Pre-print de: BELLI Luca, Soberania digital e Inteligência Artificial: da teoria à prática GARCIA, Eugênio V.; GERMANO, Igor (org.). Diplomacia da inovação: soberania digital e política externa brasileira. Brasília, DF: Fundação Alexandre de Gusmão, 2026.

Soberania digital e Inteligência Artificial: da teoria à prática

Luca Belli[1]

1. Introdução: A ascensão, evolução e ambiguidades da soberania digital

Na última década, o discurso jurídico internacional e o debate em torno da política tecnológica passaram a incorporar, de forma crescente, o conceito de soberania digital[2], expressão simultaneamente central e notoriamente elusiva. Aquilo que, no início dos anos 2000, se restringia a discussões acadêmicas sobre os limites jurisdicionais da Internet emergente — como exemplificado pelo caso LICRA v. Yahoo![3] — consolidou-se, progressivamente, como uma prioridade estratégica dos Estados contemporâneos. A ausência de uma definição precisa, contudo, confere ao conceito caráter ambivalente, permitindo sua utilização tanto como instrumento de proteção de interesses nacionais quanto como mecanismo de projeção geopolítica. Nesse contexto, iniciativas voltadas à soberania tecnológica e à localização de dados podem ser justificadas pela necessidade de estimular a inovação doméstica, assegurar tributação adequada de serviços digitais

[1] Doutor em Direito Público pela Université Paris-Panthéon-Assas, é professor e pesquisador da FGV Direito Rio, onde coordena o Centro de Tecnologia e Sociedade (CTS-FGV) e o projeto CyberBRICS. É membro do Conselho Consultivo do Comitê Interministerial sobre Transformação Digital, membro do Comitê Nacional sobre Cibersegurança, Diretor da edição latino-americana da conferência Computers Privacy and Data Protection, e editor da International Data Privacy Law Journal publicado pela Oxford University Press.

[2] Veja geralmente R. Avila Pinto, 'Digital Sovereignty or Digital Colonialism?' (2018) 15(27) *International Journal of Human Rights* 15; Luciano Floridi, 'The Fight for Digital Sovereignty: What It Is, and Why It Matters, Especially for the EU' (2020) 33(3) *Philosophy and Technology* 369; Julia Pohle and Thorsten Thiel, 'Digital Sovereignty' (2020) 9(4) *Internet Policy Review*; Luca Belli, 'BRICS Countries to Build Digital Sovereignty' in Luca Belli (ed), *CyberBRICS: Cybersecurity Regulations in the BRICS Countries* (Springer 2021); Luca Belli, 'Structural Power as a Critical Element of the Private Sovereignty of Digital Platforms' in Edoardo Celeste, Andreas Heldt and Clara Iglesias Keller (eds), *Constitutionalising Social Media* (Hart Publishing 2022) 81; Luca Belli, *Building Good Digital Sovereignty through Digital Public Infrastructures and Digital Commons in India and Brazil* (T20 India 2023); Luca Belli, 'To Get Its AI Foothold, Brazil Needs to Apply the Key AI Sovereignty Enablers (KASE)' in Steven Feldstein (ed), *New Digital Dilemmas: Resisting Autocrats, Navigating Geopolitics, Confronting Platforms* (Carnegie 2023); Min Jiang and Luca Belli (eds), *Digital Sovereignty from the BRICS: How the Global South and Emerging Power Alliances Are Reshaping Digital Governance* (Cambridge University Press 2024); Luca Belli et al., *Soberania Digital e Inteligência Artificial: Rumo à Autonomia Tecnológica* (Lumen Juris 2026).

[3] Yahoo*! Inc v La Ligue Contre le Racisme et l'Antisémitisme* (Tribunal de grande instance de Paris, 20 November 2000) ('*LICRA v Yahoo!*'). O caso surgiu a partir de uma ordem judicial francesa que exigia que o Yahoo! restringisse o acesso na França a memorabilia nazista hospedado em sua plataforma de leilões sediada nos EUA, e é amplamente considerado um marco inicial nos debates sobre jurisdição da internet e regulação territorial online. Veja também Joel R Reidenberg, 'Yahoo and Democracy on the Internet' (2002) 42 *Jurimetrics* 261; Luca Belli, *De la gouvernance à la régulation de l'Internet* (Berger-Levrault 2015) 219–20.

e modelos econômicos baseados em extração de dados, bem como garantir a observância da legislação nacional. Ao mesmo tempo, tais estratégias podem igualmente ser mobilizadas para fins protecionistas ou mesmo autoritários.

Apesar de sua crescente centralidade política, a soberania digital permanece marcada por elevada fluidez conceitual, em razão da inexistência de uma definição universalmente consolidada. O termo pode ser mobilizado tanto para sustentar reivindicações relacionadas ao controle individual e estatal sobre dados pessoais ou sensíveis quanto para defender o fortalecimento das capacidades nacionais de inovação tecnológica. Paralelamente, também pode servir como fundamento retórico para políticas de natureza essencialmente protecionista. Essa elasticidade conceitual constitui precisamente um dos fatores que tornam o conceito simultaneamente atrativo e problemático no plano político: ela permite aos Estados reivindicar autoridade sobre um ecossistema digital originalmente concebido para transcender fronteiras territoriais. No entanto, sob a perspectiva da teoria jurídica e da governança prática, tal ambiguidade produz desafios relevantes, uma vez que conceitos excessivamente abrangentes tendem a perder densidade analítica e precisão normativa.

Diante desse cenário, um conjunto crescente de pesquisas sobre soberania digital — campo para o qual o autor contribuiu de forma significativa – tem buscado conferir maior precisão conceitual ao tema. Nessa perspectiva, o autor define soberania digital, ou soberania em inteligência artificial (IA), como "a capacidade de compreender o funcionamento, desenvolver e regular sistemas digitais ou de IA, preservando autodeterminação, autonomia e controle sobre tais sistemas"[4]. Essa abordagem afasta interpretações fundadas em autarquia tecnológica ou isolamento digital. Em sentido diverso, sustenta que a soberania digital deve ser compreendida como uma capacidade relacional. Sob tal perspectiva, a soberania não constitui uma condição binária, suscetível de simples presença ou ausência, mas sim a capacidade de Estados e sociedades exercerem influência efetiva sobre as infraestruturas digitais e os processos de governança responsáveis por moldar seu desenvolvimento futuro.

O presente artigo sustenta que a transição da teoria para a prática exige igualmente uma mudança de enfoque: da soberania concebida apenas em termos abstratos para a soberania entendida como autonomia operacionalizada. Com esse propósito, após examinar o conceito de soberania digital, o texto reconhece a realidade da interdependência tecnológica global e propõe uma abordagem apta a lidar estrategicamente com tal condição. Em seguida, são apresentados os Facilitadores Essenciais de Soberania em Inteligência Artificial (FESIA), *framework* desenvolvido pelo autor e aqui utilizado como arcabouço conceitual para a análise da soberania em IA. O artigo também chama atenção para a emergência de práticas de "*sovereignty washing*", caracterizadas pela

[4] Veja, em particular, as obras de Luca Belli citadas na nota de rodapé n. 2.

apresentação de iniciativas potencialmente agravadoras da dependência tecnológica como expressões de "IA soberana". Por fim, propõe-se uma abordagem pentadimensional para a operacionalização da soberania digital, concebida como um processo estratégico de natureza cooperativa.

2. Conceitualizando a soberania digital e entendendo restrições estruturais

As concepções tradicionais de soberania encontram-se historicamente vinculadas ao paradigma westfaliano, estruturado em torno da autoridade territorial, da delimitação de fronteiras físicas e do exercício centralizado do poder estatal.[5] Quando transpostas para o ambiente digital, tais concepções frequentemente se traduzem na aspiração por uma independência tecnológica plena. Embora essa narrativa encontre ressonância política diante das preocupações relacionadas aos dados como recurso estratégico — frequentemente descritos como o "novo petróleo"[6] — e da concentração da infraestrutura computacional em um número reduzido de corporações predominantemente sediadas nos Estados Unidos e, crescentemente, na China, sua concretização esbarra em limitações materiais significativas. Diferentemente das fronteiras físicas, suscetíveis de controle mediante tecnologias relativamente estáveis, a infraestrutura digital constitui um ecossistema dinâmico, altamente especializado e em constante transformação.

As tecnologias digitais, embora utilizadas em escala global, não são produzidas em um único espaço geográfico, mas desenvolvidas por meio de cadeias globais de valor profundamente interdependentes, marcadas por elevados níveis de especialização e por intensos efeitos de rede. A fabricação de um semicondutor avançado, por exemplo, envolve empresas de design localizadas na Califórnia ou no Reino Unido, equipamentos de litografia produzidos na Holanda e plantas industriais instaladas em Taiwan. Nesse contexto, a pretensão de alcançar soberania tecnológica mediante isolamento produtivo desconsideraria décadas de integração econômica global e de especialização tecnológica. Isso não significa, contudo, que políticas industriais nacionais voltadas ao fortalecimento da produção doméstica de hardware sejam desnecessárias. Ao contrário, tais

[5] Samantha Besson, 'Sovereignty' in Anne Peters and Rüdiger Wolfrum (eds), *Max Planck Encyclopaedia of Public International Law* (Oxford University Press 2021).

[6] "Dados são o novo petróleo!" foi o título de uma palestra proferida pelo matemático britânico Clive Humby em 2006, em uma conferência da *Association of National Advertisers* (Associação de Anunciantes Nacionais). Em sua apresentação, Humby afirmou que os dados brutos precisam ser processados, assim como o petróleo bruto precisa ser refinado, para que passem a ter valor. A frase se tornou um ditado extremamente popular entre especialistas de políticas digitais nas últimas décadas. HUMBY, Clive; PALMER, M. **Data is the New Oil**. *In*: ANA Maestros. [S. l.], 3 nov. 2006. Disponível em: https://ana.blogs.com/maestros/2006/11/data_is_the_new.html. Acesso em: 29 mai. 2026.

políticas podem desempenhar papel relevante na diversificação e no aumento da resiliência das cadeias de suprimento estratégicas.[7]

Dinâmica semelhante se verifica nas camadas de software e inteligência artificial, em que as relações de dependência são igualmente profundas. Sistemas contemporâneos de IA dependem de bases de dados de origem global, bibliotecas de código mantidas por comunidades transnacionais e infraestruturas de computação em nuvem operadas por um número restrito de provedores globais.[8] Nessas circunstâncias, a busca por autossuficiência integral revela-se não apenas de difícil implementação, mas potencialmente contraproducente do ponto de vista econômico, na medida em que pode restringir o acesso de atores locais às tecnologias mais avançadas disponíveis.

Não obstante, os riscos econômicos, estratégicos e democráticos associados à dependência digital são substanciais e demandam respostas institucionais adequadamente estruturadas. O objetivo central não deve consistir no isolamento dos sistemas nacionais em relação às redes globais, mas na construção de condições que permitam a integração internacional sem comprometimento da capacidade decisória autônoma dos Estados. Sob essa ótica, uma dimensão altamente sensível da dependência digital reside no fato de que as infraestruturas que sustentam a transformação digital dos setores público e privado encontram-se sob o controle de agentes estrangeiros, regulados por ordenamentos jurídicos externos. A utilização de serviços de computação em nuvem, redes de comunicação e infraestruturas de dados operadas por provedores estrangeiros produz não apenas vulnerabilidades econômicas e operacionais, mas também riscos jurídicos relevantes.

Dados armazenados em infraestruturas controladas por entidades estrangeiras podem tornar-se acessíveis em razão de legislações extraterritoriais ou normas de segurança nacional editadas fora da jurisdição em que tais dados foram gerados ou processados. A legislação norte-americana, por exemplo, estabelece amplos mecanismos de acesso a dados mantidos por provedores domésticos de tecnologia, suscitando preocupações relativas à influência externa e ao controle sobre informações produzidas e armazenadas além das fronteiras territoriais dos Estados Unidos. Instrumentos normativos como a Seção 702 do Foreign Intelligence Surveillance Act (FISA), o Communications Assistance for Law Enforcement Act (CALEA) e o Clarifying Lawful Overseas Use of Data Act (CLOUD Act), nos Estados Unidos, assim como o artigo 7º da Lei de Segurança Nacional da China, exemplificam mecanismos pelos quais autoridades públicas podem compelir

[7] Luca Belli, *Soberania digital no Brasil: diagnóstico, desafios e caminhos sob a perspectiva da ciência, tecnologia e inovação* (Texto para Discussão, Observatório de Tecnologias Digitais, Ministério da Ciência, Tecnologia e Inovação 2026).
[8] Felix Richter, 'Infographic: Big Three Hold Dominant Lead in Accelerating Cloud Market' (*Statista Daily Data*, 2026) https://www.statista.com/chart/18819/worldwide-marketshare-of-leading-cloud-infrastructure-service-providers.

o acesso a comunicações, metadados e dados armazenados por provedores de serviços, inclusive quando localizados fora do território nacional.[9]

Esse tipo de arranjo compromete a previsibilidade e a efetividade de regimes nacionais de proteção de dados e de cibersegurança, fragilizando o controle sobre informações pessoais, estratégicas e comercialmente sensíveis. As implicações ultrapassam, portanto, preocupações estritamente relacionadas à privacidade, alcançando questões mais amplas de autonomia jurídica, *accountability* e supervisão democrática. Quando infraestruturas digitais críticas permanecem submetidas a sistemas jurídicos estrangeiros, Estados e empresas podem enfrentar limitações estruturais no exercício da sua capacidade operacional e de sua autoridade sobre ativos informacionais de elevado valor econômico e estratégico.[10] Em consequência, a soberania digital passa a envolver não apenas a titularidade da infraestrutura tecnológica, mas também os arranjos jurídicos e jurisdicionais por meio dos quais se exerce controle sobre ativos digitais e sobre as arquiteturas responsáveis por determinar quem pode extrair valor econômico e estratégico desses dados.[11]

Para além de sua associação tradicional com a cibersegurança, a soberania digital consolidou-se como elemento central para a geração de valor econômico de longo prazo e para a construção de resiliência estratégica. Economias contemporâneas dependem de infraestruturas digitais em múltiplas camadas, responsáveis por definir padrões de competitividade industrial e capacidade de inovação. Quando essas camadas fundamentais permanecem sob controle de atores externos, os Estados, empresas e populações inteiras tornam-se suscetíveis a formas de dependência sistêmica frequentemente descritas como "colonialismo digital".[12] Tal assimetria estrutural permite a extração de rendas econômicas, valor derivado de dados e benefícios de inovação por empresas estrangeiras, comprometendo o desenvolvimento de capacidades produtivas domésticas e reduzindo os mecanismos de reinvestimento necessários ao crescimento endógeno.

---

[9] *Foreign Intelligence Surveillance Act of 1978* (as amended by the *FISA Amendments Act of 2008*), 50 USC § 1881a; *Communications Assistance for Law Enforcement Act 1994*, 47 USC §§ 1001–1010; *Clarifying Lawful Overseas Use of Data Act 2018* (CLOUD Act), Pub L No 115–141, div V, 132 Stat 348; National People's Congress. **中华人民共和国国家情报法** [National Intelligence Law of the People's Republic of China]. Order No. 69, June 27, 2017 (amended by the Standing Committee of the National People's Congress, Dec. 29, 2018).

[10] Luca Belli, Walter Britto Gaspar and Jatinder Singh, 'Data Sovereignty and Data Transfers as Fundamental Elements of Digital Transformation: Lessons from the BRICS Countries' (2024) 54 *Computer Law & Security Review* 106017.

[11] Ibid.

[12] Renata Avila Pinto, 'Digital Sovereignty or Digital Colonialism? New Tensions of Privacy, Security and National Policies' (2018) 15(27) *SUR: International Journal on Human Rights* 15; Everisto Benyera, *The Fourth Industrial Revolution and the Recolonisation of Africa: The Coloniality of Data* (Routledge 2021); Nick Couldry and Ulises A Mejias, *The Costs of Connection: How Data Is Colonizing Human Life and Appropriating It for Capitalism* (Stanford University Press 2019); Cecilia Rikap and Bengt-Åke Lundvall, *The Digital Innovation Race: Conceptualizing the Emerging New World Order* (Palgrave Macmillan 2021).

Essa dependência também decorre, em parte, de trajetórias políticas e regulatórias que historicamente priorizaram a regulação por meio de restrições legislativas, em detrimento do uso da política industrial como ferramenta de regulação facilitadora, capaz de construir capacidades industriais e tecnológicas.[13] Embora parte da literatura enquadre a soberania digital em uma oposição binária entre protecionismo e abertura econômica, o fortalecimento estratégico de capacidades domésticas não pressupõe isolamento ou autarquia. Ao contrário, o desenvolvimento de capacidades tecnológicas nacionais deve ser compreendido como instrumento de promoção da resiliência econômica, estímulo à inovação e preservação da capacidade estrutural do Estado de influenciar seus próprios trajetos de desenvolvimento em uma economia globalizada.

Essa abordagem desloca o foco da mera titularidade para a noção de capacidade efetiva. Nem Estados nem corporações precisam deter integralmente a propriedade da infraestrutura digital para exercer soberania. O elemento central reside na capacidade jurídica, técnica e operacional de definir as regras que disciplinam o uso dessas infraestruturas e assegurar sua observância.[14] Nessa perspectiva, a soberania digital depende da possibilidade de Estados, empresas e indivíduos escolherem — e, quando necessário, substituírem — parceiros tecnológicos, estabelecerem os termos de sua integração tecnológica e garantirem a efetividade dessas condições. A ausência dessa capacidade conduz à subordinação estrutural.

3. Restrições estruturais e arquiteturas de dependência

Qualquer tentativa consistente de contextualizar a soberania digital deve partir de uma análise realista da arquitetura material da economia digital contemporânea. As camadas centrais da infraestrutura digital — especialmente aquelas relacionadas a semicondutores avançados, serviços de computação em nuvem e modelos fundacionais que sustentam sistemas avançados de inteligência artificial — encontram-se concentradas em um número reduzido de empresas e jurisdições. Tal assimetria não constitui mero resultado contingente das dinâmicas de mercado, mas decorre de vantagens acumuladas ao longo de décadas, relacionadas à elevada intensidade de capital, aos regimes de propriedade intelectual, ao acesso a mão de obra altamente qualificada e, sobretudo, ao controle sobre padrões tecnológicos e plataformas digitais.[15]

No plano do hardware, a produção de semicondutores avançados apresenta níveis excepcionais de concentração geográfica e tecnológica. Os chips necessários para o treinamento e a implementação

[13] Luca Belli, *Soberania digital no Brasil: diagnóstico, desafios e caminhos sob a perspectiva da ciência, tecnologia e inovação* (Texto para Discussão, Observatório de Tecnologias Digitais, Ministério da Ciência, Tecnologia e Inovação 2026); Luca Belli et al., *Soberania Digital e Inteligência Artificial: Rumo à Autonomia Tecnológica* (Lumen Juris 2026).
[14] *Idem.*
[15] Cecilia Rikap, *Capitalism, Power and Innovation: Intellectual Monopoly Capitalism Uncovered* (Routledge 2021).

de sistemas avançados de IA dependem de instalações de fabricação altamente especializadas, como aquelas operadas pela *Taiwan Semiconductor Manufacturing Company* (TSMC), bem como de equipamentos de litografia produzidos quase exclusivamente pela empresa holandesa ASML (*Advanced Semiconductor Materials Lithography*). Esse grau de concentração cria pontos relevantes de alavancagem geopolítica. Os controles de exportação impostos pelos Estados Unidos sobre semicondutores avançados e equipamentos de fabricação destinados a determinadas jurisdições, notadamente a China, ilustram de forma concreta como dependências tecnológicas podem ser instrumentalizadas estrategicamente.[16] Ao restringir o acesso a unidades de processamento gráfico (GPUs) de alto desempenho e a tecnologias de litografia ultravioleta extrema, tais medidas buscaram limitar o avanço das capacidades domésticas de inteligência artificial em países considerados estratégicos. Independentemente da avaliação normativa dessas políticas, sua efetividade decorre precisamente da assimetria estrutural das cadeias globais de suprimento.

As dependências associadas ao software e à infraestrutura digital são igualmente relevantes, embora frequentemente menos visíveis. Parcela substancial da infraestrutura digital global depende de serviços de computação em nuvem fornecidos por um número reduzido de empresas, em especial Amazon Web Services, Microsoft Azure e Google Cloud, responsáveis por mais de 70% do mercado global de nuvem.[17] Essas plataformas não se limitam ao fornecimento de armazenamento e capacidade computacional, mas integram ferramentas proprietárias, interfaces de programação de aplicações (APIs) e serviços de aprendizado de máquina que condicionam o desenvolvimento e a implementação de aplicações digitais. Uma vez incorporados a esses ecossistemas, os custos de migração tornam-se elevados, gerando formas de dependência simultaneamente econômicas, técnicas e regulatórias.

A disputa envolvendo o governo dos Estados Unidos e a plataforma TikTok, em 2020, fornece exemplo ilustrativo de como dependências relacionadas a plataformas digitais e serviços de software podem ser mobilizadas em disputas geopolíticas.[18] De modo semelhante, as restrições[19]

[16] Henry Farrell and Abraham L Newman, 'Weaponized Interdependence: How Global Economic Networks Shape State Coercion' (2019) 44(1) *International Security* 42.
[17] Veja Richter, 'Infographic: Big Three Hold Dominant Lead in Accelerating Cloud Market'
[18] Marianne Clausius, 'The Banning of TikTok, and the Ban of Foreign Software for National Security Purposes' (2022) 21 *Washington University Global Studies Law Review* 273.
[19] Veja Departamento do Tesouro dos EUA, Office of Foreign Assets Control, *Determination Pursuant to Section 1(a)(ii) of Executive Order 14071: Prohibition on Certain Information Technology and Software Services* (12 June 2024, effective 12 September 2024) https://ofac.treasury.gov/media/932951/download?inline. The determination prohibits the export, re-export, sale or supply to any person in the Russian Federation of '(1) information technology (IT) consultancy and design services; and (2) IT support services and cloud-based services' relating to enterprise management and design and manufacturing software https://ofac.treasury.gov/media/932951/download?inline. A determinação proíbe a exportação, reexportação, venda ou fornecimento a qualquer pessoa na Federação Russa de '(1)

impostas ao acesso russo a atualizações de software, serviços em nuvem e ferramentas de desenvolvimento após 2022 demonstram como infraestruturas digitais podem rapidamente converter-se em instrumentos de coerção econômica e política.

Mesmo ecossistemas aparentemente abertos permanecem sujeitos a formas relevantes de dependência estrutural. A ampla utilização de *frameworks* de código aberto, como TensorFlow e PyTorch, não elimina a centralidade dos atores corporativos responsáveis por sua manutenção nem a dependência de ecossistemas de hardware otimizados para seu funcionamento. Quando o acesso à infraestrutura computacional subjacente — especialmente GPUs de alto desempenho, como as produzidas pela NVIDIA — é restringido, a utilização prática desses frameworks torna-se significativamente limitada, independentemente de sua abertura formal. Nesse contexto, uma abordagem ecossistêmica das tecnologias digitais, particularmente no domínio da inteligência artificial, mostra-se indispensável para a adequada identificação de riscos e para a formulação de estratégias eficazes de contingência. As recentes restrições à exportação de chips avançados de IA, incluindo os modelos A100 e H100 da NVIDIA, evidenciam como o controle exercido na camada de hardware produz efeitos diretos sobre as possibilidades de desenvolvimento nas camadas superiores de software e modelagem.[20]

Para diversos Estados, especialmente aqueles situados no Sul Global, tais dependências em múltiplas camadas resultam em formas limitadas de participação na economia digital, comprometendo sua capacidade de regular efetivamente sistemas de inteligência artificial.[21] Dados produzidos domesticamente são frequentemente processados em infraestruturas de nuvem controladas por agentes estrangeiros, por meio de pilhas de software desenvolvidas e governadas em outras jurisdições e otimizadas para hardware submetido a controles externos. Nesse cenário, atores locais participam dos ecossistemas digitais sem, contudo, possuir capacidade significativa de influenciar sua arquitetura ou governança. O resultado ultrapassa a mera transferência de valor econômico, envolvendo limitações estruturais à autonomia, à segurança e à autodeterminação tecnológica.

Uma dimensão adicional, e crescentemente relevante, da dependência digital encontra-se nas bases materiais da própria economia tecnológica: os minerais críticos. Semicondutores avançados, baterias, infraestruturas de *data centers* e diversas tecnologias civis e militares dependem de insumos estratégicos, como terras raras, lítio, cobalto e silício de alta pureza. As cadeias globais

serviços de consultoria e design de tecnologia da informação (TI); e (2) serviços de suporte de TI e serviços baseados em nuvem relacionados à gestão empresarial e software de design e fabricação.

[20] Michael Funke and Alexander Wende, 'Modeling Semiconductor Export Restrictions and the US–China Trade Conflict' (2022) *SSRN Electronic Journal*.

[21] Luca Belli and Walter Britto Gaspar (eds), *The Quest for AI Sovereignty, Transparency and Accountability* (Springer 2025).

de extração, processamento e refino desses recursos permanecem fortemente concentradas, com papel predominante da China em diferentes etapas produtivas.[22] Tal configuração cria um vetor adicional de vulnerabilidade geopolítica, na medida em que o acesso a insumos essenciais pode ser utilizado como instrumento de pressão estratégica.

Nesse contexto, países como o Brasil ocupam posição potencialmente relevante nas cadeias globais de valor tecnológico.[23] As reservas nacionais de minerais estratégicos, incluindo terras raras e lítio, oferecem base material para uma inserção mais significativa na economia digital global. Contudo, a mera disponibilidade de recursos naturais revela-se insuficiente. Sem uma estratégia de longo prazo capaz de integrar extração mineral, processamento industrial, desenvolvimento tecnológico e governança ambiental, persiste o risco de reprodução de padrões históricos de dependência, nos quais o país permanece limitado à condição de exportador de matérias-primas. Mostra-se necessária, portanto, uma formulação estratégica orientada por investimentos em capacidade de refino, alinhamento entre política mineral e política industrial, bem como pela construção de parcerias aptas a promover transferência de conhecimento e agregação de valor tecnológico, e não apenas exploração de recursos.

Essas dinâmicas suscitam preocupações ainda mais profundas quando funções públicas essenciais — como serviços governamentais, sistemas financeiros, registros de saúde, gestão de identidade digital e até mesmo infraestrutura eleitoral — passam a depender de infraestruturas digitais controladas externamente. Nessas circunstâncias, a capacidade estatal de assegurar a aplicação de suas próprias normas jurídicas e constitucionais torna-se condicionada por infraestruturas privadas submetidas a legislações estrangeiras e políticas corporativas transnacionais. A autoridade jurisdicional pode permanecer formalmente atribuída ao Estado, mas o controle operacional efetivo passa a ser exercido de maneira mediada e contingente.[24]

Isso não significa que a interdependência tecnológica deva ou possa ser eliminada. A economia digital global é estruturalmente interconectada. O desafio consiste, antes, em compreender como essas dependências são organizadas, quais atores exercem controle sobre elas e em que termos podem ser negociadas. Sem o enfrentamento das realidades materiais associadas à concentração tecnológica e à capacidade demonstrada de instrumentalização dessas estruturas, os debates sobre soberania digital correm o risco de permanecer no plano meramente retórico, dissociados de uma formulação estratégica efetiva.

[22] Luca Belli, *Soberania digital no Brasil: diagnóstico, desafios e caminhos sob a perspectiva da ciência, tecnologia e inovação* (Texto para Discussão, Observatório de Tecnologias Digitais, Ministério da Ciência, Tecnologia e Inovação 2026).
[23] Ibid.
[24] Luca Belli et al., *Soberania Digital e Inteligência Artificial: Rumo à Autonomia Tecnológica* (Lumen Juris 2026).

4. Aplicação do Framework dos Facilitadores Essenciais de Soberania em IA (FESIA) para compreender os riscos de dependência

O crescimento da adoção da IA, bem como a ampliação de sua relevância econômica, estratégica e social, alteraram profundamente o debate sobre soberania digital. Nesse contexto, a infraestrutura digital deixa de constituir mero suporte neutro para atividades econômicas e passa a representar um espaço central de disputa política e de exercício de poder. Conforme observam Bąk et al. (2025), os conflitos contemporâneos entre plataformas digitais e Estados vêm redefinindo concepções tradicionais de soberania. O chamado "poder estrutural"[25] exercido por grandes empresas de tecnologia manifesta-se na capacidade de moldar comportamentos, controlar fluxos informacionais e extrair valor em escala por meio do desenho e da governança das infraestruturas digitais que operam.

Quando a infraestrutura subjacente à transformação digital permanece sob controle de corporações estrangeiras dominantes, tanto Estados quanto agentes privados tornam-se suscetíveis a formas significativas de bloqueio tecnológico. Na ausência de capacidades domésticas voltadas à compreensão, regulação ou desenvolvimento de alternativas tecnológicas, fornecedores externos podem progressivamente substituir competências operacionais locais. Esse déficit de soberania digital compromete não apenas a autonomia estratégica dos atores econômicos, mas também fundamentos essenciais da própria ordem democrática.

Com o objetivo de enfrentar a complexidade inerente à governança da inteligência artificial, o presente artigo adota como referência o *framework* Facilitadores Essenciais de Soberania em IA (FESIA ou KASE no original em língua inglesa), desenvolvido pelo autor em 2023 e posteriormente utilizado para mapear capacidades de soberania em IA nos países dos BRICS.[26] O modelo propõe um conjunto de dimensões analíticas interdependentes, abrangendo dados, software e modelos de IA, infraestrutura de hardware, conectividade, recursos energéticos, capital humano, capacidades de cibersegurança, marcos regulatórios e resiliência cognitiva.[27] Cada uma

[25] O conceito de 'poder estrutural' foi desenvolvido pela primeira vez por Susan Strange em *States and Markets*. Strange conceitua o poder estrutural como a capacidade de moldar os quadros dentro dos quais outros operam — determinando as condições, restrições e oportunidades que estruturam a ação. A metáfora de um labirinto é útil nesse sentido: aqueles que detêm o poder estrutural definem onde ficam as paredes, quando as portas podem se abrir ou fechar e, consequentemente, como aqueles dentro da estrutura podem se mover. Veja Susan Strange, *States and Markets* (Continuum 1988).

[26] Esse mapeamento foi realizado no âmbito do projeto CyberBRICS, sediado no Centro de Tecnologia e Sociedade da Fundação Getulio Vargas Law School do Rio de Janeiro, que foca na análise de políticas digitais em todo o grupo BRICS. Veja CyberBRICS https://cyberbrics.info

[27] Luca Belli, 'To Get Its AI Foothold, Brazil Needs to Apply the Key AI Sovereignty Enablers (KASE)' in Steven Feldstein (ed), *New Digital Dilemmas: Resisting Autocrats, Navigating Geopolitics, Confronting Platforms* (Carnegie 2023); Luca Belli, 'Exploring the Key AI Sovereignty Enablers (KASE) of Brazil, to Build an AI Sovereignty Stack' in Luca Belli and Walter Britto Gaspar (eds), *The Quest for AI Sovereignty, Transparency and Accountability* (Springer

dessas dimensões representa simultaneamente um espaço de desenvolvimento de capacidades e um potencial vetor de dependência estrutural. Assim, qualquer abordagem consistente sobre soberania em IA deve partir da identificação das formas pelas quais tais dependências se constituem e limitam a capacidade de agência dos Estados e das sociedades.

No domínio dos dados, o principal risco decorre das assimetrias de acesso, controle e apropriação econômica. Conforme anteriormente destacado, grandes volumes de dados produzidos em uma determinada jurisdição são frequentemente armazenados, processados e monetizados por plataformas estrangeiras localizadas em outras jurisdições. Essa dinâmica cria uma situação em que atores locais contribuem para a geração de valor sem participarem proporcionalmente de sua captura econômica. Além disso, a dependência de padrões proprietários e ecossistemas fechados eleva custos de migração e reduz níveis de interoperabilidade. Na ausência de mecanismos robustos de governança de dados, estes deixam de funcionar como base para inovação e desenvolvimento doméstico e passam a atuar predominantemente como instrumentos de extração de valor.[28]

As dependências relacionadas a software e modelos de IA apresentam natureza mais difusa, porém igualmente relevante. Embora a expansão de *frameworks* e modelos de código aberto (*open source*) tenha ampliado o acesso tecnológico, ela não eliminou as assimetrias estruturais existentes. Muitos desses sistemas continuam dependentes de infraestruturas, comunidades técnicas e patrocinadores corporativos sediados no exterior. Isso produz dependência não apenas em relação ao código-fonte, mas também quanto a ciclos de atualização, correções de segurança e diretrizes técnicas estabelecidas externamente. Em setores sensíveis, a opacidade de determinados modelos limita adicionalmente a capacidade estatal de auditá-los ou adaptá-los a parâmetros jurídicos e éticos locais. Desse modo, a aparente abertura tecnológica pode ocultar formas mais profundas de dependência quando inexistem capacidades domésticas suficientes para compreender, modificar e governar tais sistemas.

A infraestrutura de hardware constitui um dos pontos mais críticos de dependência estrutural. Como discutido anteriormente, a produção de semicondutores avançados e o acesso a recursos computacionais de alto desempenho permanecem concentrados em um número reduzido de empresas e jurisdições. Essa concentração expõe os Estados a riscos relacionados a interrupções de fornecimento, controles de exportação, instrumentalização geopolítica de dependências tecnológicas e volatilidade de preços. Mais do que isso, limita a capacidade de desenvolvimento

2025); Luca Belli et al., *Soberania Digital e Inteligência Artificial: Rumo à Autonomia Tecnológica* (Lumen Juris 2026).

[28] Luca Belli, Walter Britto Gaspar and Jatinder Singh, 'Data Sovereignty and Data Transfers as Fundamental Elements of Digital Transformation: Lessons from the BRICS Countries' (2024) 54 *Computer Law & Security Review* 106017.

autônomo de sistemas avançados de IA em larga escala. Nesse domínio, a soberania não pressupõe necessariamente a replicação integral da cadeia produtiva, mas exige estratégias voltadas à mitigação de vulnerabilidades, diversificação de fornecedores e posicionamento estratégico nas cadeias globais de valor.

A conectividade, frequentemente tratada como elemento neutro de inclusão digital, também pode reproduzir relações estruturais de dependência. Em diversos países do Sul Global — ressalvadas algumas exceções, como a Índia — o acesso formal à Internet não implica necessariamente participação efetiva em um ecossistema digital aberto. Em muitos casos, a conectividade é mediada por Internet móvel e modelos de *zero-rating*, nos quais aplicações específicas recebem subsídios de acesso enquanto o acesso amplo à Internet permanece limitado ou economicamente inacessível. Esse modelo favorece estruturalmente determinadas plataformas, especialmente serviços vinculados à Meta, que frequentemente integram pacotes subsidiados e incorporam crescentemente funcionalidades baseadas em IA. Em contextos de baixa disponibilidade de alternativas tecnológicas, essas plataformas tendem a converter-se na principal interface de acesso à inteligência artificial, reforçando concentração de dados, dependência tecnológica e limitações à inovação doméstica.

Os recursos energéticos e minerais estratégicos acrescentam uma dimensão frequentemente subestimada ao debate sobre soberania em IA. *Data centers*, semicondutores e sistemas de computação de alto desempenho demandam não apenas fornecimento energético estável e economicamente viável, mas também acesso contínuo a minerais críticos, como terras raras e outros insumos essenciais à infraestrutura digital avançada. Sistemas energéticos frágeis, intensivos em carbono ou dependentes externamente, assim como cadeias globais de fornecimento mineral concentradas, podem impor restrições estruturais significativas ao desenvolvimento tecnológico. A dependência de energia importada ou de cadeias minerais controladas por terceiros expõe ecossistemas digitais a disrupções, pressões geopolíticas e volatilidades de mercado fora do alcance das políticas digitais nacionais. Isso evidencia a necessidade de estratégias integradas capazes de articular políticas digitais, industriais, energéticas e minerais.[29]

O capital humano constitui, possivelmente, o elemento mais fundamental — e simultaneamente mais desigualmente distribuído — da soberania digital. A dependência nesse domínio ultrapassa a contratação de especialistas estrangeiros ou consultorias externas, refletindo também insuficiências estruturais em políticas de alfabetização digital e formação de capacidades técnicas

[29] Luca Belli, 'Exploring the Key AI Sovereignty Enablers (KASE) of Brazil, to Build an AI Sovereignty Stack' in Luca Belli and Walter B Gaspar (eds), *The Quest for AI Sovereignty, Transparency and Accountability* (Springer 2025); Luca Belli et al., *Soberania Digital e Inteligência Artificial: Rumo à Autonomia Tecnológica* (Lúmen Juris 2026); Luca Belli, *Soberania digital no Brasil: diagnóstico, desafios e caminhos sob a perspectiva da ciência, tecnologia e inovação* (Observatório de Tecnologias Digitais, Ministério da Ciência, Tecnologia e Inovação 2026).

domésticas. O desenvolvimento de uma população digitalmente qualificada é condição indispensável para assegurar que indivíduos compreendam os riscos e oportunidades associados às tecnologias digitais e participem ativamente da construção do futuro tecnológico.[30]

Na ausência desse investimento, sociedades tendem a permanecer predominantemente consumidoras de tecnologias importadas, em vez de produtoras de inovação, conhecimento e soluções tecnológicas próprias. Embora a expertise externa possa gerar ganhos de eficiência no curto prazo, dependências prolongadas tendem a inibir o desenvolvimento de capacidades endógenas e aprofundar assimetrias estruturais na produção de conhecimento. Com o tempo, isso produz ciclos de dependência tecnológica nos quais instituições e sociedades permanecem subordinadas a atores externos para funções críticas, restringindo inovação doméstica, supervisão pública e autonomia tecnológica de longo prazo.

As capacidades de cibersegurança reproduzem lógica semelhante. Muitos Estados dependem de ferramentas de segurança, inteligência de ameaças e serviços de resposta a incidentes desenvolvidos externamente. Tal dependência gera vulnerabilidades não apenas técnicas, mas também institucionais e políticas. Quando as ferramentas destinadas à proteção de infraestruturas críticas são opacas ou controladas externamente, torna-se impossível assegurar plenamente sua integridade e confiabilidade. Em um cenário no qual sistemas de IA passam a integrar domínios sensíveis, a dependência em matéria de cibersegurança adquire caráter sistêmico.

Os marcos regulatórios ocupam posição central no debate sobre soberania digital e desempenham papel indispensável na mitigação dos riscos sociais associados à inteligência artificial. Entretanto, embora a regulação seja necessária, ela não é suficiente como estratégia isolada. A mera disciplina normativa dos riscos associados à IA não é capaz de responder integralmente à complexidade, incerteza e velocidade das transformações tecnológicas contemporâneas. Uma governança efetiva exige não apenas supervisão regulatória, mas também investimento contínuo em pesquisa científica voltada à compreensão dos riscos emergentes, de seus impactos sociais e de suas implicações de longo prazo. Igualmente importante é o desenvolvimento de estratégias técnicas de mitigação e de alternativas tecnológicas mais seguras, concebidas desde os níveis de infraestrutura e design.

Sem capacidades domésticas de pesquisa e inovação, sociedades permanecem dependentes de atores externos não apenas em relação às tecnologias em si, mas também quanto ao conhecimento, metodologias e instrumentos necessários para avaliar e administrar seus riscos. A dependência regulatória emerge precisamente quando estruturas de governança passam a depender

[30] Ibid

excessivamente de padrões importados, expertise estrangeira e mecanismos de conformidade desenvolvidos em outras jurisdições. O resultado é uma forma de governança delegada, na qual existe autoridade regulatória formal, mas limitada capacidade prática de influenciar trajetórias tecnológicas e desenvolver alternativas adequadas às realidades locais.

Por fim, a resiliência cognitiva evidencia uma dimensão menos tangível, porém crescentemente relevante, da soberania digital: a capacidade de construir e preservar ambientes informacionais autônomos. No contexto da inteligência artificial, a percepção pública acerca das oportunidades e riscos tecnológicos é amplamente mediada por grandes empresas de tecnologia, cujos incentivos econômicos influenciam diretamente a construção das narrativas sobre IA. Essas empresas não apenas desenvolvem sistemas tecnológicos, mas também exercem influência significativa sobre os discursos públicos que definem os limites do debate regulatório e das expectativas sociais em torno da tecnologia.

Por meio do controle de canais de comunicação, financiamento de pesquisas, redes de especialistas e ecossistemas de plataformas digitais, esses atores podem moldar percepções sobre inevitabilidade tecnológica, necessidade econômica e aceitabilidade regulatória. Essa influência narrativa pode ser instrumentalizada para minimizar iniciativas regulatórias, enquadrar mecanismos de governança como obstáculos à inovação ou promover interpretações seletivas de benefícios e riscos alinhadas a interesses comerciais específicos. Surge, assim, uma forma de dependência epistêmica, na qual sociedades passam a depender de agentes privados economicamente interessados para definir os próprios termos pelos quais a inteligência artificial é compreendida e regulada.

O desafio, portanto, ultrapassa questões relacionadas à desinformação ou à moderação de plataformas digitais. Trata-se da capacidade de sociedades e instituições desenvolverem avaliações independentes sobre transformações tecnológicas, examinarem criticamente narrativas concorrentes e formularem estratégias regulatórias protegidas da influência concentrada de atores privados dominantes.

Em conjunto, esses facilitadores demonstram que a soberania em inteligência artificial não é comprometida por um único fator isolado, mas por uma arquitetura complexa de interdependências estruturais. Enfrentar tais vulnerabilidades não exige eliminar a interdependência — objetivo impraticável em uma economia digital globalizada —, mas compreendê-la, avaliá-la criticamente e recalibrá-la estrategicamente quando necessário. Nessa perspectiva, o *framework* KASE deve ser entendido não apenas como um mapa de capacidades a serem desenvolvidas, mas também como instrumento analítico destinado a identificar de que maneira e em quais pontos as dependências limitam a capacidade de agência tecnológica dos Estados e das sociedades.

5. Uma operacionalização pentadimensional

Para superar abordagens meramente abstratas da soberania digital e convertê-la em política pública operacionalizável, propõe-se sua decomposição em cinco dimensões estruturantes: governança, regulação, política industrial, capacitação e consciência situacional.[31]

A governança refere-se aos arranjos formais e informais por meio dos quais decisões relativas ao ambiente digital são formuladas, coordenadas e implementadas.[32] No domínio digital, o exercício efetivo da soberania exige uma abordagem multinível e multissetorial, capaz de articular diferentes atores institucionais e sociais. A participação de múltiplas partes interessadas, contudo, não deve ser compreendida como mera criação de espaços deliberativos amplos e genéricos, mas como o engajamento estratégico de atores dotados de competências e capacidades específicas, tanto na formulação quanto na implementação das soluções mais adequadas para enfrentar os diferentes Facilitadores Essenciais de Soberania em IA (FESIA).

A regulação, por sua vez, não deve ser reduzida a um conjunto de proibições ou à simples manifestação formal da autoridade estatal. Trata-se de um conjunto mais amplo de instrumentos políticos voltados à consecução de objetivos específicos e à orientação do desenvolvimento de determinados setores.[33] Os arcabouços regulatórios podem abranger normas jurídicas, padrões técnicos, incentivos econômicos, arranjos institucionais, estratégias de investimento público e arquiteturas tecnológicas concebidas para influenciar trajetórias de desenvolvimento. Nesse sentido, uma governança digital eficaz pressupõe uma concepção ampliada da regulação: não apenas como limitação normativa formal, mas como um conjunto coordenado de instrumentos destinados a moldar o desenvolvimento e a utilização de tecnologias digitais.

Nesse contexto, a política industrial assume papel particularmente relevante. Após décadas marcadas pela predominância de paradigmas neoliberais, observa-se o retorno do Estado como agente de coordenação estratégica, com a política industrial reassumindo centralidade como instrumento de desenvolvimento tecnológico e econômico. A promoção de capacidades produtivas domésticas, a redução de dependências estruturais e o fortalecimento da competitividade tecnológica passam, assim, a integrar dimensões essenciais da soberania digital contemporânea.

---

[31] Luca Belli et al, *Soberania Digital e Inteligência Artificial: Rumo à Autonomia Tecnológica* (Lúmen Juris 2026); Luca Belli, *Soberania digital no Brasil: diagnóstico, desafios e caminhos sob a perspectiva da ciência, tecnologia e inovação* (Texto para Discussão, Observatório de Tecnologias Digitais, Ministério da Ciência, Tecnologia e Inovação 2026).
[32] Luca Belli, *De la Gouvernance à la Régulation de l'Internet* (Berger-Lévrault 2015).
[33] Ibid.

O fortalecimento de capacidades constitui igualmente um dos pilares centrais de uma governança digital efetiva. Sem capacidades institucionais, técnicas e sociais adequadas, o potencial das demais dimensões da soberania digital permanece significativamente limitado. O desenvolvimento de capacidades é indispensável para a consolidação de ecossistemas de governança funcionalmente integrados, nos quais formuladores de políticas públicas, reguladores, atores econômicos, pesquisadores e organizações da sociedade civil compartilhem níveis mínimos de compreensão acerca dos sistemas tecnológicos e possam participar de processos deliberativos qualificados.

Da mesma forma, a efetividade regulatória depende não apenas da existência de autoridade formal, mas também da capacidade de compreender o funcionamento dos setores regulados, identificar dinâmicas estruturais e antecipar os impactos das transformações tecnológicas. Paralelamente, políticas industriais bem-sucedidas exigem expertise suficiente para identificar quais capacidades, infraestruturas e investimentos são necessários para promover crescimento sustentável e competitividade de longo prazo em setores estratégicos. Na ausência dessas capacidades, os processos de governança tendem a assumir caráter reativo, fragmentado e excessivamente dependente de expertise externa, reduzindo a capacidade institucional de orientar o desenvolvimento tecnológico conforme prioridades domésticas e objetivos estratégicos nacionais.

Por fim, a consciência situacional constitui elemento indispensável para o exercício da soberania digital em contextos marcados por rápidas transformações tecnológicas e geopolíticas. A velocidade das mudanças frequentemente supera a capacidade adaptativa dos mecanismos tradicionais de governança, tornando necessária não apenas a capacidade de monitorar inovações tecnológicas emergentes, alterações em estruturas de mercado e reconfigurações geopolíticas, mas também a habilidade institucional de traduzir essas informações em respostas políticas coordenadas.

A consciência situacional desempenha, assim, função integradora entre governança, regulação, política industrial e capacitação, permitindo que instituições identifiquem riscos, antecipem cenários e ajustem estratégias de maneira contínua. Importa destacar que essa capacidade não deve ser concebida como atividade episódica ou meramente reativa. Ao contrário, requer processos institucionais estruturados, voltados tanto à incorporação de conhecimentos provenientes de experiências internacionais e desenvolvimentos externos quanto à projeção internacional de conhecimentos, inovações e práticas regulatórias domésticas. Essa circulação bidirecional de conhecimento é essencial para assegurar que iniciativas nacionais permaneçam alinhadas às transformações globais, ao mesmo tempo em que contribuam para a formação de normas internacionais e para a definição de trajetórias tecnológicas.

Nesse contexto, os ministérios das relações exteriores assumem relevância crescente. Para além de suas funções diplomáticas tradicionais, passam a atuar como articuladores estratégicos de consciência situacional, conectando instituições domésticas aos processos internacionais de governança digital, monitorando transformações tecnológicas e geopolíticas emergentes e facilitando mecanismos de cooperação transnacional. Nessa função, contribuem para traduzir dinâmicas externas em insumos estratégicos capazes de orientar políticas nacionais de governança, regulação, desenvolvimento industrial e fortalecimento de capacidades tecnológicas.

6. Conclusões: Evitar a "lavagem da soberania" e reconceituar a soberania como um processo

O discurso contemporâneo sobre soberania digital caracteriza-se por elevada complexidade institucional, mas também por significativa ambiguidade conceitual. Conforme discutido anteriormente, a soberania digital possui forte densidade política e econômica, ao mesmo tempo em que permanece suficientemente aberta para sustentar interpretações distintas e, por vezes, contraditórias. Essa fluidez conceitual cria condições propícias para o fenômeno que se pode denominar "lavagem da soberania" (ou *sovereignty washing*): a utilização estratégica da linguagem da soberania para legitimar políticas, estruturas de governança ou práticas empresariais que não ampliam substancialmente a autonomia, a capacidade de agência coletiva ou as capacidades tecnológicas de uma sociedade.

A questão transcende o plano meramente terminológico. Reivindicações associadas à soberania digital influenciam crescentemente estratégias industriais, estruturas de mercado, decisões de investimento público e modelos regulatórios, tornando essencial distinguir iniciativas efetivamente voltadas ao fortalecimento da autonomia tecnológica daquelas que apenas se apropriam de sua retórica. Políticas que preservam ineficiências estruturais, restringem o acesso à inovação ou aprofundam mecanismos de bloqueio tecnológico podem ser apresentadas sob o rótulo de "soberania digital", embora, na prática, enfraqueçam a autonomia ao elevar custos, reduzir competitividade e limitar a capacidade adaptativa de longo prazo.

De forma semelhante, o discurso da soberania pode ser instrumentalizado para justificar mecanismos amplos de controle estatal sobre ambientes informacionais, frequentemente sob argumentos relacionados à proteção cultural, à segurança nacional ou à integridade do espaço digital. Tais abordagens correm o risco de substituir processos participativos e formas distribuídas de agência por estruturas excessivamente centralizadas de controle, restringindo a inovação, limitando o acesso ao conhecimento e comprometendo a legitimidade democrática. Nesse contexto, revela-se necessário adotar postura analiticamente crítica em relação a iniciativas qualificadas como "soberanas", examinando seu conteúdo material e seus efeitos concretos, em vez de simplesmente aceitar a terminologia utilizada.

Essas distorções tornam-se particularmente relevantes nos ambientes informacionais contemporâneos, nos quais a soberania é disputada não apenas no plano da infraestrutura tecnológica, mas também no âmbito das narrativas e da produção de conhecimento. Grandes empresas de inteligência artificial e plataformas digitais exercem influência significativa sobre a construção de discursos públicos relacionados a riscos tecnológicos, oportunidades econômicas e prioridades regulatórias. Em razão de seus interesses econômicos substanciais, tais atores possuem incentivos claros para moldar percepções de formuladores de políticas públicas e usuários, enquadrando debates sobre adoção tecnológica e regulação de maneira compatível com seus objetivos comerciais.

Nesse cenário, a resiliência cognitiva emerge como componente essencial da própria soberania digital. Sociedades incapazes de avaliar criticamente informações, identificar mecanismos de manipulação narrativa e preservar confiança institucional tornam-se vulneráveis não apenas em termos tecnológicos, mas também sob a perspectiva informacional e psicológica. A soberania, portanto, passa igualmente pela capacidade coletiva de compreender criticamente os processos de construção discursiva associados às tecnologias digitais.

É nesse contexto que a consciência situacional, discutida anteriormente, assume papel central. No âmbito da governança digital, essa capacidade envolve a identificação de dependências tecnológicas, o reconhecimento de novas formas de concentração econômica e influência política, a compreensão das transformações nas estruturas de mercado e a antecipação de riscos sistêmicos emergentes. A consciência situacional atua, assim, como elemento integrador entre governança, regulação, política industrial e fortalecimento de capacidades. Na ausência dessa capacidade analítica, intervenções regulatórias podem tornar-se obsoletas, políticas industriais podem inadvertidamente reproduzir dependências existentes e estruturas de governança podem revelar-se incapazes de responder à velocidade das transformações tecnológicas.

Importa destacar que a consciência situacional não pode permanecer restrita às instituições estatais. O exercício efetivo da soberania digital requer formas distribuídas de conhecimento e monitoramento envolvendo reguladores, comunidades técnicas, setor privado, academia, sociedade civil e redes internacionais de cooperação. Essa perspectiva reflete o entendimento de que a soberania digital não pode ser alcançada exclusivamente por meio da atuação isolada do Estado ou da simples coordenação de mercado. Processos multissetoriais estruturados desempenham papel fundamental na agregação de expertise distribuída, na identificação de pontos cegos institucionais, na mitigação de riscos de captura regulatória e na construção de mecanismos adaptativos de governança aptos a lidar com a crescente complexidade tecnológica.

Igualmente relevante é o desenvolvimento de capacidades diplomáticas dotadas de alfabetização tecnológica, capazes de expandir a consciência situacional para além do contexto doméstico e atuar como instrumentos de articulação estratégica das capacidades nacionais em ambientes internacionais. A soberania digital desenvolve-se cada vez mais em arenas transnacionais de governança, fóruns de padronização técnica e contextos geopolíticos complexos. Nesse sentido, a diplomacia assume função que ultrapassa a representação tradicional do Estado, convertendo-se em mecanismo essencial para monitoramento de transformações globais, antecipação de dependências externas e participação ativa na formulação de normas internacionais.

Essas dinâmicas evidenciam uma compreensão mais ampla da soberania digital. Trata-se menos de uma condição estática a ser alcançada do que de um processo contínuo de calibração, adaptação e negociação. Em ambientes digitais, a soberania exige equilíbrio permanente entre autonomia e interdependência, abertura e controle, prioridades nacionais e dinâmicas globais.

As dimensões de governança, regulação, política industrial, capacitação e consciência situacional oferecem os fundamentos institucionais para esse processo. Sua efetividade, contudo, depende de sistemas mais amplos de coordenação, aprendizado institucional e adaptação contínua. Nessa perspectiva, a soberania digital não reside no isolamento nem em afirmações meramente simbólicas de controle, mas na construção de capacidade estratégica duradoura: a aptidão de sociedades e instituições para compreender transformações tecnológicas, orientar seu desenvolvimento conforme valores democraticamente definidos, cooperar de maneira estratégica e preservar mecanismos de supervisão democrática em ecossistemas digitais crescentemente complexos.

Bibliografia

AVILA PINTO Renata, ‘Digital Sovereignty or Digital Colonialism? New Tensions of Privacy, Security and National Policies’ (2018) 15(27) *SUR: International Journal on Human Rights* 15.

BELLI Luca and GASPAR Walter Britto (eds), *The Quest for AI Sovereignty, Transparency and Accountability* (Springer Nature 2025).

BELLI Luca and others, *Soberania Digital e Inteligência Artificial no Brasil: Rumo à Autonomia Tecnológica* (Lumen Juris 2026).

BELLI Luca, ‘BRICS Countries and AI Sovereignty: Introduction to Thematic Section’ (2024) 34 *African Journal of Information and Communication (AJIC)* 1.

BELLI Luca, *Building Good Digital Sovereignty through Digital Public Infrastructures and Digital Commons in India and Brazil* (T20 India 2023).

BELLI Luca, *De la gouvernance à la régulation de l'Internet* (Berger-Levrault 2015).

BELLI Luca, GASPAR Walter Britto and SINGH JS, 'Data Sovereignty and Data Transfers as Fundamental Elements of Digital Transformation: Lessons from the BRICS Countries' (2024) 54 *Computer Law & Security Review* 106017.

BELLI Luca, 'Net Neutrality, Zero Rating and the Minitelisation of the Internet' (2017) 2(1) *Journal of Cyber Policy* 96.

BELLI Luca, *Soberania digital no Brasil: diagnóstico, desafios e caminhos sob a perspectiva da ciência, tecnologia e inovação* (Texto para Discussão, Observatório de Tecnologias Digitais, Ministério da Ciência, Tecnologia e Inovação 2026).

BELLI Luca, 'Structural Power as a Critical Element of the Private Sovereignty of Digital Platforms' in Edoardo Celeste, Andreas Heldt and Clara Iglesias Keller (eds), *Constitutionalising Social Media* (Hart Publishing 2022) 81.

BELLI Luca, 'To Get Its AI Foothold, Brazil Needs to Apply the Key AI Sovereignty Enablers (KASE)' in FELDSTEIN S (ed), *New Digital Dilemmas: Resisting Autocrats, Navigating Geopolitics, Confronting Platforms* (Carnegie 2023).

BENYERA Everisto, *The Fourth Industrial Revolution and the Recolonisation of Africa: The Coloniality of Data*(Routledge 2021).

CASSIOLATO José Eduardo, 'The Brazilian System of Innovation Policy Challenges' (2008) 16 *Discussion Paper TD DIT* 44.

CLAUSIUS Marianne, 'The Banning of TikTok, and the Ban of Foreign Software for National Security Purposes' (2022) 21 *Washington University Global Studies Law Review* 273.

COHEN Julie E, *Between Truth and Power: The Legal Constructions of Informational Capitalism* (Oxford University Press 2019).

COULDRY Nick and MEJIAS Ulises A, *The Costs of Connection: How Data Is Colonizing Human Life and Appropriating It for Capitalism* (Stanford University Press 2019).

DOSI Giovanni and others, 'Mission-Oriented Policies and the "Entrepreneurial State" at Work: An Agent-Based Exploration' (2023) *Journal of Economic Dynamics and Control*.

FARRELL Henry and NEWMAN Abraham L, 'Weaponized Interdependence: How Global Economic Networks Shape State Coercion' (2019) 44(1) *International Security* 42.

FLORIDI Luciano, 'The Fight for Digital Sovereignty: What It Is, and Why It Matters, Especially for the EU' (2020) 33(3) *Philosophy and Technology* 369.

FUNKE Michael and WENDE Alexander, 'Modeling Semiconductor Export Restrictions and the US–China Trade Conflict' (2022) *SSRN Electronic Journal*.

JIANG Min and BELLI Luca (eds), *Digital Sovereignty from the BRICS: How the Global South and Emerging Power Alliances Are Reshaping Digital Governance* (Cambridge University Press 2024).

LESSIG Lawrence, *Code: And Other Laws of Cyberspace* (Basic Books 1999).

MAZZUCATO Mariana, *The Entrepreneurial State* (Penguin 2018).

OWCZAREK, Michał; WŁOCH, Renata. The Power of Digital Infrastructure: How Conflicts between Platforms and States Redefine Sovereignty? Athenaeum Polskie Studia Politologiczne, [S. l.], v. 88, p. 92-115, jan. 2025. DOI: 10.15804/athena.2025.88.05.

POHLE Julia and THIEL Thorsten, 'Digital Sovereignty' (2020) 9(4) *Internet Policy Review*.

REIDENBERG Joel R, 'Yahoo and Democracy on the Internet' (2002) 42 *Jurimetrics* 261.

RICHTER Felix, 'Infographic: Big Three Hold Dominant Lead in Accelerating Cloud Market' (Statista Daily Data 2026).

RIKAP Cecilia, *Capitalism, Power and Innovation: Intellectual Monopoly Capitalism Uncovered* (Routledge 2021).

STRANGE Susan, *States and Markets* (Continuum 1988).