendia estes serviços para grupos e partidos políticos no intuito de moldar a opinião pública conforme seus interesses.⁶³

É notório como a concentração destes usuários em plataformas de redes sociais que não estavam sendo reguladas foi o fator que possibilitou a efetiva comercialização de ferramentas e estratégias para manipulação da opinião pública. Somam-se a estes outros exemplos como debates correntes acerca do uso de fake news em plataformas como o X, (antigo Twitter)⁶⁴ e tensões legais decorrentes da ausência de representantes de empresas de tecnologia no Brasil, como ocorrido com o Telegram.⁶⁵ Em um contexto em que a difusão

⁶² BELLI, L. (2023). *Soberania em Inteligência Artificial: O que é e quais facilitadores essenciais podem tornar o Brasil um país soberano em IA?* CyberBRICS. <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, L., et al. (2023). *Cibersegurança: uma visão sistêmica rumo a uma proposta de Marco Regulatório para um Brasil digitalmente soberano*. FGV.

<https://repositorio.fgv.br/items/4814c750-6b42-4d48-b8bb-302ce467b4ea>

⁶³ CONFESSORE, Nicholas. Cambridge Analytica and Facebook: The Scandal and the Fallout So Far. *The New York Times*, 4 abr. 2018. NEWTON, Casey. **Facebook suspended Donald Trump's data operations team for misusing people's personal information**. Disponível em: <https://www.theverge.com/2018/3/16/17132172/facebook-cambridge-analytica-suspended-donald-trump-strategic-communication-laboratories>. Acesso em: 21 maio. 2024.

⁶⁴ GOMES, Vitória Lopes. X terá que explicar política de privacidade polêmica de IA. *Olhar Digital*, 21 out. 2024.

GOUVEIA, Aline. **X, ex-Twitter, vai sair do Brasil? País é o 6º com mais usuários da rede**. Disponível em:

<https://www.correiobraziliense.com.br/brasil/2024/04/6835070-x-ex-twiiter-vai-sair-do-brasil-pais-e-o-6-com-mais-usuarios-da-rede.html>. Acesso em: 4 out. 2024.

MPSP apura disseminação de pornografia infantil no Twitter e Discord. MPSP - Ministério Público do Estado de São Paulo, 5 fev. 2023. Disponível em:

<https://www.mpsp.mp.br/w/mpsp-apura-dissemina%C3%A7%C3%A3o-de-pornografia-infantil-no-twitter-e-discord>. Acesso em: 9 jan. 2025

⁶⁵ BARROS, Mateus. **Justiça dá 30 dias para Telegram e Signal se adequarem às leis brasileiras. Olhar Digital**, 4 jan. 2022. Disponível em:

de IA generativa e deepfakes se tornam cada vez mais comuns, a integridade informacional e a opinião pública são postas em risco. Este risco se intensifica em momentos de polarização política e em anos eleitorais, de forma que o risco de manipulação informacional passa a incluir as próprias instituições democráticas.⁶⁶

3.3 Exposição a interrupções em cadeias de suprimento

Ao passo que países emergentes iniciam ou aceleram processos de digitalização de serviços essenciais e infraestruturas críticas, muitos se tornam dependentes de fontes estrangeiras, haja vista que estas indústrias não foram desenvolvidas de forma nativa em diversos países. Neste âmbito, nações e empresas que lideraram movimentos de digitalização por vezes exportam modelos de digitalização, cibersegurança ou de atualização de infraestruturas críticas, almejando atingir novos usuários, mercados, ou mesmo acesso a novos recursos minerais; em uma dinâmica que comumente reforça práticas de colonização digital.

Neste cenário, países emergentes comumente se encontram à mercê dos interesses e pressões das nações exportadoras de tecnologias onde acordos comerciais e de desenvolvimento são instrumentos para afirmar dominância de um sobre o outro. De forma que tensões geopolíticas podem comprometer o acesso a serviços ou a componentes de hardwares essenciais, tais como semicondutores, impactando setores estratégicos, dentre eles cibersegurança, inteligência artificial e tecnologias quânticas. Na prática, reforçando a concentração destas tecnologias nos países que as desenvolveram originalmente.

Como exemplo destas tensões, mesmo entre grandes exportadores de tecnologia como EUA e China, casos como o da Nvidia são emblemáticos da atual realidade geopolítica. No caso, a empresa Nvidia enfrenta restrições do

<<https://olhardigital.com.br/2022/04/01/internet-e-redes-sociais/justica-da-30-dias-para-telegram-e-signal-se-adequarem-as-leis-brasileiras/>>. Acesso em: 4 jan. 2025
FIGUEIREDO, Ana Luiza. **Justiça suspende Telegram por não entregar dados de neonazistas**. Disponível em: <<https://olhardigital.com.br/2023/04/26/internet-e-redes-sociais/telegram-e-suspenso-no-brasil-por-determinacao-da-justica/>>. Acesso em: 4 maio. 2025.

⁶⁶ 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. [S.l.]: Cambridge University Press, 2025.

POWER, Sam; HÜSCH, Dr Pia; ANGELIS, Emma De. **AI in the Year of Elections: A Force to be Reckoned With?** Disponível em: <<https://rusi.orghttps://rusi.org>>. Acesso em: 18 mar. 2024.

governo norte americano para comercializar seus chips H20, direcionados ao desenvolvimento e treinamento de modelos de IA na China, ilustrando como o acesso a tecnologias necessárias para processos de desenvolvimento são moldados por interesses econômicos e estratégicos.⁶⁷

Estas tensões são replicadas e intensificadas em países emergentes. No caso do Brasil, por exemplo, a já mencionada implementação do PIX ocasionou frustrações em gigantes do setor financeiro, e vem sendo tema de escrutínio pelo governo norte americano.⁶⁸ Outro exemplo que se destacou foram as tensões geopolíticas testemunhadas no Brasil e no mundo em decorrência da expansão da Digital Silk Road chinesa, onde investimentos em redes de telecomunicações e dispositivos impulsionaram a adoção de redes 5G ao redor do mundo. Esta expansão, por sua vez, foi recebida com grande resistência de gigantes de telecomunicações norte-americanas e europeias⁶⁹, inclusive colocando em risco alianças militares em função de restrições no compartilhamento de inteligência.⁷⁰

Um ponto focal da expansão das redes 5G ao redor do mundo foi a empresa chinesa Huawei. Mais recentemente, a adesão de chips para o desenvolvimento de IA vendidos pela Huawei se tornou tema central de um alerta do governo norte americano.⁷¹ Segundo a administração Trump, a compra e uso de chips da Huawei estaria em violação dos controles de exportação norte-americanos devido ao fato de que estes chips teriam sido desenvolvidos mediante acesso indevido a tecnologias norte-americanas.⁷² Não obstante as críticas norte-americanas, a Huawei recentemente abriu o

⁶⁷ SHAPER, Julia. **Nvidia navigates US-China “tightrope” in AI chip sales.** *The Hill*, 11 ago. 2025. Disponível em: <<https://thehill.com/policy/technology/5441397-nvidia-us-china-ai-chips/>>. Acesso em: 27 ago. 2025

⁶⁸ ALVIM, Mariana; GALLAS, Daniel. **Pix investigado por EUA: como Brasil defende sistema de pagamentos.** Disponível em: <<https://www.bbc.com/portuguese/articles/cm2vrnq17vdo>>. Acesso em: 27 ago. 2025.

⁶⁹ BARIFOUSE, Rafael. Por que 5G da Huawei põe Brasil em saia-justa com China e EUA. **BBC News Brasil**, 28 nov. 2019.

⁷⁰ WINTOUR, Patrick. US defence secretary warns Huawei 5G will put alliances at risk. **The Guardian**, 15 fev. 2020.

⁷¹ PHAM, Sherisse. **US move against Huawei could slow the global rollout of 5G** | *CNN Business*. Disponível em: <<https://www.cnn.com/2019/05/16/tech/huawei-us-5g-rollout>>. Acesso em: 27 ago. 2025.

⁷² SEVASTOPULO, Demetri; WU, Zijing; MCMORROW, Ryan. **US warns companies around the world to stay away from Huawei chips.** Disponível em: <<https://www.ft.com/content/2033b5b3-974d-4d40-8498-1c46d3a8db79>>. Acesso em: 27 ago. 2025.

código de seus modelos de IA em uma iniciativa para impulsionar a adesão de seus produtos no mercado internacional.⁷³

3.4. Incapacidade de entender e enfrentar à interferências estrangeiras

Dentre os exemplos mais chamativos, pode-se citar casos recentes, como a divulgação de que um gerente de políticas públicas da empresa Meta teria elaborado o documento de emenda apresentado por um deputado federal ao Projeto de Lei que discutia a proteção de crianças no ambiente digital.⁷⁴ O caso, denunciado pelo jornal Intercept Brasil, evidencia a relação de grande proximidade entre Big Techs e congressistas brasileiros, o que foi detectado por um lapso, já que o executivo esquecera de deletar os metadados do arquivo posteriormente juntado pelo parlamentar.

Além disso, tem-se o caso recente de que representantes de empresas de tecnologias estadunidenses reclamaram ao governo norte-americano do Supremo Tribunal Federal (e suas recentes decisões envolvendo as empresas) e também do método de pagamento instantâneo pix.⁷⁵ Corroborase, assim, a ideia de que as empresas estariam tentando atrair o apoio de governo estrangeiro para ajudá-las a enfrentar limitações que observam no Brasil.

Finalmente, tem-se o caso da atuação do Google que, em 2023, às vésperas da votação pela Câmara dos Deputados do Projeto de Lei conhecido como PL das Fake News, que regularia as plataformas, decidiu colocar na página principal de seu buscador um link que conduzia os internautas a um texto que

⁷³ COELHO, Cido. **Huawei abre código de modelos de IA enquanto busca adoção no mercado global. Times Brasil- Licenciado Exclusivo CNBC**, 1 jul. 2025. Disponível em: <<https://timesbrasil.com.br/empresas-e-negocios/tecnologia-e-inovacao/huawei-abre-codigo-de-modelos-de-ia-enquanto-busca-adocao-no-mercado-global/>>. Acesso em: 27 ago. 2025.

⁷⁴ DIAS, Tatiana. **Lobista da Meta criou emenda que afrouxa lei para proteger crianças na internet. Intercept Brasil**, 14 ago. 2025. Disponível em: <<https://www.intercept.com.br/2025/08/14/deputado-bolsonarista-emenda-lobista-meta-lei-criancas-internet/>>. Acesso em: 1 set. 2025.

⁷⁵ REDAÇÃO G1. **Representantes de big techs reclamam de STF, Anatel, Congresso e PIX para órgão dos EUA que investiga Brasil**. Disponível em: <<https://g1.globo.com/tecnologia/noticia/2025/08/21/representantes-de-big-techs-reclamam-de-stf-anatel-congresso-e-pix-para-orgao-dos-eua-que-investiga-brasil.ghtml>>. Acesso em: 1 set. 2025. A íntegra das manifestações pode ser obtida por meio dos seguintes links: <https://ccianet.org/wp-content/uploads/2025/08/CCIA-Comments-on-301-Investigation-into-Brazils-Digital-Trade-Barriers.pdf>; <https://www.itic.org/documents/trade/2025NationalTradeEstimateReport-ITICCommentsFinal.pdf>; <https://www.cta.tech/media/fvbjkc0u/cta-comments-on-ustr-section-301-investigation-on-brazil.pdf>. Acesso em: 1 set. 2025.

descrevia como o Projeto de Lei poderia piorar a internet dos brasileiros.⁷⁶ O episódio foi bastante relevante porque o impacto da conduta da empresa foi tão grande, que o Projeto de Lei foi retirado de pauta e nunca mais voltou a ser discutido. Importante notar, ainda, que a empresa não forneceu qualquer contraponto a visões distintas, o que acabou aumentando a repercussão do caso.

Como se pode observar, a resiliência dos países à interferência desproporcional de países e governos estrangeiros é algo difícil de se alcançar por meio de órgãos ou políticas públicas específicas, pois não se trata de espionagem, que poderia ensejar, por exemplo a invocação da ABIN ou do GSI. Trata-se, ao fim do dia, de um componente que precisa permear o tecido das discussões transversais do governo, a fim de que haja uma prontidão para responder a eventuais pressões desproporcionais, o que poderia ser alcançado, por exemplo, por meio da regulação do lobby, que, até o presente momento, não existe no Brasil.

4. CAMINHOS E SOLUÇÕES

4.1 Governança da Soberania Digital

O fortalecimento da soberania digital exige a consolidação simultânea de múltiplas camadas interdependentes, que se articulam em torno de dados, capacidade computacional, software e algoritmos, recursos energéticos e minerais, recursos humanos qualificados, mitigação de riscos de cibersegurança e resiliência à interferência estrangeira em processos internos, conforme antes mencionado. Cada uma dessas camadas demanda arranjos institucionais próprios, com estruturas e burocracias específicas destinadas ao desenvolvimento de políticas públicas.

A proteção de dados pessoais, por exemplo, possui aparato regulatório centrado na Autoridade Nacional de Proteção de Dados, enquanto a política nacional de inovação é organizada em torno da Lei 10.973/2004 e, mais

⁷⁶ RODRIGUES, Alex. **Notificada, Google retira link para texto contra PL das Fake News**. Disponível em: <<https://agenciabrasil.ebc.com.br/geral/noticia/2023-05/notificada-google-retira-link-para-texto-contr-pl-das-fake-news>>. Acesso em: 1 set. 2025. FONSECA, Bruno. **Google pagou R\$ 670 mil em anúncios contra o PL 2630. Agência Pública**, 9 maio 2023. Disponível em: <<https://apublica.org/2023/05/google-pagou-mais-de-meio-milhao-de-reais-em-anuncios-no-facebook-contr-pl-das-fake-news/>>. Acesso em: 1 set. 2025

recentemente, guiada pelo programa Nova Indústria Brasil, instituído pela Resolução CNDI/MDIC nº1/2023. Essa amplitude de camadas que compõem a soberania digital implica, assim, um aumento do número de atores e arranjos institucionais mobilizados para sua implementação.

Essas dimensões se tornam ainda mais complexas com a fragmentação interna do Estado, entendida não apenas como divisão física em órgãos, ministérios, agências e setores especializados, mas também autonomia funcional, ou seja, unidades que desenvolvem suas próprias agendas, regras internas e prioridades⁷⁷. Quando um objetivo de política pública envolve múltiplos setores, como é o caso da soberania digital, os desafios de coordenação tornam-se evidentes, pois para cada camada surgem subespaços decisórios com práticas e lógicas próprias.

Além da fragmentação estatal, é importante pontuar a inadequação do modelo tradicional hierárquico de desenvolvimento de políticas públicas, no qual a formulação e implementação das ações e iniciativas era uma prerrogativa exclusiva do Executivo e Legislativo. Atualmente, a literatura sobre governança em redes aponta para a crescente incapacidade dos recursos estatais e capacidades organizacionais alcançarem isoladamente os objetivos estabelecidos em políticas públicas complexas⁷⁸, como é o caso da soberania digital. A implementação da política pública, nesse novo paradigma, emerge de interações complexas entre uma variedade de atores estatais e não-estatais.

É nesse contexto que ganha força a noção de governança, em subsídio à ideia de capacidade estatal. Governança transcende o conceito tradicional estatal de condução de política pública e remete a formas adicionais de condução social, envolvendo múltiplos atores públicos em diferentes níveis hierárquicos. A política de soberania digital, portanto, não pode ser compreendida como um produto exclusivo da hierarquia governamental, mas como o resultado de

⁷⁷ SCHNEIDER, Volker. Redes de políticas públicas e a condução de sociedades complexas. **Civitas-Revista de Ciências Sociais**, v. 5, n. 1, p. 29-58, 2005. Disponível em: <https://doi.org/10.15448/1984-7289.2005.1.33>

⁷⁸ RHODES, Roderick Arthur William. The new governance: governing without government. **Political studies**, v. 44, n. 4, p. 652-667, 1996. Disponível em: <https://journals.sagepub.com/doi/10.1111/j.1467-9248.1996.tb01747.x>; STOKER, Gerry. Governance as theory: five propositions. *International social science journal*, v. 50, n. 155, p. 17-28, 1998; MASSARDIER, G.. Redes de Política Pública. In: **Políticas Públicas (Col.)**. Brasília: ENAP, v. 2, p. 161-186, 2007. Disponível em: http://www.enap.gov.br/index.php?option=com_docman&task=doc_view&gid=2870

interações entre diferentes instâncias da administração pública e outros atores privados.

Esse cenário aponta para a conformação de uma governança em rede, em que políticas públicas deixam de ser formuladas exclusivamente pelo Estado e passam a incorporar a participação de diversos atores da sociedade. Além disso, conforme mencionado, a própria fragmentação da Administração Pública em múltiplos centros decisórios reforça a ideia de que a governança da soberania digital depende de mecanismos de coordenação e articulação efetivos.

No atual contexto político-institucional brasileiro, são vários os atores e interesses a serem coordenados e processados em uma eventual política pública sobre soberania digital. Burocracias de diferentes níveis de governo, empresas de tecnologia, universidades e centros de pesquisa, sociedade civil etc. A próxima seção irá detalhar esses atores e suas respectivas atuações.

4.2 Principais atores na governança da soberania digital no Brasil

A governança da soberania digital no Brasil envolve uma multiplicidade de atores com diferentes papéis, interesses e capacidades. A coordenação entre esses atores é fundamental para a implementação de políticas públicas eficazes. Abaixo, são listados alguns dos atores que fazem parte dessa rede de governança para a construção da soberania digital brasileira.

Atores governamentais:

1. Autoridade Nacional de Proteção de Dados (ANPD): Criada pela Lei Geral de Proteção de Dados (Lei nº 13.709/2018), a ANPD é o órgão responsável por zelar pela proteção de dados pessoais e fiscalizar o cumprimento da LGPD no Brasil. Sua atuação é importante, vez que a proteção de dados é um pilar fundamental para a autonomia dos cidadãos e do Estado no ambiente digital. A ANPD atua na regulamentação, fiscalização e aplicação de sanções em caso de descumprimento da lei, influenciando diretamente a forma como dados são coletados, armazenados e utilizados no país.
2. Ministério da Ciência, Tecnologia e Inovação (MCTI): O MCTI desempenha um papel central no fomento à pesquisa, desenvolvimento e inovação tecnológica no Brasil. Para a soberania digital, o ministério é vital na promoção de tecnologias nacionais, no apoio a centros de pesquisa e universidades e na formulação de políticas que visem à redução da dependência tecnológica externa. Iniciativas relacionadas à inteligência artificial, computação quântica e desenvolvimento de software livre frequentemente passam por sua alçada.

3. Ministério do Desenvolvimento, Indústria, Comércio e Serviços (MDIC): O MDIC, por meio de programas como o Nova Indústria Brasil, busca fortalecer a indústria nacional, incluindo o setor de tecnologia e incluindo aspectos de soberania digital em ações de suas seis missões – e.g., sua previsão de “[d]esenvolver tecnologias da informação e da comunicação, com **domínio nacional de dados**”⁷⁹ (destaque nosso). Sua atuação é relevante para a soberania digital ao incentivar a produção local de hardware, software e serviços digitais, criando um ecossistema tecnológico robusto e menos dependente de importações. A política industrial voltada para o setor digital é essencial para a construção de capacidades tecnológicas próprias.
4. Ministério da Gestão e da Inovação em Serviços Públicos (MGI): O MGI, através da Secretaria de Governo Digital, é responsável por coordenar a transformação digital da administração pública federal. A Rede Nacional de Governo Digital (Rede GOV.BR), sob sua coordenação, busca integrar e digitalizar os serviços públicos em todos os níveis de governo. Sua atuação é fundamental para garantir que a digitalização do Estado seja feita de forma segura, eficiente e com foco na autonomia tecnológica, preferencialmente utilizando soluções nacionais e de código aberto.
5. Ministério das Comunicações (MCom): O MCom é responsável pelas políticas de telecomunicações e radiodifusão no Brasil. Sua atuação impacta a soberania digital ao definir diretrizes para a infraestrutura de conectividade, como a expansão da banda larga e o desenvolvimento de redes 5G. A garantia de uma infraestrutura de comunicação robusta e segura é um pré-requisito para a soberania digital.
6. Agência Nacional de Telecomunicações (ANATEL): A ANATEL é a agência reguladora do setor de telecomunicações no Brasil. Sua função é regulamentar, fiscalizar e outorgar serviços de telecomunicações, garantindo a competição e a qualidade dos serviços. Para a soberania digital, a ANATEL desempenha um papel crucial na regulação da infraestrutura de rede, na segurança das comunicações e na implementação de políticas que visam à universalização do acesso e à proteção dos direitos dos usuários de telecomunicações. A agência também atua na homologação de equipamentos, o que pode influenciar a adoção de tecnologias nacionais ou estrangeiras.
7. Conselho Interministerial sobre Transformação Digital (CITD): Este conselho tem como finalidade a coordenação da política industrial e digital, reunindo representantes de diversos ministérios, como Ciência e Tecnologia, Defesa, Comunicações, Educação e Economia. Sua atuação é essencial para harmonizar as ações governamentais e garantir uma abordagem integrada para a soberania digital, superando a fragmentação de políticas e promovendo a sinergia entre os diferentes órgãos.

⁷⁹ BRASIL [MDIC]. Nova Indústria Brasil: Plano de ação para a Neoindustrialização.

Conselho Nacional de Desenvolvimento Industrial, MDIC. 2024, p. 39. Disponível em: <https://www.gov.br/mdic/pt-br/composicao/se/cndi/plano-de-acao/nova-industria-brasil-plano-de-acao.pdf>

8. Ministério da Defesa: Embora não seja um ator diretamente ligado à formulação de políticas digitais civis, o Ministério da Defesa e as Forças Armadas têm um papel crucial na ciberdefesa e na proteção de infraestruturas críticas. A defesa cibernética é um componente essencial da soberania digital, garantindo a resiliência do país em face de ataques e interferências externas.
9. Congresso Nacional (Câmara dos Deputados e Senado Federal): O Poder Legislativo é responsável pela criação e revisão das leis que regem o ambiente digital, como o Marco Civil da Internet e a Lei Geral de Proteção de Dados. A atuação de parlamentares e comissões especializadas é fundamental para moldar o arranjo institucional da soberania digital, refletindo os interesses da sociedade e as necessidades do país.
10. Poder Judiciário: O Judiciário, em suas diversas instâncias, atua na interpretação e aplicação das leis digitais, resolvendo conflitos e garantindo o cumprimento dos direitos e deveres no ciberespaço. Decisões judiciais podem ter um impacto significativo na proteção de dados, na liberdade de expressão e na responsabilização de plataformas, influenciando a dinâmica da soberania digital.
11. Financiadora de Estudos e Projetos (FINEP): Vinculada ao MCTI, a FINEP é a principal agência de fomento à ciência, tecnologia e inovação no Brasil. Sua atuação é fundamental para a soberania digital ao apoiar financeiramente projetos de pesquisa e desenvolvimento em áreas estratégicas, como inteligência artificial, cibersegurança e tecnologias digitais, tanto em empresas quanto em instituições de pesquisa.
12. Conselho Nacional de Desenvolvimento Científico e Tecnológico (CNPq): Vinculado ao MCTI, o CNPq atua por meio de concessão de bolsas de pesquisa para estudantes, apoiando o desenvolvimento de projetos de pesquisa e desenvolvimento, além de promover a formação de recursos humanos qualificados em diversas áreas do conhecimento, incluindo as tecnologias digitais. Ele contribui para o fortalecimento da base científica e tecnológica nacional, essencial para a autonomia do país no ambiente digital.
13. Coordenação de Aperfeiçoamento de Pessoal de Nível Superior (CAPES): Vinculada ao Ministério da Educação (MEC), a CAPES desempenha um papel crucial no fomento à pós-graduação e na formação de recursos humanos no Brasil. Para a soberania digital, a CAPES contribui ao apoiar programas de pós-graduação em áreas de tecnologia, conceder bolsas de estudo para mestrado, doutorado e pós-doutorado, e promover a cooperação internacional em pesquisa. Sua atuação é essencial para a capacitação de profissionais que atuarão no desenvolvimento e na gestão de tecnologias digitais no país.
14. Banco Nacional de Desenvolvimento Econômico e Social (BNDES): O BNDES é o principal instrumento de financiamento de longo prazo para a realização de investimentos em todos os segmentos da economia brasileira. No contexto da soberania digital, o BNDES atua no apoio a projetos de infraestrutura digital, no financiamento de empresas de tecnologia nacionais e no desenvolvimento de cadeias produtivas ligadas ao setor, contribuindo para a autonomia tecnológica do país.

Atores da Sociedade Civil e Academia

1. Organizações da Sociedade Civil (OSCs) e Movimentos Sociais diversas entidades, movimentos sociais, pesquisadores e ativistas atuam pela defesa da autonomia tecnológica e incidência política para a construção de um Plano Nacional para Soberania Digital. Representa uma voz importante na pressão por políticas mais alinhadas aos interesses nacionais e populares. Exemplos incluem o Instituto Brasileiro de Defesa do Consumidor (Idec) e o Núcleo de Informação e Coordenação do Ponto BR (NIC.br), que, embora seja uma entidade privada sem fins lucrativos, atua em prol da internet no Brasil e hospeda o CGI.br.
2. Comitê Gestor da Internet no Brasil (CGI.br): O CGI.br é um modelo multissetorial de governança da internet no Brasil, reunindo representantes do governo, setor empresarial, terceiro setor e comunidade acadêmica e tecnológica. Sua função é estabelecer diretrizes estratégicas para o uso e desenvolvimento da internet no Brasil, promovendo princípios como a neutralidade de rede, a liberdade de expressão e a inclusão digital. O CGI.br é um espaço fundamental para o debate e a construção de consensos sobre a governança da internet, incluindo aspectos da soberania digital.
3. Empresa Brasileira de Pesquisa e Inovação Industrial (EMBRAPPI): A EMBRAPPI é uma organização social que atua por meio da cooperação com instituições de pesquisa tecnológica e empresas, para o desenvolvimento de projetos de inovação. Sua missão é apoiar a indústria brasileira na superação de desafios tecnológicos, sendo um ator relevante para a soberania digital ao fomentar a pesquisa aplicada e a inovação em tecnologias digitais, com foco na demanda do setor produtivo.

Atores do Setor Privado

1. Empresas de Tecnologia Nacionais: Empresas brasileiras de software, hardware e serviços digitais são fundamentais para a construção de uma base tecnológica própria. O fomento a essas empresas, por meio de políticas de incentivo e compras governamentais, é crucial para reduzir a dependência de fornecedores estrangeiros e fortalecer a soberania digital.
2. Grandes Empresas de Tecnologia (Big Techs): Empresas como Google, Meta, Amazon, Microsoft, entre outras, possuem um poder significativo no ambiente digital brasileiro devido à sua vasta infraestrutura, serviços e base de usuários. Embora sejam atores importantes na provisão de serviços, sua atuação também levanta preocupações sobre o controle de dados, a concorrência e a influência sobre o ecossistema digital nacional. A regulação dessas empresas é um desafio central para a soberania digital.

Todos os atores mapeados acima, em suas interações e dinâmicas, formam a rede de governança da soberania digital no Brasil. Em torno de cada política configuram-se mecanismos de coordenação, bem como espaços de negociação e decisão que reúnem diferentes atores estatais e sociais. Por

essa razão, considerando a interseção de muitos atores de forma híbrida, a combinação de elementos heterogêneos na forma de incentivos e controles (técnicos e políticos) impõe dinâmicas de interação que devem ser gerenciadas por um centro estratégico, tal como colocado por Fiani⁸⁰. A próxima subseção propõe a existência de uma estrutura para articular e coordenar essa rede de atores voltada para o desenvolvimento da soberania digital.

4.3 Instrumentos de coordenação para a soberania digital

Para promover uma abordagem de política pública guiada pela soberania digital é necessário um arranjo institucional híbrido, e considerando que ações sobre soberania digital necessitam de um agente com a capacidade de se sobrepor aos interesses individuais, considera-se que o Estado se situa em uma posição mais adequada para exercer o papel estratégico e central dessa rede de atores.

Justificando uma posição central do Estado, Ronaldo Fiani destaca três funções para os casos de desenvolvimento de ativos específicos: (i) coordenar investimentos privados para alcançar um equilíbrio superior; (ii) atuar de forma empreendedora, fornecendo uma visão de futuro; e (iii) administrar conflitos⁸¹.

A primeira função, de coordenação mostra-se importante porque em casos como infraestrutura, grandes investimentos em atividades de risco e formação de mão de obra especializada é indispensável que o Estado atue garantindo um movimento coordenado de todos os agentes envolvidos, garantindo o produto final⁸².

A segunda função, atuar de forma empreendedora, se deve a que somente o Estado pode programar as ações políticas para alcançar a soberania digital, projetando uma visão de futuro que formula novas possibilidades de

⁸⁰ FIANI, Ronaldo. **Arranjos institucionais e desenvolvimento: o papel da coordenação em estruturas híbridas**. Texto para Discussão, 2013. Disponível em: https://portalantigo.ipea.gov.br/agencia/images/stories/PDFs/TDs/td_1815.pdf

⁸¹ FIANI, Ronaldo. **Arranjos institucionais e desenvolvimento: o papel da coordenação em estruturas híbridas**. Texto para Discussão, 2013, p. 38-44. Disponível em: https://portalantigo.ipea.gov.br/agencia/images/stories/PDFs/TDs/td_1815.pdf

⁸² CHANG, H. J.; ROWTHORN, R. Entrepreneurship and conflict management. **The Role of the State in Economic Change**, p. 31-47, 1995; FIANI, Ronaldo. **Arranjos institucionais e desenvolvimento: o papel da coordenação em estruturas híbridas**. Texto para Discussão, 2013, p. 38-44. Disponível em: https://portalantigo.ipea.gov.br/agencia/images/stories/PDFs/TDs/td_1815.pdf

transformação no ecossistema digital⁸³. Ademais, o protagonismo em tecnologias digitais frequentemente envolve investimento em novas trajetórias tecnológicas, abertura e consolidação de novos mercados e, enfim, investimentos cercados de incerteza – para os quais o Estado é melhor equipado, como provedor de investimento paciente e de longo prazo⁸⁴.

Por fim, a terceira função se relaciona com as mudanças estruturais que novos programas podem ocasionar na economia, afetando o valor de ativos específicos e gerando ameaças de perda de demanda a atores que investiram no passado em determinadas atividades de ativos que envolvam o desenvolvimento da soberania. Esses atores podem criar resistências ao processo de desenvolvimento, pelo que caberia ao Estado administrar esse conflito⁸⁵.

Dessa forma, considerando a necessidade de promover a integração entre instituições públicas, níveis de governo e atores privados, entende-se que seria necessária de uma estrutura de coordenação para concertar ações, envolvendo um quadro de pessoal, regras e procedimentos próprios, vinculado à Presidência da República, que por sua posição institucional teria maior capacidade de articulação política e inserção no mais alto nível decisório do governo.

Uma estrutura enxuta facilitaria a implementação do modelo do ponto de vista orçamentário, uma vez que poderia inicialmente contar com recursos humanos requisitados de outros órgãos, sem ônus adicional, evoluindo posteriormente para a constituição de um quadro próprio, composto por servidores concursados com capacidades técnicas e políticas⁸⁶.

Para implementar políticas públicas informadas pela soberania digital, essa estrutura estatal teria à sua disposição alguns instrumentos, como (i) gestão direta, particularmente interessante quando o Estado precisa manter capacidade governamental, (ii) corporações governamentais; (iii) regulação econômica ou social; (iv) contratação; (v) assistência financeira; (vi) renúncia fiscal; (vii) impostos corretivos ou taxas, etc⁸⁷. É interessante pontuar que cada

⁸³ FIANI, Ronaldo. **Arranjos institucionais e desenvolvimento**.

⁸⁴ MAZZUCATO, Mariana. **The Entrepreneurial State**. London: Penguin, 2018.

⁸⁵ FIANI, Ronaldo. **Arranjos institucionais e desenvolvimento**.

⁸⁶ AMARAL, H. K. do. Desenvolvimento de competências de servidores na administração pública brasileira. **Revista Do Serviço Público**, 57(4), p. 549-563.

<https://doi.org/10.21874/rsp.v57i4.211>

⁸⁷ Essa tipologia é apresentada por Salamon. SALAMON, L. **The tools of government: a guide to the new governance**. Oxford University Press. 2002.

política pública ou um programa ou ação pode utilizar mais de um instrumento para sua implementação, sendo a sua escolha um ponto de atenção, pois o instrumento utilizado influencia o próprio processo de implementação da política⁸⁸, levando a aproximação ou distanciamento dos objetivos originais guiados pela soberania digital. Desenhados pelos formuladores de políticas públicas como meio de alcançar os objetivos inicialmente traçados, esses instrumentos configuram-se como uma ação estratégica do Estado.

Especificamente em se tratando de política industrial e, de forma mais ampla, da política de inovação informada pela soberania digital, pressupõe-se atuação estatal por meio de determinados instrumentos de política pública. Estes instrumentos podem atuar na oferta — voltados à construção de capacidades tecnológicas — e na demanda — destinados a reduzir riscos de mercado, guiá-lo em direções de interesse público e difundir novas tecnologias. Entre os mecanismos disponíveis estão subvenções, incentivos fiscais à P&D, financiamentos preferenciais, compras públicas, capital de risco e instrumentos de apropriabilidade. Aplicados de modo seletivo ou genérico, esses instrumentos permitem ao Estado não apenas mitigar riscos, mas também orientar trajetórias tecnológicas estratégicas. Destaca-se, nesse sentido, o papel das compras governamentais⁸⁹ como sinalizadores de demanda e indutores de escala, inovação e objetivos públicos, como sustentabilidade e eficiência energética.

Ademais, o Estado pode aplicar políticas horizontais, que abrangem a totalidade da economia (ex.: incentivos fiscais, crédito, infraestrutura, propriedade intelectual), e políticas verticais, voltadas a setores ou cadeias produtivas específicos. Um exemplo eloquente destas últimas foram as Parcerias para o Desenvolvimento Produtivo (PDPs) desenvolvidas pelo Ministério da Saúde, que se baseavam simultaneamente na demanda

⁸⁸ OLLAIK, Leila Giandoni; MEDEIROS, Janann Joslin. Instrumentos governamentais: reflexões para uma agenda de pesquisas sobre implementação de políticas públicas no Brasil. **Revista de Administração Pública**, v. 45, p. 1943-1967, 2011. Disponível em: <https://www.scielo.br/j/rap/a/W9Q8g6LXrPjkFSRj9mrVxCt/?format=pdf&lang=pt>

⁸⁹ É interessante pontuar que o poder de compra pelo poder público é um mecanismo que permite ao Estado induzir o desenvolvimento de novas tecnologias e mercado. A título de exemplo, as encomendas tecnológicas, previstas na Lei de Inovação, podem ser contratadas de forma direta pelo Estado. Isso porque a Lei de Licitações (Lei 14.133/2021) estabeleceu a inovação como um dos seus princípios norteadores (artigo 11 do diploma mencionado). Dessa forma, a lei prevê modalidades de contratação que vão além do critério menor preço, permitindo a contratação de soluções que promovam o desenvolvimento tecnológico e sustentável no país, como disposto no artigo 75 da lei citada.

observada no SUS e na necessidade de reforço da capacidade tecnológica da base produtiva nacional. É interessante notar, ainda, a criação recente do Programa de Desenvolvimento e Inovação Local (PDIL) no âmbito da Estratégia Nacional para o Desenvolvimento do Complexo Econômico-Industrial da Saúde, modalidade que “visa promover o desenvolvimento da produção e inovação locais voltados aos desafios em saúde, a sustentabilidade e resiliência do Sistema Único de Saúde (SUS) e a ampliação do acesso à saúde, a fim de reduzir a vulnerabilidade produtiva e tecnológica do SUS” (Brasil [MS], s.d.).

Essa perspectiva desloca o Estado de uma função meramente garantidora das condições de mercado para a de agente promotor e direcionador de inovações e transformações sociotécnicas. Borrás e Edler (2020) identificam múltiplos papéis estatais nesse processo, que vão do observador ao facilitador, promotor, garante e iniciador – papéis associados a intervenções transformadoras. Em linha semelhante, a abordagem do “Estado empreendedor” (Mazzucato, 2018) enfatiza políticas de inovação diretas capazes de gerar inovações radicais e difundi-las na economia.

Modelos recentes (Dosi et al., 2023) reforçam a eficácia de políticas de inovação orientadas por missão e baseadas em instituições públicas de pesquisa. A evidência sugere que políticas diretas não apenas ampliam a base de conhecimentos e oportunidades tecnológicas disponíveis, mas também induzem investimentos privados em P&D, consolidando o Estado como ator central na promoção da inovação e no fortalecimento da soberania tecnológica. Uma das intervenções de maior eficácia é a criação de institutos públicos de pesquisa associados a empresas públicas em arranjos focados em indústrias tecnologicamente avançadas (Dosi et al., 2023; Silva; Teixeira, 2011).

Estes instrumentos também podem operar sobre regimes de regulação (concorrência, comércio, propriedade intelectual, consumidor, meio ambiente) e sobre regimes de incentivos (subsídios, estímulos fiscais e financeiros). De qualquer forma, sua efetividade depende da existência de autoridades regulatórias e arranjos institucionais capazes de fiscalizar e coordenar sua implementação. Isto, associado a uma visão clara do potencial de *catch-up* tecnológico à disposição do país a partir de suas capacidades tecnológicas existentes e de janelas de oportunidade inauguradas por eventos exógenos ou endógenos (e.g., transições de paradigma tecnoeconômico ou intervenções

regulatórias) (Lee; Malerba, 2014, 2017) configura uma abordagem de política pública informada pelo ideal da soberania digital.

REFERÊNCIAS

ALVIM, Mariana; GALLAS, Daniel. **Pix investigado por EUA: como Brasil defende sistema de pagamentos.** Disponível em: <<https://www.bbc.com/portuguese/articles/cm2vrng17vdo>>. Acesso em: 27 ago. 2025.

BARIFOUSE, Rafael. Por que 5G da Huawei põe Brasil em saia-justa com China e EUA. **BBC News Brasil**, 28 nov. 2019.

BARROS, Mateus. **Justiça dá 30 dias para Telegram e Signal se adequarem às leis brasileiras.** **Olhar Digital**, 4 jan. 2022. Disponível em: <<https://olhardigital.com.br/2022/04/01/internet-e-redes-sociais/justica-da-30-dias-para-telegram-e-signal-se-adequarem-as-leis-brasileiras/>>. Acesso em: 4 jan. 2025

BBC NEWS BRASIL. **CrowdStrike: por que empresa de segurança foi responsável por apagão cibernético global.** Disponível em: <<https://www.bbc.com/portuguese/articles/cjr4l9ndd4do>>. Acesso em: 27 ago. 2025.

BELLI, L. (2023). Building Good Digital Sovereignty through Digital Public Infrastructures and Digital Commons in India and Brazil. T20 India. <https://t20ind.org/research/building-good-digital-sovereignty-through-digital-public-infrastructures/>

BELLI, L. (2023). *Da soberania digital à soberania em IA.* JOTA. <https://www.jota.info/opiniao-e-analise/columnas/ia-regulacao-democracia/da-soberania-digital-a-soberania-em-ia>

BELLI, L. (2023). *Soberania em Inteligência Artificial: O que é e quais facilitadores essenciais podem tornar o Brasil um país soberano em IA?* CyberBRICS. <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, L. (2024). *BRICS countries and AI sovereignty: Introduction to Thematic Section.* AJIC, 34, 1–6. <https://doi.org/10.23962/ajic.i34.128842>

BELLI, L. (2025). *How are BRICS countries building AI sovereignty?* AJIC, 35, 1–4. <https://doi.org/10.23962/ajic.i35.23192>

BELLI, L., et al. (2023). *Cibersegurança: uma visão sistêmica rumo a uma proposta de Marco Regulatório para um Brasil digitalmente soberano*. FGV. <https://repositorio.fgv.br/items/4814c750-6b42-4d48-b8bb-302ce467b4ea>

BELLI, Luca. **AI Meets Cybersecurity: A Brazilian Perspective**. (2024). Carnegie Endowment for International Peace., , 2024.

BELLI, Luca. **To Get Its AI Foothold, Brazil Needs to Apply the Key AI Sovereignty Enablers (KASE)**. Rochester, NY, 25 maio 2023. Disponível em: <<https://papers.ssrn.com/abstract=4465501>>. Acesso em: 21 ago. 2024

BELLI, Luca; GASPAR, Water B.; SINGH JASWANT, Shilpa. 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.

BORRÁS, Susana; EDLER, Jakob. **The roles of the state in the governance of socio-technical systems' transformation**. **Research Policy** Elsevier B.V., , 2020. Disponível em: <<https://www.scopus.com/inward/record.uri?eid=2-s2.0-85083087971&doi=10.1016%2fj.respol.2020.103971&partnerID=40&md5=ef781c4b05337ff4e9436982451ffd5d>>

BRASIL [MS]. **Programa de Desenvolvimento e Inovação Local**. Disponível em: <<https://www.gov.br/saude/pt-br/composicao/sectics/pdil/programa-de-desenvolvimento-e-inovacao-local>>. Acesso em: 28 ago. 2025.

CASSIOLATO, José Eduardo. The Brazilian System of Innovation: policy challenges. **Texto para Discussão**, TD DIT. v. 16, p. 44, 2008.

CISA. **Widespread IT Outage Due to CrowdStrike Update | CISA**. Disponível em: <<https://www.cisa.gov/news-events/alerts/2024/07/19/widespread-it-outage-due-crowdstrike-update>>. Acesso em: 11 set. 2024.

COELHO, Cido. **Huawei abre código de modelos de IA enquanto busca adoção no mercado global**. **Times Brasil- Licenciado Exclusivo CNBC**, 1 jul. 2025. Disponível em: <<https://timesbrasil.com.br/empresas-e-negocios/tecnologia-e-inovacao/huawei-abre-codigo-de-modelos-de-ia-enquanto-busca-adocao-no-mercado-global/>>. Acesso em: 27 ago. 2025

CONFESSORE, Nicholas. Cambridge Analytica and Facebook: The Scandal and the Fallout So Far. **The New York Times**, 4 abr. 2018.

COSTA, Viviane da; GASPAR, Walter Britto; JOHANSSON, Germano. Brazilian AI Sovereignty: an agenda evaluation. *In*: BELLI, Luca;

MAGALHÃES, Larissa (Orgs.). **AI Sovereignty and AI Governance: Perspectives from the BRICS and Beyond**. [S.l.: S.n.].

DAVE, Paresh. This Website Shows How Much Google's AI Can Glean From Your Photos. **Wired**, 2 dez. 2024.

DEVANNY, Joe; MARTIN, Ciaran; STEVENS, Tim. On the strategic consequences of digital espionage. **Journal of Cyber Policy**, v. 6, n. 3, p. 429–450, 2 set. 2021.

DIGWATCH TEAM. **US bans chips, quantum and AI investment in China | Digital Watch Observatory**. **DigWatch**, 11 ago. 2023. Disponível em: <<https://dig.watch/updates/us-bans-chips-quantum-and-ai-investment-in-china>>. Acesso em: 20 maio. 2024

DOSI, Giovanni *et al.* **Mission-oriented policies and the “Entrepreneurial State” at work: An agent-based exploration**. **Journal of Economic Dynamics and Control**. Elsevier B.V., 2023. Disponível em: <<https://www.scopus.com/inward/record.uri?eid=2-s2.0-85158914521&doi=10.1016%2fj.jedc.2023.104650&partnerID=40&md5=742eef327a453c5e52a37a26f948ca9a>>.

FIGUEIREDO, Ana Luiza. **Justiça suspende Telegram por não entregar dados de neonazistas**. Disponível em: <<https://olhardigital.com.br/2023/04/26/internet-e-redes-sociais/telegram-e-suspenso-no-brasil-por-determinacao-da-justica/>>. Acesso em: 4 maio. 2025.

GOMES, Vitória Lopes. X terá que explicar política de privacidade polêmica de IA. **Ohar Digital**, 21 out. 2024.

GOUVEIA, Aline. **X, ex-Twitter, vai sair do Brasil? País é o 6º com mais usuários da rede**. Disponível em: <<https://www.correiobraziliense.com.br/brasil/2024/04/6835070-x-ex-twiiter-vai-sair-do-brasil-pais-e-o-6-com-mais-usuarios-da-rede.html>>. Acesso em: 4 out. 2024.

GUZMAN, Chad de. **A Timeline of the U.S.-China Trade War During Trump's Second Term**. Disponível em: <<https://time.com/7292207/us-china-trade-war-trump-tariffs-timeline/>>. Acesso em: 15 ago. 2025.

JACKSON, Rosanna. The purpose of policy space for developing and developed countries in a changing global economic system. **Research in Globalization**, v. 3, p. 100039, 1 dez. 2021.

JIANG, M., & Belli, L. (Eds.). (2024). *Digital Sovereignty from the BRICS Countries*. Cambridge University Press. <https://www.cambridge.org/core/books/digital-sovereignty-in-the-brics-countries/27E9FD7E4579C76C8D4BA52F7670B431>

JOHANSSON NETO, G. P., Farias da Costa, V. C., & Gaspar, W. B. (2024). *Brazil's Artificial Intelligence Plan (PBIA) of 2024: Enabler of AI sovereignty?* AJIC, 34. <https://ajic.wits.ac.za/article/view/20424>

LANDYMORE, Frank. **Meta Is Being Incredibly Sketchy About Training Its AI on Your Private Photos**. Disponível em: <<https://futurism.com/meta-sketchy-training-ai-private-photos>>. Acesso em: 27 ago. 2025.

LEE, Keun; MALERBA, Franco. Catch-up cycles and changes in industrial leadership: Windows of opportunity and responses of firms and countries in the evolution of sectoral systems. **Research Policy**, v. 46, n. 2, p. 338–351, mar. 2017.

LEE, Keun; MALERBA, Franco. Changes in Industry Leadership and Catch-up by the Latecomers: Toward a theory of catch-up cycles. In: GLOBELICS CONFERENCE. **Anais...** Ankara: mar. 2014.

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

MEDEIROS, Breno Pauli *et al.* O uso do ciberespaço pela administração pública na pandemia da COVID-19: diagnósticos e vulnerabilidades. **Revista de Administração Pública**, v. 54, p. 650–662, 28 ago. 2020.

MPSP apura disseminação de pornografia infantil no Twitter e Discord. MPSP - Ministério Público do Estado de São Paulo, 5 fev. 2023. Disponível em: <<https://www.mpsp.mp.br/w/mpsp-apura-dissemina%C3%A7%C3%A3o-de-pornografia-infantil-no-twitter-e-discord>>. Acesso em: 9 jan. 2025

NEWTON, Casey. **Facebook suspended Donald Trump's data operations team for misusing people's personal information**. Disponível em: <<https://www.theverge.com/2018/3/16/17132172/facebook-cambridge-analytica-suspended-donald-trump-strategic-communication-laboratories>>. Acesso em: 21 maio. 2024.

POWER, Sam; HÜSCH, Dr Pia; ANGELIS, Emma De. **AI in the Year of Elections: A Force to be Reckoned With?** Disponível em: <<https://rusi.orghttps://rusi.org>>. Acesso em: 18 mar. 2024.

ORSI, Fabienne; CORIAT, Benjamin. The New Role and Status of Intellectual Property Rights in Contemporary Capitalism. **Competition & Change**, v. 10, n. 2, p. 162–179, jun. 2006.

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

PEREZ, Carlota. Microelectronics, long waves and world structural change: New perspectives for developing countries. **World development**, v. 13, n. 3, p. 441–463, 1985.

RIKAP, Cecilia. **Capitalism, Power and Innovation; Intellectual Monopoly Capitalism Uncovered**. London & New York: Routledge, 2021.

SEVASTOPULO, Demetri; WU, Zijing; MCMORROW, Ryan. **US warns companies around the world to stay away from Huawei chips**. Disponível em: <<https://www.ft.com/content/2033b5b3-974d-4d40-8498-1c46d3a8db79>>. Acesso em: 27 ago. 2025.

SHAPERO, Julia. **Nvidia navigates US-China “tightrope” in AI chip sales**. **The Hill**, 11 ago. 2025. Disponível em: <<https://thehill.com/policy/technology/5441397-nvidia-us-china-ai-chips/>>. Acesso em: 27 ago. 2025

SILVA, Ester G.; TEIXEIRA, Aurora A. C. **Does structure influence growth? A panel data econometric assessment of “relatively less developed” countries, 1979-2003**. **Industrial and Corporate Change** Oxford University Press, , 2011.

WINTOUR, Patrick. US defence secretary warns Huawei 5G will put alliances at risk. **The Guardian**, 15 fev. 2020.