GEOECONOMIA DAS TECNOLOGIAS CRÍTICAS: AUDITABILIDADE, REVERSIBILIDADE E INTEROPERABILIDADE COMO CRITÉRIOS DE AUTONOMIA ESTRATÉGICA NO BRASIL

Fabio Elissandro Cassimiro Ramos[1]
Stefani Juliana Vogel[2]

Resumo: Este artigo examina como a geoeconomia das tecnologias críticas se manifesta no Brasil através de dependências pós-aquisição que transcendem a origem do fornecedor. Argumenta-se que autonomia estratégica em infraestruturas críticas, como defesa, segurança pública, energia e telecomunicações, não é função da compra isolada, mas da capacidade estatal de governar o ciclo de vida tecnológico por meio de três critérios operacionais: auditabilidade, que significa conhecer e inspecionar sistemas; reversibilidade, que implica migrar dados e trocar fornecedores; e interoperabilidade, que envolve integrar com ecossistemas nacionais. Mediante análise institucional comparada de marcos regulatórios brasileiros, norte-americanos, europeus e multilaterais sobre governança de inteligência artificial, cibersegurança, dados e contratações estratégicas, o artigo identifica lacunas críticas em exigibilidade transversal de governança pós-aquisição. O diagnóstico revela que a dependência funcional, fenômeno de longo prazo após entrega formal, é tão relevante quanto a dependência inicial e frequentemente mais duradoura e menos visível em estatísticas de comércio. Propõem-se seis medidas de política contratual e institucional para reduzir vulnerabilidades estruturais em tecnologias críticas.

---

[1] Doutorando em Estado de Direito e Governança Global pela Universidade de Salamanca, Mestre em Ciências de Segurança e Defesa Interamericana pelo Colégio Interamericano de Defesa, Mestre em Segurança Internacional pela Universidade Carlos III de Madri. Especialista em Altos Estudos de Defesa pela Escola Superior de Defesa. E-mail: fabiocassimiro@usal.es. ORCID: 0000-0003-2324-0624.

[2] Doutoranda em Estado de Direito e Governança Global pela Universidade de Salamanca, Mestre em Segurança Internacional pela Universidade Carlos III de Madri, certificada em proteção de dados pessoais pela Associação Internacional de Privacidade (IAPP), ex-presidente suplente do Conselho Nacional de Proteção de Dados Pessoais (CNPD) e especialista em cibersegurança, inteligência artificial e proteção de dados. E-mail: stefani.vogel@usal.es. ORCID: 0000-0003-4239-7248.

Palavras-chave: Geoeconomia. Tecnologias Críticas. Autonomia Estratégica. Ciclo de Vida. Auditabilidade. Reversibilidade. Interoperabilidade. Brasil.

Abstract: This article examines how geoeconomic vulnerabilities in critical technologies manifest in Brazil through post-acquisition dependencies that exceed supplier nationality concerns. It argues that strategic autonomy in critical infrastructure, including defense, public security, energy, and telecommunications, is not a function of isolated procurement but of state capacity to govern technological lifecycle through three operational criteria: auditability, which means inspecting and verifying systems; reversibility, which implies migrating data and switching suppliers; and interoperability, which involves integrating with national ecosystems. Through institutional and comparative analysis of regulatory frameworks from Brazil, the United States, Europe, and multilateral organizations regarding artificial intelligence governance, cybersecurity, data, and strategic procurement, the article identifies critical gaps in cross-cutting post-acquisition governance enforceability. The diagnosis reveals that functional dependency, a long-term phenomenon after formal delivery, is as consequential as initial procurement dependency and often more durable and less visible in trade statistics. Six policy measures regarding contracting and institutional governance are proposed to reduce structural vulnerabilities in critical technology systems.

Keywords: Geoeconomics. Critical Technologies. Strategic Autonomy. Lifecycle Governance. Auditability. Reversibility. Interoperability. Brazil.

1. Introdução

Em outubro de 2022, o Bureau of Industry and Security dos Estados Unidos impôs restrições à exportação de semicondutores avançados e unidades de processamento gráfico para a China, alegando proteção da segurança nacional.[3] A medida, posteriormente reforçada por atualizações regulatórias em 2023 e 2024, não constituiu apenas ato comercial isolado, mas sinalizou a normalização de instrumentos

[3] BUREAU OF INDUSTRY AND SECURITY. Implementation of Additional Export Controls: Certain Advanced Computing and Semiconductor Manufacturing Items; Supercomputer and Semiconductor End Use; Entity List Modification. Federal Register, 13 out. 2022.

geoeconômicos como controles de exportação, triagem de investimentos, sanções tecnológicas e condicionamento de acesso a cadeias críticas.[4]

Esse movimento revela uma transformação estrutural nas relações internacionais: tecnologias digitais deixaram de ser mercadorias convencionais e passaram a funcionar como infraestruturas de poder. Semicondutores, inteligência artificial (IA), dados e infraestrutura computacional configuram novos pontos de estrangulamento geoeconômico.[5]

Para países de poder médio como o Brasil, a inserção em cadeias globais de semicondutores, infraestrutura computacional avançada, modelos fundacionais de IA, sensores complexos e sistemas digitais críticos não implica vulnerabilidade inevitável, mas amplia a exposição a fornecedores, padrões técnicos, restrições externas, controles de exportação, choques tecnológicos e reconfigurações geopolíticas.

Assim, a vulnerabilidade brasileira não reside simplesmente na aquisição de tecnologia estrangeira, mas na incorporação e operação de sistemas críticos sem capacidade institucional suficiente para auditá-los, integrá-los, atualizá-los, adaptá-los ou substituí-los ao longo do tempo. Trata-se, neste artigo, de hipótese documentalmente situada: não se pretende demonstrar empiricamente toda a dependência tecnológica brasileira, mas examinar como a baixa exigibilidade pública de auditabilidade, reversibilidade, interoperabilidade, governança de dados e validação independente pode ampliar riscos de dependência pós-aquisição em tecnologias críticas.

A configuração contemporânea do poder internacional também deixou de ser definida apenas por arsenais convencionais, mobilização militar clássica ou volume de comércio exterior. Cada vez mais, a soberania estatal depende da capacidade de processar, proteger, interpretar, auditar e acionar dados em ecossistemas tecnológicos complexos. Essa leitura dialoga com a literatura recente sobre *new*

---

[4] Id. Implementation of Additional Export Controls: Certain Advanced Computing Items; Supercomputer and Semiconductor End Use; Updates and Corrections. Federal Register, 25 out. 2023; Id. Commerce strengthens export controls to restrict China's capability to produce advanced semiconductors for military applications. Washington, DC: U.S. Department of Commerce, 2024.

[5] EUROPEAN UNION. Regulation (EU) 2023/1781 of the European Parliament and of the Council of 13 September 2023 establishing a framework of measures for strengthening Europe's semiconductor ecosystem and amending Regulation (EU) 2021/694 (Chips Act). Official Journal of the European Union, 2023.

economic statecraft[6], especialmente quanto ao uso estratégico de instrumentos econômicos, tecnológicos e regulatórios em disputas por cadeias críticas e aos dilemas enfrentados por potências médias.[7]

Essa transformação afeta diretamente o comércio internacional: tecnologias antes tratadas como bens ou serviços de alto valor agregado passaram a operar como pontos de estrangulamento geoeconômico. O acesso diferenciado a chips avançados, modelos de IA, sistemas de comunicação segura, sensores, nuvem e softwares embarcados pode condicionar a capacidade estatal de modernizar a defesa, proteger infraestruturas críticas, responder a crises e preservar autonomia estratégica.

Nesse contexto, este artigo propõe deslocar a análise da aquisição para a capacidade: a questão decisiva não é apenas de quem o Brasil compra, mas em que medida consegue operar, auditar, adaptar, manter, integrar e substituir aquilo que incorpora. Em sistemas baseados em IA, software, sensores, dados e conectividade, a entrega formal não encerra a dependência; frequentemente inaugura vínculo prolongado com fornecedor, arquitetura técnica, padrões proprietários, infraestrutura de dados, atualizações e manutenção.

A discussão torna-se mais relevante diante de infraestruturas críticas e serviços essenciais, dependentes de tecnologias digitais integradas, como sensores, sistemas de supervisão industrial, plataformas de georreferenciamento, comunicações críticas, softwares analíticos, IA, *data centers*, nuvem, drones, radares, plataformas de comando e controle e sistemas de reconhecimento de padrões. Por serem tecnologias de uso dual ou múltiplo, aplicáveis à defesa, segurança pública, vigilância de fronteiras, monitoramento ambiental, proteção energética, segurança portuária, resposta a desastres e continuidade de serviços essenciais, sua aquisição não constitui ato administrativo neutro.

À luz da literatura sobre compras militares brasileiras, este artigo parte do diagnóstico de que aquisições estratégicas formam capacidades, inserção internacional e dependência tecnológica, mas desloca o foco da geoeconomia da aquisição para a geoeconomia da operação. O argumento central é que a dependência pós-aquisição, persistente após

---

[6] Segundo Aggarwal e Reddie (2025), *new economic statecraft* designa o uso estratégico de instrumentos econômicos, tecnológicos e regulatórios para objetivos de poder estatal, especialmente em disputas envolvendo tecnologias críticas.

[7] AGGARWAL, Vinod K.; REDDIE, Andrew W. New economic statecraft and global technology conflicts: the dilemma for middle powers. Business and Politics, 2025.

a incorporação formal do sistema, pode ser tão relevante quanto a dependência da compra inicial e, frequentemente, mais duradoura.

A pergunta de pesquisa é: em que medida lacunas de governança do ciclo de vida em sistemas de inteligência artificial e tecnologias críticas de uso dual aumentam o risco de que aquisições brasileiras de defesa, segurança pública e proteção de infraestruturas críticas se convertam em dependências pós-aquisição?

A hipótese central é que a autonomia estratégica em tecnologias críticas não pode ser aferida apenas pelo volume de aquisições, nacionalidade do fornecedor, transferência formal de tecnologia ou incorporação de equipamentos avançados. Ela designa a capacidade estatal de operar, auditar, adaptar, integrar e substituir sistemas críticos sem dependência determinante de fornecedor único, preservando continuidade operacional, controle sobre dados sensíveis e possibilidade real de saída. Assim, sem auditabilidade, reversibilidade, interoperabilidade, soberania de dados, documentação técnica, validação independente e supervisão humana qualificada, a contratação estratégica pode converter-se em vetor de vulnerabilidade, obsolescência precoce e dependência funcional.

O objetivo geral é analisar criticamente a dependência pós-aquisição em sistemas de IA e tecnologias críticas aplicadas à defesa, à segurança pública e às infraestruturas críticas brasileiras. Especificamente, busca-se distinguir aquisição tecnológica, transferência de tecnologia e capacidade operacional efetiva; examinar a geoeconomia das infraestruturas críticas como extensão do comércio internacional de tecnologias sensíveis; identificar camadas de dependência pós-aquisição em sistemas digitais críticos; discutir o problema da última milha em IA aplicada a ambientes críticos; avaliar riscos da fragmentação institucional entre defesa, segurança pública e infraestrutura crítica; e propor parâmetros de governança contratual e institucional para reduzir dependências duradouras.

O artigo organiza-se em sete seções: introdução, método, geoeconomia tecnológica, dependência pós-aquisição, caso brasileiro e comparação internacional, discussão com proposições institucionais e conclusão. Essa passagem da aquisição para a operação será retomada na Seção 4, após a análise das múltiplas camadas da geoeconomia contemporânea: aquisição, operação, dados, substituição e norma.

2. Método e estratégia analítica

Este estudo é qualitativo e analítico-comparativo. Como não produz dados primários nem pretende medir causalidade estatística, sua estratégia metodológica fundamenta-se na análise institucional crítica, compreendida como abordagem voltada a identificar como regras formais, arranjos organizacionais, incentivos, capacidades estatais e relações de poder condicionam resultados de governança. A ênfase recai sobre mecanismos institucionais que transformam decisões de contratação tecnológica em dependências operacionais, informacionais, contratuais e comerciais ao longo do tempo, em diálogo com a tradição institucionalista e com abordagens críticas de análise institucional.[8]

A análise foi conduzida por revisão bibliográfica interdisciplinar, exame documental e comparação institucional, abrangendo documentos normativos, políticas públicas, estratégias nacionais, relatórios governamentais, documentos doutrinários, instrumentos regulatórios e publicações institucionais sobre governança de IA, defesa, segurança pública, soberania digital, cibersegurança, infraestruturas críticas e comércio internacional de tecnologias sensíveis.

No contexto brasileiro, o *corpus* inclui marcos de defesa e contratação pública, especialmente a Lei nº 12.598/2012 e a Lei nº 14.133/2021; marcos de segurança pública, como a Lei nº 13.675/2018, que institui o SUSP, e o Decreto nº 10.822/2021, que institui o Plano Nacional de Segurança Pública e Defesa Social 2021-2030;[9] marcos de infraestruturas críticas, cibersegurança e dados, incluindo os Decretos nº 9.573/2018, 10.569/2020, 11.200/2022, 10.222/2020, 11.856/2023 e 12.573/2025, além da Lei nº 13.709/2018; e sistemas de informação,

---

[8] NORTH, Douglass C. Institutions, Institutional Change and Economic Performance. Cambridge: Cambridge University Press, 1990; OSTROM, Elinor. Background on the Institutional Analysis and Development Framework. Policy Studies Journal, v. 39, n. 1, p. 7-27, 2011; COLE, Daniel H. Laws, norms, and the Institutional Analysis and Development Framework. Journal of Institutional Economics, v. 13, n. 4, p. 829-847, 2017; WHALEY, Luke. The critical institutional analysis and development framework. International Journal of the Commons, v. 12, n. 2, p. 137-161, 2018.

[9] BRASIL. Lei nº 13.675, de 11 de junho de 2018. Institui o Sistema Único de Segurança Pública (SUSP) e cria a Política Nacional de Segurança Pública e Defesa Social. Brasília, DF: Presidência da República, 2018; BRASIL. Decreto nº 10.822, de 28 de setembro de 2021. Institui o Plano Nacional de Segurança Pública e Defesa Social 2021-2030. Brasília, DF: Presidência da República, 2021.

como o Sinesp e dados públicos do Ministério da Justiça e Segurança Pública.[10]

O *corpus* internacional compreende documentos da OTAN e da OCDE sobre IA responsável; regulações europeias sobre IA, semicondutores, governança e acesso a dados; instrumentos norte-americanos de controle de exportação em semicondutores e computação avançada; a estratégia de IA responsável do Departamento de Defesa dos Estados Unidos; os *frameworks* NIST AI RMF 1.0 e NIST AI RMF *Generative AI Profile*; e padrões ISO/IEC pertinentes, especialmente ISO/IEC 42001:2023 e ISO/IEC 23894:2023, relativos à gestão de riscos e a sistemas de gestão de IA.[11]

A comparação internacional é qualitativa, exploratória e heurística, sem finalidade ranqueadora ou pretensão de mensuração estatística. A matriz organiza evidência documental pública sobre cinco dimensões diretamente relacionadas à pergunta de pesquisa: auditabilidade técnica, reversibilidade contratual, interoperabilidade tecnológica, soberania, residência e portabilidade de dados, e validação independente. Suas classificações indicam densidade documental e exigibilidade pública, não capacidade real, desempenho operacional ou maturidade tecnológica total.

A estratégia aproxima-se do método comparado de Lijphart[12] e da comparação estruturada e focada de George e Bennett,[13] ao empregar critérios previamente definidos para examinar modelos distintos e identificar padrões institucionais relevantes. Para evitar falsa equivalência institucional e restringir a análise ao *corpus* primário auditável, foram selecionadas três jurisdições com documentação pública diretamente citável, Estados Unidos, União Europeia e Brasil, além da OTAN como

---

[10] MINISTÉRIO DA JUSTIÇA E SEGURANÇA PÚBLICA. Sinesp: Sistema Nacional de Informações de Segurança Pública. Brasília, DF: MJSP, 2026.

[11] INTERNATIONAL ORGANIZATION FOR STANDARDIZATION; INTERNATIONAL ELECTROTECHNICAL COMMISSION. ISO/IEC 42001:2023: artificial intelligence management system. Geneva: ISO, 2023; INTERNATIONAL ORGANIZATION FOR STANDARDIZATION; INTERNATIONAL ELECTROTECHNICAL COMMISSION. ISO/IEC 23894:2023: artificial intelligence: guidance on risk management. Geneva: ISO, 2023.

[12] LIJPHART, Arend. Comparative politics and the comparative method. American Political Science Review, v. 65, n. 3, p. 682-693, 1971.

[13] GEORGE, Alexander L.; BENNETT, Andrew. Case Studies and Theory Development in the Social Sciences. Cambridge, MA: MIT Press, 2005.

regime multilateral de referência. A OCDE é utilizada apenas como *benchmark* normativo geral de IA responsável, sem entrada própria na matriz, por não exercer exigibilidade direta sobre contratações nacionais.

Nesse desenho, o institucionalismo explica como regras, incentivos e capacidades condicionam trajetórias de dependência; o método comparado estrutura a análise entre modelos documentais; e a governança de IA e tecnologias críticas fornece parâmetros técnicos adicionais, extraídos de *frameworks* de gestão de risco, padrões de sistemas de gestão de IA, regras de dados e mecanismos de validação independente.

A seleção distingue jurisdições soberanas e regime multilateral: Estados Unidos e União Europeia foram mantidos por oferecerem, respectivamente, matriz técnico-institucional de gestão de risco e modelo regulatório de alto risco para IA; o Brasil constitui o caso principal; e a OTAN figura apenas como referência técnico-doutrinária em IA responsável, interoperabilidade e TEV&V[14] em defesa.

Os documentos foram analisados segundo cinco dimensões institucionais: auditoria técnica; reversibilidade contratual; interoperabilidade tecnológica; soberania, residência e portabilidade de dados; e validação técnica. Essas dimensões correspondem às principais camadas de manifestação da dependência pós-aquisição em sistemas digitais críticos. O Quadro 1 apresenta a matriz de codificação documental adotada para reduzir arbitrariedade e assegurar rastreabilidade entre argumento, indicador e fonte documental.

Para fins de transparência metodológica, a matriz ampliada de evidências documentais utilizada na análise é apresentada no Apêndice A.

[14] *Test, Evaluation, Verification and Validation*: conjunto de processos de teste, avaliação, verificação e validação de sistemas, especialmente em contexto de defesa e inteligência artificial.

Quadro 1 – Estratégia de codificação documental

Dimensão	Pergunta operacional	Indicadores de codificação	Fonte de verificação
Auditabilidade	O marco normativo ou contrato exige inspeção técnica?	"auditoria"; "logs"; "documentação técnica"; "testes independentes"; "certificação"	Lei 14.133/2021; NIST AI RMF 1.0; ISO/IEC 23894
Reversibilidade	Há previsão de saída, migração de dados ou suporte pós-rescisão?	"reversão"; "migração"; "transição"; "plano de saída"; "suporte pós--contrato"	Lei 14.133/2021; ISO/IEC 23894; Data Act e AI Act como benchmarks
Interoperabilidade	O marco exige padrões abertos ou APIs documentadas?	"padrão aberto"; "API"; "integração"; "formato portável"; "compatibilidade"	Lei 14.133/2021; Sinesp; ePING; padrões técnicos
Soberania de dados	Há regras de residência, acesso, portabilidade ou exclusão?	"território nacional"; "residência"; "portabilidade"; "propriedade"; "exclusão"; "criptografia"	Decreto 12.573/2025; LGPD; Data Act; AI Act
Validação	Há exigência de teste independente pré ou pós--implantação?	"validação"; "teste"; "certificação"; "laboratório"; "robustez"; "avaliação contextual"	NIST AI RMF Generative AI Profile; ISO/IEC 23894

Fonte: Elaboração dos autores (2026), com base nos marcos documentais citados.

Para fins de verificabilidade, a análise examinou: (a) o conjunto de legislação federal selecionado como central para defesa, licitações, segurança pública, infraestruturas críticas, cibersegurança e proteção de dados; e (b) os marcos internacionais citados, incluindo NIST AI RMF 1.0, NIST AI RMF *Generative AI Profile*, ISO/IEC 42001:2023, ISO/IEC 23894:2023, *AI Act, Data Governance Act*, *Data Act*, estratégia de IA responsável do *Department of Defense* (DoD), estratégias da OTAN e recomendações da OCDE sobre IA. A análise não inclui documentação sigilosa, contratos classificados, dados proprietários de órgãos de defesa ou práticas operacionais não documentadas em marcos públicos.

A codificação documental foi conduzida por dimensão e por modelo analisado. Para cada dimensão, foram identificados: (i) dispositivo normativo ou diretriz técnica aplicável; (ii) presença ou ausência de obrigação verificável; (iii) existência de mecanismo de fiscalização, validação, certificação ou auditoria; e (iv) evidência pública de institucionalização. A classificação "densidade forte" foi atribuída apenas quando os três indicadores estavam simultaneamente presentes;

"lacuna parcial" quando havia um ou dois indicadores; e "lacuna crítica" quando não havia indicador integrado ou exigível. A classificação não mede desempenho operacional real, mas densidade documental pública e exigibilidade formal.

As categorias utilizadas indicam apenas o grau em que a documentação pública examinada torna visíveis, exigíveis e rastreáveis requisitos de governança pós-aquisição. Não devem ser interpretadas como diagnóstico definitivo de maturidade tecnológica, desempenho operacional, capacidade efetiva ou inexistência de práticas institucionais internas. A referência ao PNCP é meramente contextual e não constitui base amostral, estatística ou empírica deste artigo.

O estudo possui limitações relevantes. Primeira, trabalha predominantemente com documentos públicos, impedindo avaliar integralmente contratos sigilosos, aquisições classificadas ou práticas internas de órgãos de defesa e operadores privados de infraestrutura crítica; a análise revela limites de transparência e exigibilidade, sem autorizar conclusão sobre inexistência de práticas internas. Segunda, a comparação internacional enfrenta assimetria de transparência entre jurisdições democráticas, regimes híbridos e regimes opacos. Terceira, a análise centra-se em marcos normativos e documentais, não em implementação operacional real. Quarta, o artigo não afirma que toda tecnologia estrangeira seja indesejável nem que autonomia equivalha a autossuficiência absoluta; o objeto é identificar quando a baixa exigibilidade de governança converte dependência tecnológica estrutural em vulnerabilidade estratégica evitável. Quinta, a tese é defensável apenas com aquilo que é publicamente verificável.

3. Geoeconomia tecnológica e comércio internacional de sistemas críticos

Edward Luttwak cunhou o termo geoeconomia para designar a substituição parcial da competição militar direta por instrumentos econômicos de poder.[15] Diante da centralidade das tecnologias digitais, porém, o conceito precisa abranger não apenas tarifas, sanções e instrumentos financeiros, mas também o controle de cadeias produtivas críticas, padrões técnicos, infraestrutura computacional, semicondutores, dados, algoritmos, plataformas digitais, sistemas de comunicação e capacidades de IA. Essa

[15] LUTTWAK, Edward N. From geopolitics to geo-economics: logic of conflict, grammar of commerce. The National Interest, n. 20, p. 17-23, 1990.

transformação altera a lógica do comércio internacional: tecnologias críticas, antes tratadas sobretudo como bens ou serviços de alto valor agregado, passaram a ser avaliadas por sua função estratégica, pois certos bens, serviços e infraestruturas tornaram-se condições de funcionamento do Estado, da defesa, da segurança pública, da economia e da vida social.[16] Assim, o comércio internacional de tecnologias críticas converte-se em espaço de disputa por capacidade estatal.

Semicondutores, IA, dados e infraestrutura computacional configuram novos pontos de estrangulamento geoeconômico, pois o controle sobre chips avançados, modelos de IA, *data centers*, nuvem, sensores, sistemas operacionais, redes de comunicação e padrões de interoperabilidade pode influenciar a capacidade de outros Estados de modernizar a defesa, proteger infraestruturas críticas, desenvolver indústria nacional e responder a crises. Nesse contexto, a dependência tecnológica não é apenas econômica, mas também operacional, institucional e política.

A literatura sobre interdependência convertida em instrumento de poder ajuda a explicar esse fenômeno: redes globais, inicialmente justificadas por eficiência, podem tornar-se mecanismos de coerção quando atores específicos controlam nós centrais.[17] No campo tecnológico, esses nós incluem fabricantes de semicondutores, provedores de nuvem, sistemas operacionais, satélites, plataformas de IA, cibersegurança, integradores de sistemas e padrões proprietários, cuja dependência se torna especialmente problemática quando projetada sobre defesa, segurança pública e infraestruturas críticas.

Sob perspectiva institucionalista, dependências tecnológicas tendem a reproduzir-se quando regras, incentivos e capacidades permanecem inalterados ao longo do tempo. O conceito de *path dependence*[18] é útil nesse ponto: decisões iniciais de contratação, padrões

---

[16] BABIĆ, Milan; DE GRAAFF, Nana; LINSI, Lukas; WEINHARDT, Clara. The geoeconomic turn in international trade, investment, and technology. Politics and Governance, v. 12, 2024; RUCK, Jan. A geoeconomic fix? European industrial policy on semiconductors amidst global competition. JCMS: Journal of Common Market Studies, v. 64, n. 2, p. 742-761, 2026.

[17] FARRELL, Henry; NEWMAN, Abraham L. Weaponized interdependence: how global economic networks shape state coercion. International Security, v. 44, n. 1, p. 42-79, 2019.

[18] Em North (1990), *path dependence* (dependência de trajetória) designa o processo pelo qual escolhas institucionais anteriores condicionam alternativas futuras,

técnicos escolhidos, fornecedores selecionados e arquiteturas adotadas podem elevar custos de mudança e restringir alternativas futuras.[19] Em sistemas digitais críticos, o *lock-in*[20] não surge apenas de cláusulas contratuais. Ele também decorre da integração com bases de dados, treinamento de pessoal, rotinas administrativas, protocolos operacionais e dependência de atualizações proprietárias.

A geoeconomia tecnológica opera em cinco camadas interdependentes: aquisição, definida por fornecedor, condições, restrições e regime de exportação; operação relativa à manutenção, atualização, correção, calibração e integração dos sistemas; dados, envolvendo armazenamento, acesso, processamento, exportação e histórico operacional; substituição, referente à capacidade estatal de trocar fornecedores sem perda crítica; e norma, composta por instituições, contratos e padrões capazes de limitar dependências. A principal contribuição deste artigo situa-se justamente na passagem da aquisição para a operação: em sistemas de IA e infraestrutura crítica, a dependência mais sensível pode surgir após a compra, na manutenção, no suporte, no treinamento, na auditoria, na conectividade, na atualização, na interoperabilidade e na impossibilidade de saída.

Esse diagnóstico não nega a relevância do comércio internacional nem da cooperação tecnológica. Países de poder médio dificilmente alcançarão autossuficiência completa em semicondutores, nuvem, sensores avançados, modelos fundacionais ou plataformas de IA. O ponto central não é a origem estrangeira da tecnologia, mas a ausência de uma arquitetura de governança capaz de preservar capacidade decisória, continuidade operacional, segurança de dados e possibilidade real de substituição. Se a geoeconomia tecnológica transforma mercados em infraestruturas de poder, as infraestruturas críticas tornam esse deslocamento imediatamente operacional, pois nelas as dependências digitais deixam de ser abstratas e passam a afetar continuidade, segurança e capacidade estatal.

---

limitando mudanças e reforçando padrões estabelecidos.

[19] NORTH, op. cit.; OSTROM, op. cit.; COLE, op. cit.

[20] Aprisionamento tecnológico: situação em que custos de mudança, efeitos de rede e compatibilidades acumuladas tornam economicamente inviável a substituição de um fornecedor ou sistema. O fenômeno é associado à economia de redes e à análise de dependência de trajetória (NORTH, 1990; OSTROM, 2011; COLE, 2017)

3.1. Infraestruturas críticas como nova fronteira da dependência geoeconômica

Infraestruturas críticas assumiram centralidade geoeconômica porque deixaram de constituir apenas problema de segurança doméstica e passaram a integrar disputas internacionais por capacidade estatal. Energia, telecomunicações, transportes, portos, aeroportos, sistemas financeiros, abastecimento de água, saneamento, saúde, logística, produção e distribuição de alimentos, serviços digitais, *data centers* e estruturas de resposta a emergências compõem esse universo, em linha com a evolução normativa brasileira sobre segurança de infraestruturas críticas.[21] Sua relevância decorre de três fatores: indispensabilidade à continuidade do Estado e da economia; dependência crescente de tecnologias digitais, sensores, software, conectividade e IA; e inserção dessas tecnologias em cadeias globais concentradas, sujeitas a restrições comerciais, disputas geopolíticas, controles de exportação, sanções, falhas de suprimento e dependência de fornecedores estrangeiros. A combinação desses elementos transforma infraestruturas críticas em pontos de vulnerabilidade geoeconômica.

A digitalização deslocou o centro da vulnerabilidade dessas infraestruturas. A proteção física de instalações, a continuidade operacional e a resposta à sabotagem material permanecem relevantes, mas foram ampliadas por riscos digitais. Sistemas elétricos dependem de sensores, controle industrial, comunicação segura, software de supervisão, proteção cibernética e recuperação; portos dependem de plataformas logísticas, rastreamento, controle de acesso, comunicações, integração alfandegária e bancos de dados; hospitais dependem de prontuários eletrônicos, redes, equipamentos conectados, sistemas de gestão, fornecedores de software e segurança de dados. A cadeia de vulnerabilidade tornou-se, portanto, dupla: física e digital, material e informacional.

A inteligência artificial aprofunda a centralidade geoeconômica das infraestruturas críticas ao apoiar manutenção preditiva, detecção de fraudes, gestão de tráfego, monitoramento de fronteiras, análise de

---

[21] BRASIL. Decreto nº 9.573, de 22 de novembro de 2018. Aprova a Política Nacional de Segurança de Infraestruturas Críticas. Brasília, DF: Presidência da República, 2018; BRASIL. Decreto nº 10.569, de 9 de dezembro de 2020. Aprova a Estratégia Nacional de Segurança de Infraestruturas Críticas. Brasília, DF: Presidência da República, 2020; BRASIL. Decreto nº 11.200, de 15 de setembro de 2022. Aprova o Plano Nacional de Segurança de Infraestruturas Críticas. Brasília, DF: Presidência da República, 2022.

imagens, priorização de alertas, reconhecimento de padrões, segurança portuária, vigilância territorial, resposta a desastres e coordenação de crises. Contudo, sua incorporação também introduz opacidade algorítmica, assimetria informacional, dependência de dados, necessidade de treinamento contínuo, risco de viés, vulnerabilidade adversarial e dificuldade de auditoria. Em infraestruturas críticas, tais riscos têm efeitos sistêmicos, pois uma falha algorítmica pode comprometer não apenas a eficiência de um serviço, mas a continuidade de funções essenciais.

A natureza dual ou múltipla dessas tecnologias torna inadequada uma política de compras fragmentada. Drones, plataformas de comando e controle e sistemas de reconhecimento de padrões podem atravessar defesa, segurança pública, defesa civil, monitoramento ambiental, energia, portos, inteligência, logística e resposta a crises, gerando dependências comuns entre setores distintos. Quando cada órgão contrata sistemas próprios sem matriz nacional de interoperabilidade, padrões mínimos de auditabilidade, cláusulas de soberania de dados e plano de reversibilidade, o Estado pode produzir modernização aparente e vulnerabilidade real, expressa em sistemas incompatíveis, bases isoladas, fornecedores recorrentes, protocolos proprietários, custos crescentes de manutenção e incapacidade de coordenação em crises.

O problema agrava-se porque infraestruturas críticas combinam atores públicos e privados, incluindo concessionárias, permissionárias, entidades reguladas e arranjos híbridos. Assim, a dependência pós-aquisição não se limita à contratação pública direta, mas também se manifesta em concessões, regulação setorial, exigências de segurança, padrões técnicos, auditorias regulatórias, obrigações de continuidade, gestão de riscos e coordenação entre Estado e operadores privados. Por isso, a pergunta relevante não é apenas quem comprou a tecnologia, mas que função estratégica ela desempenha, quais dados processa, de quais fornecedores depende, como é atualizada, onde está hospedada, quem pode auditá-la, quais padrões utiliza, se é interoperável com sistemas nacionais e se pode ser substituída sem colapso funcional. A contratação deixa de ser evento isolado e passa a constituir decisão estrutural sobre a resiliência estatal, deslocando o foco da titularidade formal do ativo para o ciclo de vida efetivamente governado. É nesse ponto que a dependência pós-aquisição se torna categoria analítica própria.

4. Dependência pós-aquisição: conceito, dimensões críticas e matriz analítica

A dependência pós-aquisição é distinta, embora relacionada, ao *lock-in* tecnológico. Enquanto o *lock-in* descreve o aprisionamento decorrente de custos de mudança, efeitos de rede, compatibilidades acumuladas e dependência de trajetória, a dependência pós-aquisição é aqui tratada como categoria de governança pública: identifica vínculos técnicos, contratuais, informacionais e operacionais que persistem após a incorporação formal de sistemas críticos e podem ser mitigados por desenho contratual, capacidade regulatória, interoperabilidade, auditabilidade, portabilidade de dados e validação independente.

Essa dimensão da geoeconomia tecnológica raramente aparece nas estatísticas de comércio exterior, no valor global do contrato ou na entrega formal do sistema. Radares, drones, sensores, sistemas de vigilância, plataformas de comando, softwares analíticos ou soluções de IA podem integrar o patrimônio público ou ativos de concessionárias e, ainda assim, permanecer condicionados a licenças, atualizações proprietárias, suporte remoto, documentação incompleta, infraestrutura externa, interfaces fechadas ou ausência de auditoria independente. Para fins analíticos, o Quadro 2 organiza essa dependência em sete dimensões críticas, evidenciando como a vulnerabilidade pós-aquisição se materializa ao longo do ciclo de vida de tecnologias críticas.

Quadro 2 – Dimensões críticas da dependência pós-aquisição em tecnologias críticas

Dimensão Crítica	Elementos Abrangidos	Risco em Infraestruturas
1. Hardware	Semicondutores, sensores, componentes críticos	Indisponibilidade de peças; obsolescência sem substitutos
2. Software	Código-fonte, sistemas operacionais, firmware	Impossibilidade de auditoria; dependência de atualizações proprietárias
3. Dados	Treinamento, logs, históricos operacionais	Perda de controle sobre ativos informacionais sensíveis
4. Conectividade/Nuvem	Infraestrutura de rede, data centers, APIs	Dependência de fornecedor externo; riscos de interrupção
5. Interoperabilidade	Padrões abertos, integração com sistemas nacionais	Isolamento funcional; incapacidade de coordenação em crises
6. Manutenção/Suporte	Patches, atualizações, calibração contínua	Vulnerabilidades não mitigadas; degradação de capacidade
7. Reversibilidade	Possibilidade de substituição, migração de dados	Aprisionamento contratual; impossibilidade de saída

Fonte: Elaboração dos autores (2026).

A leitura do Quadro 2 evidencia que a dependência pós-aquisição não se limita ao fornecedor inicial nem ao equipamento adquirido, mas se distribui por camadas técnicas, informacionais, operacionais e contratuais que condicionam a autonomia estatal ao longo do tempo. Por isso, sua mitigação exige governança desde a contratação, tratando documentação técnica, auditabilidade, soberania de dados, interoperabilidade, manutenção controlada e reversibilidade como requisitos de capacidade estatal, e não como elementos acessórios do contrato.

4.1. Sistemas de IA e o problema da última milha

A inteligência artificial é frequentemente apresentada como tecnologia de ruptura, mas sua utilidade estratégica raramente se realiza no ato da aquisição. Entre a disponibilidade formal da solução e sua conversão em capacidade institucional efetiva há uma "última milha": etapa sociotécnica que exige dados adequados, conectividade, operadores treinados, fluxos claros, integração com sistemas legados, segurança cibernética, governança de falhas, validação contínua, contestação

humana, monitoramento pós-implantação e resposta institucional a falhas.[22]

Em defesa, segurança pública e infraestruturas críticas, o problema não é a ausência de tecnologia, mas sua conversão em capacidade útil sob pressão, em ambientes incompletos, ruidosos, adversariais e juridicamente sensíveis, nos quais dados fragmentados, falhas de conectividade, baixa confiança do operador, tempo decisório reduzido e premissas automatizadas invisíveis podem comprometer a utilidade operacional. Nas infraestruturas críticas, esse risco é agravado por sistemas legados, contratos acumulados, fornecedores distintos, exigência de continuidade e possibilidade de manipulação adversarial. Por isso, compras públicas devem privilegiar inovação, integração, validação contextual e capacidade efetiva, não apenas a aquisição formal de soluções tecnológicas.[23]

A validação contextual é especialmente relevante porque sistemas de IA desenvolvidos, treinados ou calibrados em outros países podem refletir dados, idiomas, padrões de infraestrutura, doutrinas operacionais, regimes jurídicos e níveis de conectividade distintos dos brasileiros, afetando acurácia, robustez, falsos positivos, explicabilidade, supervisão humana e confiabilidade operacional. Assim, a aquisição de IA deve ser acompanhada de testes locais, cenários simulados, validação operacional, avaliação de robustez e revisão periódica.[24] A supervisão humana, por sua vez, precisa ser real, e não simbólica: manter um "humano no circuito"[25] não basta se ele não dispõe de tempo, treinamento, autoridade, informação e condições institucionais para contestar a recomendação automatizada.

Nesse sentido, o GenAI.mil[26] deve ser tratado apenas como ilustração institucional documentada por fonte primária: seu lançamento

---

[22] SCHARRE, Paul. Four Battlegrounds: Power in the Age of Artificial Intelligence. New York: W. W. Norton, 2023.

[23] EDLER, Jakob; GEORGHIOU, Luke. Public procurement and innovation: resurrecting the demand side. Research Policy, v. 36, n. 7, p. 949-963, 2007.

[24] HOROWITZ, Michael C. Artificial intelligence, international competition, and the balance of power. Texas National Security Review, v. 1, n. 3, p. 36-57, 2018; SCHARRE, op. cit.

[25] Tradução de *human in the loop*: princípio de governança que exige supervisão humana significativa sobre decisões automatizadas, com poder real de contestação e intervenção.

[26] GenAI.mil é a plataforma oficial de inteligência artificial generativa do

público pelo *Chief Digital and Artificial Intelligence Office* informa que a plataforma reúne capacidades de IA generativa e ferramentas certificadas para *Controlled Unclassified Information* (CUI)[27] e *Impact Level* 5 (IL5)[28], mas esse dado não demonstra, por si só, incorporação operacional plena.[29]

A dependência pós-aquisição torna-se mais visível no ciclo de vida dos sistemas de IA, pois a aquisição inicial representa apenas uma fração de sua vida útil. As fases mais sensíveis estão na manutenção, atualização, retreinamento de modelos, correção de vulnerabilidades, adaptação a ameaças emergentes e substituição futura. Quando essas etapas carecem de governança suficiente, a compra converte-se em vínculo prolongado com fornecedor, arquitetura técnica e infraestrutura de dados. Trata-se, portanto, de problema estrutural de Estado: como preservar capacidade decisória, continuidade operacional e autonomia estratégica quando sistemas críticos dependem de fornecedores externos, atualizações proprietárias e infraestruturas digitais globais. O caso brasileiro ilustra essa realidade de forma particular e urgente.

5. O caso brasileiro e a análise comparada

O Brasil possui marcos relevantes em defesa, contratações públicas, segurança pública, interoperabilidade governamental, cibersegurança, proteção de dados e infraestruturas críticas. A Lei nº 12.598/2012 reconhece a especificidade de produtos e sistemas de

---

Departamento de Defesa dos Estados Unidos (DoD), lançada publicamente em dezembro de 2025 sob coordenação do Chief Digital and Artificial Intelligence Office (CDAO), para disponibilizar capacidades de IA generativa a usuários do Departamento em ambiente controlado. A plataforma foi adotada como exemplo por constituir iniciativa recente de incorporação institucional de IA generativa em defesa, documentada por fonte primária oficial, o que permite ilustrar a distinção entre disponibilidade formal da tecnologia e capacidade operacional efetiva, objeto central desta análise.

[27] Categoria do governo norte-americano para informação sensível, porém não classificada, sujeita a controles específicos de manuseio e proteção

[28] Nível de autorização de segurança do Departamento de Defesa dos Estados Unidos para processamento de informação controlada não-classificada em ambientes de nuvem.

[29] CHIEF DIGITAL AND ARTIFICIAL INTELLIGENCE OFFICE. The War Department Unleashes AI on New GenAI.mil Platform. Arlington, VA: CDAO, 9 dez. 2025.

defesa; a Lei nº 14.133/2021 reforça planejamento, governança, gestão de riscos e eficiência contratual; e a Lei nº 13.675/2018 institui o SUSP e a Política Nacional de Segurança Pública e Defesa Social, criando base normativa para coordenação intersetorial em segurança.[30] Esses instrumentos, contudo, não asseguram por si sós governança pós-aquisição de tecnologias críticas baseadas em IA, software, dados e conectividade, especialmente porque não estabelecem requisitos transversais de auditabilidade, reversibilidade, soberania de dados, validação independente e ciclo de vida tecnológico robusto.

A ePING indica base normativa e técnica relevante para interoperabilidade na administração pública federal,[31] enquanto a Política Nacional, a Estratégia Nacional e o Plano Nacional de Segurança de Infraestruturas Críticas estabelecem diretrizes para segurança, resiliência, continuidade e coordenação setorial.[32] No campo da cibersegurança, a E-Ciber de 2020, a Política Nacional de Cibersegurança de 2023 e a Estratégia Nacional de Cibersegurança de 2025 revelam evolução institucional relevante.[33] Ainda assim, interoperabilidade, cibersegurança, regularidade contratual e proteção de infraestruturas não equivalem automaticamente à governança do ciclo de vida tecnológico: um sistema pode estar formalmente contratado e protegido contra certos riscos cibernéticos, mas permanecer dependente

---

[30] BRASIL. Lei nº 12.598, de 21 de março de 2012. Estabelece normas especiais para compras, contratações e desenvolvimento de produtos e sistemas de defesa. Brasília, DF: Presidência da República, 2012; BRASIL. Lei nº 13.675, de 11 de junho de 2018, op. cit.; BRASIL. Lei nº 14.133, de 1º de abril de 2021. Lei de Licitações e Contratos Administrativos. Brasília, DF: Presidência da República, 2021.

[31] BRASIL. Ministério do Planejamento, Desenvolvimento e Gestão. Secretaria de Tecnologia da Informação e Comunicação. ePING: Padrões de Interoperabilidade de Governo Eletrônico: Documento de Referência, versão 2018. Brasília, DF: Governo Federal, 2018.

[32] BRASIL. Decreto nº 9.573, de 22 de novembro de 2018, op. cit.; BRASIL. Decreto nº 10.569, de 9 de dezembro de 2020, op. cit.; BRASIL. Decreto nº 11.200, de 15 de setembro de 2022, op. cit.

[33] BRASIL. Decreto nº 10.222, de 5 de fevereiro de 2020. Aprova a Estratégia Nacional de Segurança Cibernética. Brasília, DF: Presidência da República, 2020; BRASIL. Decreto nº 11.856, de 26 de dezembro de 2023. Institui a Política Nacional de Cibersegurança e o Comitê Nacional de Cibersegurança. Brasília, DF: Presidência da República, 2023; BRASIL. Decreto nº 12.573, de 4 de agosto de 2025. Institui a Estratégia Nacional de Cibersegurança. Brasília, DF: Presidência da República, 2025.

de fornecedor único, sem auditabilidade técnica, portabilidade de dados ou reversibilidade contratual.

O risco institucional brasileiro, portanto, não decorre de vazio normativo absoluto, mas da dificuldade de integrar marcos existentes em requisitos técnicos e contratuais transversais, verificáveis e exigíveis ao longo do ciclo de vida tecnológico. Defesa, segurança pública, defesa civil, agências reguladoras, empresas estatais, concessionárias e operadores privados podem contratar tecnologias críticas sem matriz comum de auditabilidade, interoperabilidade, soberania de dados, validação independente e substituição futura, ampliando o risco de modernização aparente e dependência funcional. Sob perspectiva institucional, esses déficits indicam que a dependência pós-aquisição não decorre apenas da origem do fornecedor, mas da forma como regras, incentivos, capacidades públicas e padrões técnicos condicionam a operação futura dos sistemas críticos.[34] O Quadro 3 sintetiza essa leitura ao organizar os principais déficits brasileiros em governança pós-aquisição.

[34] NORTH, op. cit.; OSTROM, op. cit.; FARRELL; NEWMAN, op. cit.

Quadro 3 – Lacunas documentais em governança pós-aquisição: evidência pública examinada[35]

Déficit	Afirmação defensável	Fonte primária	Limite da evidência	Formulação segura
Fragmentação institucional	Há marcos setoriais separados, mas sem matriz transversal de ciclo de vida.	Lei 14.133/2021; Lei 13.675/2018; decretos de cibersegurança e infraestrutura crítica.	Não permite inferir práticas internas não documentadas.	Não se identifica matriz federal transversal publicamente verificável.
Auditabilidade técnica	Há gestão contratual e gestão de riscos, mas não cláusula federal geral de auditoria técnica de IA crítica.	Lei 14.133/2021; NIST AI RMF 1.0 como benchmark técnico.	Lei geral de licitações não foi desenhada especificamente para IA crítica.	Há lacuna específica, não inexistência de controle.
Reversibilidade	Não se identifica padrão federal específico de saída e migração para IA crítica.	Lei 14.133/2021; literatura e padrões técnicos de gestão de risco.	O artigo não usa PNCP como amostra empírica.	Não se identifica padrão transversal na documentação pública examinada.
Soberania de dados	LGPD e cibersegurança não equivalem a residência, portabilidade e controle operacional de dados críticos.	LGPD; Política Nacional de Cibersegurança; Estratégia Nacional de Cibersegurança.	LGPD protege dados pessoais, não toda governança de dados críticos.	Proteção de dados e soberania operacional são dimensões distintas.
Validação independente	Não se identifica regime público transversal de certificação de IA crítica.	*NIST, ISO, AI Act e DoD Responsible AI como benchmarks.*	Pode haver iniciativas setoriais não publicamente documentadas.	Não se identifica regime público transversal na documentação examinada.

Fonte: Elaboração dos autores (2026), com base em documentação pública primária e técnica: Lei nº 14.133/2021; Lei nº 13.675/2018; Decretos nº 10.222/2020, 11.856/2023 e 12.573/2025; LGPD; Sinesp; NIST; DoD; ISO/IEC; União Europeia.

[35] Nota metodológica: a classificação baseia-se em evidência verificável em documentação pública e distingue jurisdições nacionais de regimes multilaterais. O diagnóstico não afirma que toda governança pós-aquisição esteja ausente; práticas internas podem ser mais sofisticadas. A inferência é mais cautelosa: marcos públicos explícitos ainda não revelam integração robusta de ciclo de vida em IA e tecnologias críticas.

A leitura do Quadro 3 indica que, na documentação pública examinada, o problema brasileiro não é a ausência de normas setoriais, mas a falta de matriz transversal que as converta em requisitos técnicos, contratuais e operacionais verificáveis de auditabilidade, reversibilidade, interoperabilidade, governança de dados críticos e validação independente em tecnologias baseadas em IA. Assim, contratações podem cumprir exigências administrativas formais e, ainda assim, deixar descobertas dimensões centrais do ciclo de vida tecnológico. O critério decisivo, portanto, não é a nacionalidade do fornecedor, pois tanto fornecedores estrangeiros quanto nacionais podem gerar *lock-in*, baixa auditabilidade, baixa interoperabilidade e dependência estatal, mas a governabilidade do sistema: capacidade de conhecê-lo, auditá-lo, integrá-lo, atualizá-lo, proteger seus dados e substituí-lo sem perda crítica de capacidade.

5.1. Análise comparada e regimes multilaterais

A análise comparada indica que Estados e organizações internacionais vêm avançando em princípios de IA responsável, cibersegurança, resiliência e proteção de infraestruturas sensíveis, mas ainda há distância entre diretrizes gerais e mecanismos concretos de governança pós-aquisição, especialmente em auditabilidade, reversibilidade, interoperabilidade, soberania de dados e validação independente.

Em contraste com o Brasil, os Estados Unidos apresentam documentação pública mais densa sobre gestão de risco, governança e validação de IA, por meio do NIST *AI Risk Management Framework* e da *Responsible AI Strategy and Implementation Pathway* do DoD, embora isso não equivalha a uma lei geral única e plenamente vinculante para todos os usos.[36] A União Europeia segue trajetória regulatória mais vinculante, com o *Artificial Intelligence Act*, o *Data Governance Act* e o *Data Act,* que articulam gestão de risco, governança de dados, documentação técnica, logs, transparência, supervisão humana, robustez, cibersegurança e monitoramento pós-comercialização, ainda que subsistam desafios de aplicação prática.[37]

---

[36] NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY. Artificial Intelligence Risk Management Framework (AI RMF 1.0). Gaithersburg: NIST, 2023; U.S. DEPARTMENT OF DEFENSE. Responsible Artificial Intelligence Strategy and Implementation Pathway. Washington, DC: DoD, 2022.

[37] EUROPEAN UNION. Regulation (EU) 2022/868 of the European Parliament and of the Council of 30 May 2022 on European data governance and amending

No Brasil, há marcos normativos relevantes, mas organizados em silos setoriais, como defesa, licitações, segurança pública, cibersegurança e infraestruturas críticas, sem matriz transversal de governança pós-aquisição. Regimes multilaterais, como OTAN e OCDE, oferecem parâmetros úteis de IA responsável, confiável, rastreável e governável, mas não substituem cláusulas contratuais, capacidade técnica de auditoria, soberania de dados, interoperabilidade e mecanismos de saída.[38]

Para sintetizar essa comparação, o Quadro 4 organiza matriz qualitativa de densidade documental relativa em auditabilidade, reversibilidade, interoperabilidade, soberania de dados e validação independente. Estados Unidos, União Europeia e Brasil são tratados como jurisdições; a OTAN, como regime multilateral de referência; e a OCDE, como benchmark normativo geral. A classificação "forte", "parcial" ou "crítica" indica apenas densidade documental pública e exigibilidade formal, não ranking de maturidade tecnológica, desempenho operacional ou capacidade real.

Regulation (EU) 2018/1724 (Data Governance Act). Official Journal of the European Union, 2022; EUROPEAN UNION. Regulation (EU) 2023/2854 of the European Parliament and of the Council of 13 December 2023 on harmonised rules on fair access to and use of data (Data Act). Official Journal of the European Union, 2023; EUROPEAN UNION. Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonised rules on artificial intelligence (Artificial Intelligence Act). Official Journal of the European Union, 2024.

[38] NORTH ATLANTIC TREATY ORGANIZATION. Summary of the NATO Artificial Intelligence Strategy. Brussels: NATO, 2021; NORTH ATLANTIC TREATY ORGANIZATION. Summary of NATO's revised Artificial Intelligence Strategy. Brussels: NATO, 2024; ORGANISATION FOR ECONOMIC CO-OPERATION AND DEVELOPMENT. Recommendation of the Council on Artificial Intelligence. OECD Legal Instruments, OECD/LEGAL/0449, 2019, atualizado em 2024.

Quadro 4 – Densidade documental relativa em governança pós-aquisição[39]

Categoria	Modelo	Auditoria	Saída	Interopera-bilidade	Dados	Validação
Jurisdição	Estados Unidos	Forte	Parcial	Forte	Parcial	Forte
Jurisdição	União Europeia	Forte	Forte	Parcial	Forte	Forte
Jurisdição	Brasil	Crítica/ parcial	Crítica	Parcial	Parcial	Crítica
Regime multilateral	OTAN	Forte	N/A	Forte	Parcial	Forte

Fonte: Elaboração dos autores (2026), com base na análise documental dos marcos nacionais, regulatórios e multilaterais examinados nesta seção.[40]

O Quadro 4 sugere que maior densidade documental resulta da combinação entre parâmetros técnicos, regulação, governança de dados, capacidade institucional e validação ao longo do ciclo de vida. Estados Unidos e União Europeia tornam mais visíveis e exigíveis certos requisitos de governança, embora não eliminem dependências tecnológicas. O Brasil não apresenta vazio institucional, pois dispõe de bases parciais em interoperabilidade, proteção de dados, cibersegurança e contratações públicas; contudo, a documentação pública examinada revela lacunas críticas em reversibilidade contratual e validação independente de IA crítica. A comparação reforça, assim, a hipótese central do artigo: autonomia estratégica depende menos da origem do fornecedor, do volume adquirido ou da transferência formal de tecnologia do que da capacidade estatal de governar o ciclo de vida dos sistemas incorporados.

[39] Nota: a matriz mede densidade documental pública e exigibilidade formal, não capacidade operacional real, execução contratual, práticas sigilosas, maturidade tecnológica nacional, desempenho de sistemas em uso ou efetividade institucional concreta.

[40] Bases documentais consideradas no Quadro 4: Estados Unidos: NIST AI RMF 1.0, NIST AI RMF Generative AI Profile e Responsible AI Strategy and Implementation Pathway do DoD; União Europeia: AI Act, Data Governance Act e Data Act; Brasil: Lei nº 14.133/2021, Lei nº 13.675/2018, Sinesp, ePING, LGPD e Decretos nº 9.573/2018, 10.222/2020, 10.569/2020, 11.200/2022, 11.856/2023 e 12.573/2025; OTAN: estratégias de IA de 2021 e 2024.

6. Discussão e proposições institucionais

A análise sustenta três achados: a dependência pós-aquisição deve ser tratada como categoria própria, distinta da compra inicial e do *lock-in*, pois o valor estratégico das tecnologias críticas depende da capacidade de governar atualizações, integrar bases, auditar decisões, corrigir falhas, migrar dados e substituir fornecedores; infraestruturas críticas ampliam o problema para além da defesa militar, já que tecnologias de uso dual ou múltiplo atravessam segurança pública, defesa civil, regulação econômica, logística, energia, comunicações e serviços essenciais; e o caso brasileiro revela base normativa relevante, mas integração operacional insuficientemente visível na documentação pública examinada. O desafio, portanto, não é apenas criar novas normas, mas converter normas existentes em requisitos técnicos e contratuais exigíveis ao longo do ciclo de vida tecnológico.

Quatro objeções delimitam, sem invalidar, essa tese. Requisitos robustos de auditabilidade, reversibilidade, interoperabilidade e validação independente podem elevar custos e reduzir velocidade de contratação, mas a ausência desses requisitos pode produzir custo sistêmico superior quando o Estado perde capacidade de auditar, migrar, integrar ou substituir sistemas críticos. Fornecedores nacionais também podem gerar dependência, o que confirma que a nacionalidade do fornecedor não basta para aferir autonomia estratégica.

Documentos públicos não revelam integralmente práticas internas de defesa, segurança pública ou operadores de infraestrutura crítica, razão pela qual o artigo não afirma sua inexistência, mas apenas a ausência de matriz pública transversal, consolidada e exigível nos documentos examinados. Por fim, soberania de dados não equivale automaticamente a segurança: sem criptografia, controle de acesso, logs, portabilidade, auditoria, resposta a incidentes e validação independente, pode permanecer como retórica institucional sem capacidade operacional. O objeto do artigo, assim, permanece preciso: identificar quando a baixa exigibilidade de governança pós-aquisição converte dependências tecnológicas inevitáveis em vulnerabilidades estratégicas evitáveis.

6.1. Proposições institucionais e contratuais

A resposta institucional não deve ser autossuficiência tecnológica absoluta, mas governança proporcional das dependências inevitáveis. O Brasil continuará importando tecnologias críticas e integrando soluções globais; a questão estratégica é se essas dependências serão

conhecidas, contratualmente governadas, tecnicamente auditáveis e operacionalmente reversíveis. Essa orientação aproxima-se da literatura sobre Estado empreendedor e formação de capacidades públicas, na qual o Estado atua como coordenador estratégico de missões, investimentos e capacidades tecnológicas, e não apenas como comprador passivo de soluções prontas.[41] A partir dessa premissa, seis medidas podem transformar compras tecnológicas em instrumentos de capacidade estatal.

1. **Auditabilidade técnica:** exigir logs, documentação, trilhas de decisão, acesso a evidências, explicabilidade proporcional ao risco e auditoria independente, com base em NIST, ISO/IEC e AI Act, respeitados sigilo, propriedade intelectual e segurança operacional.
2. **Reversibilidade contratual:** prever migração de dados, suporte pós-rescisão, documentação de integração, continuidade operacional, transição de fornecedor e *escrow* quando cabível, reduzindo aprisionamento funcional.
3. **Interoperabilidade:** exigir APIs documentadas, formatos portáveis, compatibilidade com sistemas públicos, documentação de interfaces e vedação de integração proprietária injustificada, sem afastar requisitos legítimos de segurança e desempenho.
4. **Governança de dados críticos:** disciplinar residência, portabilidade, criptografia, controle de acesso, exclusão segura, retenção, transferência internacional e segregação de ambientes, preservando controle sobre dados operacionais sensíveis.
5. **Validação independente:** exigir testes pré-implantação, red teaming quando cabível, laboratórios públicos ou acreditados, auditorias periódicas e validação pós-implantação, tornando riscos de viés, fragilidade adversarial e degradação silenciosa mais governáveis.
6. **Capacidade estatal permanente:** formar quadros, criar unidade especializada, elaborar matriz nacional de requisitos, manter supervisão intersetorial e articular órgãos técnicos,

[41] MAZZUCATO, Mariana. O Estado empreendedor: desmascarando o mito do setor público versus setor privado. São Paulo: Portfolio-Penguin, 2014.

reguladores, operadores e instituições de controle, desde que haja orçamento, pessoal e mandato claros.

Essas proposições podem ser implementadas gradualmente: guia nacional de contratação de tecnologias críticas, cláusulas-padrão em editais e contratos estratégicos, capacidade técnica dedicada de validação e auditoria, e integração regulatória com concessões, parcerias público-privadas e operadores privados de infraestrutura crítica. A mudança conceitual é simples: comprar tecnologia crítica é governar capacidade estatal, não apenas adquirir produto de mercado.

7. Conclusão

A geoeconomia contemporânea deslocou o centro da soberania tecnológica. No passado, a posse formal de equipamentos, a importação de bens de alto valor agregado ou a assinatura de cláusulas de transferência de tecnologia podiam parecer indicadores suficientes de modernização. Em sistemas baseados em IA, software, sensores, nuvem, dados e conectividade, essa lógica tornou-se insuficiente. A soberania tecnológica não está apenas em possuir o sistema, mas em conseguir governá-lo ao longo de seu ciclo de vida.

O presente trabalho sustentou que a governança pós-aquisição insuficientemente exigível pode aumentar o risco de que aquisições brasileiras de defesa, segurança pública e infraestruturas críticas se convertam, ao longo do ciclo de vida tecnológico, em dependências comerciais duradouras. A dependência não se encerra na compra. Ela se reproduz na manutenção, atualização, interoperabilidade, dados, conectividade, suporte, validação e possibilidade de substituição. Por isso, o problema estratégico não é simplesmente comprar tecnologia estrangeira, mas incorporar sistemas críticos sem capacidade institucional para auditá-los, adaptá-los, integrá-los e substituí-los.

A análise demonstrou que infraestruturas críticas ampliam a relevância do tema, pois dependem crescentemente de tecnologias digitais frequentemente de uso dual ou múltiplo. Essas tecnologias atravessam defesa, segurança pública, defesa civil, regulação econômica e continuidade de serviços, de modo que a fragmentação institucional pode produzir modernização aparente e vulnerabilidade real.

O caso brasileiro revela base normativa relevante, mas insuficiente integração de ciclo de vida. A existência de leis de defesa, licitações, políticas de cibersegurança e instrumentos de proteção de infraestruturas críticas não garante, por si só, governança pós-aquisição. O desafio é

converter princípios em cláusulas, cláusulas em capacidades, capacidades em instituições e instituições em autonomia operacional. A governança precisa ser contratual, técnica, regulatória e intersetorial.

A resposta proposta é evoluir da lógica de aquisição para a lógica de capacidade, incorporando auditabilidade técnica, reversibilidade contratual, interoperabilidade, governança de dados críticos, validação independente e supervisão humana significativa. O Brasil não precisa buscar autossuficiência absoluta em todas as tecnologias, mas precisa conhecer, mensurar, distribuir, auditar e tornar reversíveis as dependências que aceita.

A contribuição central do artigo é deslocar o debate sobre comércio internacional de tecnologias críticas para o pós-aquisição. A geoeconomia da dependência não se define apenas pela origem do fornecedor, pelo preço do contrato ou pela entrega do equipamento, mas pela operação cotidiana, pelo controle dos dados, pela atualização, interoperabilidade, manutenção, validação e possibilidade real de saída. No século XXI, soberania tecnológica não equivale à propriedade formal nem à autossuficiência plena; corresponde à capacidade estatal, mensurável, verificável e exigível contratualmente, de conhecer, auditar, adaptar, integrar e substituir sistemas críticos ao longo de seu ciclo de vida.

O Brasil não precisa fabricar todos os componentes que utiliza, mas deve ser capaz de auditar sistemas de IA, migrar dados, substituir fornecedores críticos e transformar dependências inevitáveis em riscos conhecidos, distribuídos e institucionalmente governáveis.

Bibliografia

AGGARWAL, Vinod K.; REDDIE, Andrew W. New economic statecraft and global technology conflicts: the dilemma for middle powers. Business and Politics, 2025. DOI: 10.1017/bap.2025.10011. Disponível em: https://www.cambridge.org/core/journals/business-and-politics/article/new-economic-statecraft-and-global-technology-conflicts-the-dilemma-for-middle-powers/A9BBC3868B56EE9AA8827029BED55054. Acesso em: 17 jun. 2026.

BABIĆ, Milan; DE GRAAFF, Nana; LINSI, Lukas; WEINHARDT, Clara. The geoeconomic turn in international trade, investment, and technology. Politics and Governance, v. 12, 2024. DOI: 10.17645/pag.9031. Disponível em: https://www.cogitatiopress.com/politicsandgovernance/article/view/9031. Acesso em: 17 jun. 2026.

BRASIL. Decreto nº 9.573, de 22 de novembro de 2018. Aprova a Política Nacional de Segurança de Infraestruturas Críticas. Brasília, DF: Presidência da República, 2018a. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/Decreto/D9573.htm. Acesso em: 17 jun. 2026.

BRASIL. Lei nº 13.675, de 11 de junho de 2018. Institui o Sistema Único de Segurança Pública (SUSP) e cria a Política Nacional de Segurança Pública e Defesa Social. Brasília, DF: Presidência da República, 2018b. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13675.htm. Acesso em: 17 jun. 2026.

BRASIL. Lei nº 13.709, de 14 de agosto de 2018. Lei Geral de Proteção de Dados Pessoais (LGPD). Brasília, DF: Presidência da República, 2018c. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm. Acesso em: 17 jun. 2026.

BRASIL. Ministério do Planejamento, Desenvolvimento e Gestão. Secretaria de Tecnologia da Informação e Comunicação. ePING: Padrões de Interoperabilidade de Governo Eletrônico: Documento de Referência, versão 2018. Brasília, DF: Governo Federal, 2018d. Disponível em: https://www.gov.br/governodigital/pt-br/infraestrutura-nacional-de-dados/ePING_v2018_20171205.pdf. Acesso em: 17 jun. 2026.

BRASIL. Decreto nº 10.222, de 5 de fevereiro de 2020. Aprova a Estratégia Nacional de Segurança Cibernética. Brasília, DF: Presidência da República, 2020a. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2019-2022/2020/decreto/d10222.htm. Acesso em: 17 jun. 2026.

BRASIL. Decreto nº 10.569, de 9 de dezembro de 2020. Aprova a Estratégia Nacional de Segurança de Infraestruturas Críticas. Brasília, DF: Presidência da República, 2020b. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2019-2022/2020/decreto/D10569.htm. Acesso em: 17 jun. 2026.

BRASIL. Decreto nº 10.822, de 28 de setembro de 2021. Institui o Plano Nacional de Segurança Pública e Defesa Social 2021-2030. Brasília, DF: Presidência da República, 2021a. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2019-2022/2021/decreto/D10822.htm. Acesso em: 17 jun. 2026.

BRASIL. Lei nº 12.598, de 21 de março de 2012. Estabelece normas especiais para compras, contratações e desenvolvimento de produtos

e sistemas de defesa. Brasília, DF: Presidência da República, 2012. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2011-2014/2012/lei/l12598.htm. Acesso em: 17 jun. 2026.

BRASIL. Lei nº 14.133, de 1º de abril de 2021. Lei de Licitações e Contratos Administrativos. Brasília, DF: Presidência da República, 2021b. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2019-2022/2021/lei/l14133.htm. Acesso em: 17 jun. 2026.

BRASIL. Decreto nº 11.200, de 15 de setembro de 2022. Aprova o Plano Nacional de Segurança de Infraestruturas Críticas. Brasília, DF: Presidência da República, 2022. Disponível em: https://www.planalto.gov.br/ccivil_03/_Ato2019-2022/2022/Decreto/D11200.htm. Acesso em: 17 jun. 2026.

BRASIL. Decreto nº 11.856, de 26 de dezembro de 2023. Institui a Política Nacional de Cibersegurança e o Comitê Nacional de Cibersegurança. Brasília, DF: Presidência da República, 2023. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2023-2026/2023/decreto/D11856.htm. Acesso em: 17 jun. 2026.

BRASIL. Decreto nº 12.573, de 4 de agosto de 2025. Institui a Estratégia Nacional de Cibersegurança. Brasília, DF: Presidência da República, 2025. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2023-2026/2025/decreto/D12573.htm. Acesso em: 17 jun. 2026.

BRASIL. Portal Nacional de Contratações Públicas (PNCP). Brasília, DF: Governo Federal, 2026. Disponível em: https://pncp.gov.br/. Acesso em: 17 jun. 2026.

BUREAU OF INDUSTRY AND SECURITY. Implementation of Additional Export Controls: Certain Advanced Computing and Semiconductor Manufacturing Items; Supercomputer and Semiconductor End Use; Entity List Modification. Federal Register, 13 Oct. 2022. Disponível em: https://www.federalregister.gov/documents/2022/10/13/2022-21658/implementation-of-additional-export-controls-certain-advanced-computing-and-semiconductor. Acesso em: 17 jun. 2026.

BUREAU OF INDUSTRY AND SECURITY. Implementation of Additional Export Controls: Certain Advanced Computing Items; Supercomputer and Semiconductor End Use; Updates and Corrections. Federal Register, 25 Oct. 2023. Disponível em: https://www.federalregister.gov/documents/2023/10/25/2023-23055/

implementation-of-additional-export-controls-certain-advanced-computing-items-supercomputer-and. Acesso em: 17 jun. 2026.

BUREAU OF INDUSTRY AND SECURITY. Commerce strengthens export controls to restrict China's capability to produce advanced semiconductors for military applications. Washington, DC: U.S. Department of Commerce, 2024. Disponível em: https://www.bis.gov/press-release/commerce-strengthens-export-controls-restrict-chinas-capability-produce-advanced-semiconductors-military. Acesso em: 17 jun. 2026.

CHIEF DIGITAL AND ARTIFICIAL INTELLIGENCE OFFICE. The War Department Unleashes AI on New GenAI.mil Platform. Arlington, VA: CDAO, 9 Dec. 2025. Disponível em: https://www.ai.mil/Latest/News-Press/PR-View/Article/4355177/the-war-department-unleashes-ai-on-new-genaimil-platform/. Acesso em: 17 jun. 2026.

COLE, Daniel H. Laws, norms, and the Institutional Analysis and Development Framework. Journal of Institutional Economics, v. 13, n. 4, p. 829-847, 2017. DOI: 10.1017/S1744137417000030. Disponível em: https://www.cambridge.org/core/journals/journal-of-institutional-economics/article/laws-norms-and-the-institutional-analysis-and-development-framework/D5A406119308DAEA1F3226FC803282FE. Acesso em: 17 jun. 2026.

EDLER, Jakob; GEORGHIOU, Luke. Public procurement and innovation: resurrecting the demand side. Research Policy, v. 36, n. 7, p. 949-963, 2007. DOI: 10.1016/j.respol.2007.03.003. Disponível em: https://www.sciencedirect.com/science/article/abs/pii/S0048733307000741. Acesso em: 17 jun. 2026.

EUROPEAN UNION. Regulation (EU) 2022/868 of the European Parliament and of the Council of 30 May 2022 on European data governance and amending Regulation (EU) 2018/1724 (Data Governance Act). Official Journal of the European Union, 2022. Disponível em: https://eur-lex.europa.eu/eli/reg/2022/868/oj/eng. Acesso em: 17 jun. 2026.

EUROPEAN UNION. Regulation (EU) 2023/1781 of the European Parliament and of the Council of 13 September 2023 establishing a framework of measures for strengthening Europe's semiconductor ecosystem and amending Regulation (EU) 2021/694 (Chips Act). Official Journal of the European Union, 2023a. Disponível em: https://eur-lex.europa.eu/eli/reg/2023/1781/oj/eng. Acesso em: 17 jun. 2026.

EUROPEAN UNION. Regulation (EU) 2023/2854 of the European Parliament and of the Council of 13 December 2023 on harmonised rules on fair access to and use of data (Data Act). Official Journal of the European Union, 2023b. Disponível em: https://eur-lex.europa.eu/eli/reg/2023/2854/oj/eng. Acesso em: 17 jun. 2026.

EUROPEAN UNION. Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonised rules on artificial intelligence (Artificial Intelligence Act). Official Journal of the European Union, 2024. Disponível em: https://eur-lex.europa.eu/eli/reg/2024/1689/oj/eng. Acesso em: 17 jun. 2026.

FARRELL, Henry; NEWMAN, Abraham L. Weaponized interdependence: how global economic networks shape state coercion. International Security, v. 44, n. 1, p. 42-79, 2019. DOI: 10.1162/isec_a_00351. Disponível em: https://direct.mit.edu/isec/article/44/1/42/12237/Weaponized-Interdependence-How-Global-Economic. Acesso em: 17 jun. 2026.

GEORGE, Alexander L.; BENNETT, Andrew. Case Studies and Theory Development in the Social Sciences. Cambridge, MA: MIT Press, 2005. Disponível em: https://mitpress.mit.edu/9780262572224/case-studies-and-theory-development-in-the-social-sciences/. Acesso em: 17 jun. 2026.

HOROWITZ, Michael C. Artificial intelligence, international competition, and the balance of power. Texas National Security Review, v. 1, n. 3, p. 36-57, 2018. DOI: 10.15781/T2639KP49. Disponível em: https://tnsr.org/2018/05/artificial-intelligence-international-competition-and-the-balance-of-power/. Acesso em: 17 jun. 2026.

INTERNATIONAL ORGANIZATION FOR STANDARDIZATION; INTERNATIONAL ELECTROTECHNICAL COMMISSION. ISO/IEC 42001:2023: artificial intelligence management system. Geneva: ISO, 2023a. Disponível em: https://www.iso.org/standard/42001. Acesso em: 17 jun. 2026.

INTERNATIONAL ORGANIZATION FOR STANDARDIZATION; INTERNATIONAL ELECTROTECHNICAL COMMISSION. ISO/IEC 23894:2023: artificial intelligence: guidance on risk management. Geneva: ISO, 2023b. Disponível em: https://www.iso.org/standard/77304.html. Acesso em: 17 jun. 2026.

LIJPHART, Arend. Comparative politics and the comparative method. American Political Science Review, v. 65, n. 3, p. 682-

693, 1971. DOI: 10.2307/1955513. Disponível em: https://www.cambridge.org/core/journals/american-political-science-review/article/comparative-politics-and-the-comparative-method/A326138E114805EF7E1B72F60EBD4295. Acesso em: 17 jun. 2026.

LUTTWAK, Edward N. From geopolitics to geo-economics: logic of conflict, grammar of commerce. The National Interest, n. 20, p. 17-23, 1990. Disponível em: https://www.jstor.org/stable/42894676. Acesso em: 17 jun. 2026.

MAZZUCATO, Mariana. O Estado empreendedor: desmascarando o mito do setor público versus setor privado. São Paulo: Portfolio-Penguin, 2014. Disponível em: https://www.companhiadasletras.com.br/trechos/13659.pdf. Acesso em: 17 jun. 2026.

MINISTÉRIO DA JUSTIÇA E SEGURANÇA PÚBLICA. Sinesp: Sistema Nacional de Informações de Segurança Pública. Brasília, DF: MJSP, 2026. Disponível em: https://www.gov.br/mj/pt-br/assuntos/sua-seguranca/seguranca-publica/sinesp-1. Acesso em: 17 jun. 2026.

NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY. Artificial Intelligence Risk Management Framework (AI RMF 1.0). Gaithersburg: NIST, 2023. DOI: 10.6028/NIST.AI.100-1. Disponível em: https://nvlpubs.nist.gov/nistpubs/ai/NIST.AI.100-1.pdf. Acesso em: 17 jun. 2026.

NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY. Artificial Intelligence Risk Management Framework: Generative Artificial Intelligence Profile. Gaithersburg: NIST, 2024. DOI: 10.6028/NIST.AI.600-1. Disponível em: https://nvlpubs.nist.gov/nistpubs/ai/NIST.AI.600-1.pdf. Acesso em: 17 jun. 2026.

NORTH, Douglass C. Institutions, Institutional Change and Economic Performance. Cambridge: Cambridge University Press, 1990.

NORTH ATLANTIC TREATY ORGANIZATION. Summary of the NATO Artificial Intelligence Strategy. Brussels: NATO, 2021. Disponível em: https://www.nato.int/cps/en/natohq/official_texts_187617.htm. Acesso em: 17 jun. 2026.

NORTH ATLANTIC TREATY ORGANIZATION. Summary of NATO's revised Artificial Intelligence Strategy. Brussels: NATO, 2024. Disponível em: https://www.nato.int/en/about-us/official-texts-and-resources/official-texts/2024/07/10/summary-of-natos-revised-artificial-intelligence-ai-strategy. Acesso em: 17 jun. 2026.

ORGANISATION FOR ECONOMIC CO-OPERATION AND DEVELOPMENT. Recommendation of the Council on Artificial Intelligence. OECD Legal Instruments, OECD/LEGAL/0449, 2019, atualizado em 2024. Disponível em: https://legalinstruments.oecd.org/en/instruments/oecd-legal-0449. Acesso em: 17 jun. 2026.

OSTROM, Elinor. Background on the Institutional Analysis and Development Framework. Policy Studies Journal, v. 39, n. 1, p. 7-27, 2011. DOI: 10.1111/j.1541-0072.2010.00394.x. Disponível em: https://onlinelibrary.wiley.com/doi/10.1111/j.1541-0072.2010.00394.x. Acesso em: 17 jun. 2026.

RUCK, Jan. A geoeconomic fix? European industrial policy on semiconductors amidst global competition. JCMS: Journal of Common Market Studies, v. 64, n. 2, p. 742-761, 2026. DOI: 10.1111/jcms.13710. Disponível em: https://onlinelibrary.wiley.com/doi/full/10.1111/jcms.13710. Acesso em: 17 jun. 2026.

SCHARRE, Paul. Four Battlegrounds: Power in the Age of Artificial Intelligence. New York: W. W. Norton, 2023.

U.S. DEPARTMENT OF DEFENSE. Responsible Artificial Intelligence Strategy and Implementation Pathway. Washington, DC: DoD, 2022. Disponível em: https://media.defense.gov/2022/Jun/22/2003022604/-1/-1/0/Department-of-Defense-Responsible-Artificial-Intelligence-Strategy-and-Implementation-Pathway.PDF. Acesso em: 17 jun. 2026.

WHALEY, Luke. The critical institutional analysis and development framework. International Journal of the Commons, v. 12, n. 2, p. 137-161, 2018. DOI: 10.18352/ijc.848. Disponível em: https://thecommonsjournal.org/articles/10.18352/ijc.848. Acesso em: 17 jun. 2026.

APÊNDICE A – MATRIZ DE EVIDÊNCIAS DOCUMENTAIS

A matriz sintetiza a base documental pública utilizada para classificar densidade forte, lacuna parcial e lacuna crítica. Ela não mede desempenho operacional real nem práticas internas sigilosas; mede apenas densidade documental pública e exigibilidade formal.

Modelo	Dimensão	Documento	Dispositivo/seção	Evidência textual curta	Indicador 1	Indicador 2	Indicador 3	Classificação
EUA	Auditabilidade	NIST AI RMF 1.0	Govern, Map, Measure, Manage	Gestão e mensuração de riscos de IA	Sim	Sim	Sim	Densidade forte
EUA	Validação	*DoD Responsible AI Strategy; NIST AI 600-1*	RAI ecosystem; GenAI profile	Teste, avaliação e gestão de riscos de IA	Sim	Sim	Parcial	Densidade forte com ressalva ou Densidade parcial
UE	Auditabilidade e validação	AI Act	Arts. 9 a 15, 72 e 86	Gestão de risco, documentação, logs e supervisão humana	Sim	Sim	Sim	Densidade forte
UE	Dados	Data Governance Act; Data Act	Acesso, uso e compartilhamento de dados	Portabilidade, acesso e governança de dados	Sim	Sim	Sim	Densidade forte
Brasil	Auditabilidade	Lei 14.133/2021	Gestão contratual e fiscalização	Fiscalização administrativa e gestão de riscos	Parcial	Parcial	Não	Lacuna parcial
Brasil	Reversibilidade	Lei 14.133/2021	Execução contratual	Rescisão e continuidade contratual em termos gerais	Parcial	Não	Não	Lacuna crítica
Brasil	Interoperabilidade	Lei 13.675/2018; Sinesp; ePING	Integração de informações de segurança pública	Integração setorial de bases e existência de padrão federal de interoperabilidade governamental	Sim	Parcial	Não	Lacuna parcial
Brasil	Dados	LGPD; PNCiber; E-Ciber	Proteção de dados e cibersegurança	Proteção de dados pessoais e diretrizes de segurança	Sim	Parcial	Parcial	Lacuna parcial
Brasil	Validação independente	Marcos públicos examinados	Defesa, licitações, cibersegurança e infraestruturas críticas	Não se identifica certificação federal geral de IA crítica	Parcial	Não	Não	Lacuna crítica
OTAN	Interoperabilidade	NATO AI Strategy	IA responsável em defesa	Rastreabilidade, governabilidade e interoperabilidade doutrinária	Sim	Parcial	Parcial	Densidade forte com ressalva ou Densidade parcial

Fonte: Elaboração dos autores (2026), com base nos documentos primários e técnicos citados no corpo do artigo.