UFSM

InterAção

ISSN 2357-7975
ACESSO ABERTO

IA., Santa Maria, v. 17, n. 3, e99717, p. 1-21, 2026 • https://dx.doi.org/10.5902/2357797599717
Submissão: 08/11/2026 • Aprovação: 16/11/2026 • Publicação: 23/11/2026

Artigos Dossiê

Soberania cooperativa em inteligência artificial: o arranjo brasileiro (2021–2026) e as lições do Sul Global

Cooperative sovereignty in artificial intelligence: the Brazilian arrangement (2021–2026) and lessons from the Global South

Cileno de Magalhães Ribeiro[I]

[I]Exército Brasileiro, Fortaleza, CE, Brasil

Resumo

Este artigo analisa como o Brasil exerce soberania sobre a inteligência artificial (IA) entre 2021 e 2026 e o que a experiência comparada de outros países do Sul Global e de economias avançadas sugere para a política brasileira. Por meio de análise documental qualitativa de instrumentos de política, normas e programas, o estudo mapeia o arranjo brasileiro em cinco dimensões (investimento e infraestrutura, cibersegurança e segurança da informação, proteção de dados, regulação de IA e normas setoriais de 2026) e o compara com iniciativas da União Europeia, Índia, China, Japão, Coreia do Sul, Canadá, Austrália e Nigéria. Os resultados indicam três tensões: entre soberania jurisdicional e soberania do cidadão, entre autonomia e interdependência com fornecedores estrangeiros e entre política declaratória e capacidade operacional em órgãos de pequeno porte. O artigo propõe a soberania cooperativa, entendida como a retenção da capacidade de decisão sobre dados, chaves criptográficas, operações e escolhas estratégicas, combinada à participação em pesquisa, padrões e validação internacionais, e apresenta sete diretrizes de política pública. Conclui que o Brasil avançou em estratégia, infraestrutura e normas, mas carece de instrumentos que graduem as exigências pela classificação do dado e de indicadores públicos de dependência.

Palavras-chave: Inteligência artificial; Soberania digital; Sul Global; Políticas públicas; Interdependência gerenciada

Artigo publicado por InterAção sob uma licença CC BY-NC-SA 4.0.

Abstract

This article examines how Brazil exercises sovereignty over artificial intelligence (AI) between 2021 and 2026 and what the experience of other Global South countries and advanced economies suggests for Brazilian policy. Using qualitative document analysis of policy instruments, norms and programmes, the study maps the Brazilian arrangement in five dimensions (investment and infrastructure, cybersecurity and information security, data protection, AI regulation and 2026 sectoral rules) and compares it with initiatives of the European Union, India, China, Japan, South Korea, Canada, Australia and Nigeria. The results point to three tensions: between jurisdictional sovereignty and citizens' sovereignty, between autonomy and interdependence with foreign suppliers, and between declaratory policy and operational capacity in small bodies. The article proposes cooperative sovereignty, understood as retaining decision capacity over data, cryptographic keys, operations and strategic choices while taking part in international research, standards and validation, and presents seven public-policy guidelines. It concludes that Brazil has advanced in strategy, infrastructure and norms but lacks instruments that grade requirements by data classification and public indicators of dependence.

Keywords: Artificial intelligence; Digital sovereignty; Global South; Public policy; Managed interdependence

1 INTRODUÇÃO

A IA deixou de ser um assunto de pesquisa para se tornar infraestrutura de decisão do Estado e das empresas, e com isso a pergunta sobre quem controla os dados, os modelos e a capacidade de computação ganhou peso estratégico. O Gartner incluiu a geopatriação, isto é, a migração de dados e aplicações de nuvens públicas globais para alternativas locais ou soberanas, entre as dez tendências estratégicas de tecnologia de 2026 (GARTNER, 2025). Previsões de analistas não são evidência, mas episódios recentes mostram por que o tema mobiliza governos. Em 2025, a suspensão do e-mail do promotor-chefe do Tribunal Penal Internacional, após sanções norte-americanas, tornou-se na Europa símbolo do risco de depender de provedores sujeitos a jurisdição estrangeira, embora a empresa conteste ter interrompido serviços ao tribunal (AP NEWS, 2025; TECHZINE, 2025). No mesmo ano, um diretor jurídico da Microsoft França declarou sob juramento ao Senado francês que não podia garantir que dados de clientes europeus não seriam entregues a autoridades norte-americanas sem autorização das autoridades francesas (THE REGISTER, 2025).

Para países do Sul Global, a questão tem contornos próprios. A capacidade de computação para IA está concentrada em poucas jurisdições, e Lehdonvirta, Wú e Hawkins (2024) mostram que muitos países hospedam capacidade apenas para executar modelos, e alguns nem isso. O Brasil respondeu, entre 2021 e 2026, com um plano nacional de IA, novos investimentos em supercomputação e nuvem, uma nova estratégia de cibersegurança, um programa federal de privacidade e segurança da informação que incorporou a soberania como valor e, em 2026, normas setoriais que restringem o uso de IA generativa conforme a classificação da informação. O conjunto é amplo, mas ainda não foi analisado como arranjo, isto é, como um sistema de instrumentos com lógicas diferentes e tensões entre si.

Este artigo pergunta: como o Brasil pode exercer soberania sobre a IA sem buscar autarquia tecnológica, e o que a experiência comparada ensina? Três objetivos decorrem da pergunta: (i) mapear o arranjo brasileiro de 2021 a 2026; (ii) compará-lo, em termos qualitativos, com iniciativas de outros países; e (iii) propor diretrizes de política pública fundadas na ideia de soberania cooperativa. O estudo se relaciona, mas não se confunde, com trabalho anterior do autor sobre a proteção de cabos submarinos em Fortaleza, publicado nesta revista (RIBEIRO; MOREIRA, 2026), que tratou de uma infraestrutura crítica específica. O autor desenvolve em outro trabalho a formalização técnica da proteção do dado em uso e de indicadores de dependência, que não é reproduzida aqui: este texto trata de política e de relações internacionais.

2 REFERENCIAL TEÓRICO

2.1 Soberania digital e poder estrutural

A soberania digital é um conceito polissêmico. Pohle e Thiel (2020) a descrevem como um conjunto de reivindicações de controle sobre infraestruturas, dados e regras, e Floridi (2020) a trata como disputa entre Estados, empresas e cidadãos pelo controle de sistemas digitais. Strange (1988) define poder estrutural como a capacidade de

moldar as estruturas de segurança, produção, finanças e conhecimento em que os demais atuam, e a ideia é útil para a IA, porque desloca a atenção da posse de modelos para o controle das condições que os tornam possíveis: semicondutores, energia, centros de dados, conectividade e padrões. Farrell e Newman (2019) mostram que redes assimétricas dão aos Estados que hospedam nós centrais a capacidade de extrair informação e de negar acesso, o que explica por que concentrações de infraestrutura, como a dos cabos submarinos em Fortaleza, são ao mesmo tempo vantagem e vulnerabilidade.

2.2 Dependência e colonialismo de dados

Couldry e Mejias (2019) propuseram a noção de colonialismo de dados para descrever a apropriação de dados e de seu valor por poucas empresas e Estados. A literatura do Sul Global usa esse quadro crítico para analisar a dependência em infraestrutura, plataformas e modelos de IA (BELLI, 2025). Para a política pública, a implicação é que depender de fornecedores externos não é problema em si, mas passa a sê-lo quando concentra poder de decisão em um único fornecedor ou jurisdição e reduz a capacidade de negociar, auditar ou sair.

2.3 Soberania em IA

Mügge (2024) mostra que a "soberania em IA" abriga objetivos conflitantes e que a política europeia priorizou a independência jurisdicional sobre a soberania dos cidadãos. Belli (2025), ao apresentar um conjunto de estudos sobre os países do BRICS, examina como esses países combinam dados, computação, capacidade algorítmica, conectividade, energia, qualificação e regulação para construir soberania em IA. Singh e Sengupta (2025) modelam a soberania em IA como contínuo e concluem que a abertura moderada, com salvaguardas, supera a estratégia de isolamento. Malagon et al. (2025), em preprint, estimam que treinar no Brasil e no México um modelo de 10 trilhões de tokens é fiscalmente viável, a US$ 8 a 14 milhões com aceleradores

H100 e US$ 19 a 32 milhões com A100, considerada uma tarifa de importação de 16% sobre GPUs no caso brasileiro. A mensagem comum é que soberania não exige competir na fronteira tecnológica, mas garantir capacidade “suficiente”, auditável e sob controle de decisão.

2.4 Interdependência gerenciada e soberania cooperativa

O artigo adota a interdependência gerenciada como ponto de partida: o desafio contemporâneo não é eliminar a interdependência tecnológica, mas gerenciá-la de modo compatível com a soberania nacional, preservando a capacidade de decisão sobre dados, modelos, infraestruturas críticas e serviços essenciais. Propõe-se, a partir dela, o conceito de soberania cooperativa: um modelo em que o Estado retém autoridade de decisão sobre ativos estratégicos (dados críticos, chaves criptográficas, governança operacional e decisões sobre infraestruturas críticas) e, ao mesmo tempo, participa de pesquisa conjunta, padrões de interoperabilidade, iniciativas abertas de segurança e validação colaborativa de tecnologias confiáveis. O termo é proposta conceitual deste artigo, e não conceito consolidado na literatura. Três equivalências o delimitam: soberania não é isolamento, não é nacionalismo tecnológico e é a capacidade de decidir.

3 METODOLOGIA

O estudo é qualitativo, de caráter exploratório e descritivo, e adota a análise documental como técnica principal. O corpus reúne três grupos de fontes: (a) instrumentos federais brasileiros publicados entre 2021 e 2026, entre eles leis, decretos, portarias, instruções normativas, planos e programas; (b) documentos oficiais e legislação de outros países e blocos; e (c) literatura acadêmica de 2021 a 2026, tratada como revisão narrativa, com obras anteriores apenas quando fundamentais para o conceito. A busca ocorreu em outubro e novembro de 2026, em portais oficiais, diários oficiais, repositórios de preprints e portais acadêmicos abertos. Para alguns

atos recentes, a primeira informação veio de imprensa especializada e foi confirmada, sempre que possível, no texto oficial.

Cada instrumento foi analisado segundo três critérios: o objeto sobre o qual atua (dado, infraestrutura, modelo, norma ou pessoa), o mecanismo de que se vale (investimento, regulação, certificação, compra pública ou cooperativa) e a atitude diante da cooperação internacional (restritiva, condicionada ou aberta). A comparação internacional é qualitativa e não classifica países. São limites do estudo a ausência de busca estruturada em bases indexadas, a dependência de fontes secundárias para parte das informações de outros países e o fato de que a análise é documental e não avalia a implementação dos instrumentos. O autor atua na área de segurança da informação e de defesa, o que facilita o acesso às fontes e exige cautela para não tratar como fato o que é interpretação; as opiniões são pessoais e não expressam posição oficial de qualquer instituição.

4 O ARRANJO BRASILEIRO DE SOBERANIA EM IA (2021–2026)

4.1 Estratégia, investimento e infraestrutura

O Plano Brasileiro de Inteligência Artificial (PBIA) prevê R$ 23 bilhões entre 2024 e 2028 (MCTI, 2024). Em 2026, três anúncios deram forma à infraestrutura: um supercomputador de 7.200 petaflops no Rio Grande do Norte, de cerca de R$ 1 bilhão, cujo edital prevê transferência de tecnologia, capacitação, pesquisa e desenvolvimento, conteúdo local e participação de fornecedores brasileiros; uma infraestrutura de supercomputação no Rio de Janeiro, de R$ 1,276 bilhão, a ser implantada pela Rede Nacional de Ensino e Pesquisa em colaboração com as empresas Huawei e iFlytek, com um grande modelo de linguagem em português e operação prevista para julho de 2027; e uma parceria público-privada, a “Nuvem Brasileira”, reunindo o Ministério da Gestão e da Inovação, a ABDI, o Serpro e o BNDES. O pacote inclui ainda uma frente de chips de arquitetura aberta RISC-V em Campinas e um centro nacional de

transparência algorítmica e IA confiável, na UFMG (MOVIMENTO ECONÔMICO, 2026). O desenho já pressupõe interdependência: parte da infraestrutura nacional depende de parceiros estrangeiros em hardware e em tecnologia.

4.2 Cibersegurança e segurança da informação

A Política Nacional de Cibersegurança (Decreto nº 11.856/2023) foi desdobrada na Estratégia Nacional de Cibersegurança (E-Ciber, Decreto nº 12.573/2025), com cerca de quarenta ações e quatro eixos, um deles dedicado à soberania nacional e à governança (BRASIL, 2023a; 2025a). O Decreto nº 12.572/2025 trata da governança da segurança da informação nos órgãos federais (BRASIL, 2025b). O Programa de Privacidade e Segurança da Informação 2.0 (PPSI 2.0, Portaria SGD/MGI nº 9.511/2025) incorporou a soberania entre seus valores, tornou anuais os ciclos de avaliação e atribui à alta administração o dever de prover os recursos necessários (BRASIL, 2025c). A Instrução Normativa GSI/PR nº 5/2021 fixa requisitos mínimos de segurança para o uso de computação em nuvem na administração federal (BRASIL, 2021).

4.3 Proteção de dados

A Lei Geral de Proteção de Dados (Lei nº 13.709/2018) não se aplica ao tratamento realizado para fins exclusivos de defesa nacional, segurança do Estado e segurança pública (art. 4º, III), e prevê multas de até 2% do faturamento, limitadas a R$ 50 milhões por infração (art. 52) (BRASIL, 2018). A Resolução CD/ANPD nº 19/2024 regulamentou a transferência internacional de dados e concedeu doze meses para a adoção das cláusulas-padrão contratuais (ANPD, 2024), de modo que hospedar dados pessoais em provedor estrangeiro passou a ter custo jurídico explícito. Pesquisa anterior do autor sobre anonimização mostrou que técnicas como supressão, mascaramento e substituição podem ser insuficientes quando bases anonimizadas são cruzadas com fontes abertas, o que exige ambientes controlados e governança de dados (FERREIRA et al., 2022).

4.4 As normas setoriais de 2026 e o marco de IA

Em 2026, três atos aplicaram a lógica da classificação à IA. A Portaria MGI nº 3.485/2026, de 24 de abril, instituiu a política de governança de IA do ministério e restringiu o uso de ferramentas externas de IA generativa a informações públicas, vedando dados sigilosos ou pessoais, salvo situações autorizadas após análise de risco (BRASIL, 2026c; CONVERGÊNCIA DIGITAL, 2026). A Portaria GAB CHEC-MD nº 3.742/2026, de 13 de julho, determinou que, nas atividades acadêmicas das duas instituições de ensino superior do Ministério da Defesa, informações classificadas, operacionais, sigilosas ou de acesso restrito só sejam tratadas em ambientes institucionais controlados e autorizados, vedou seu envio a serviços de nuvem pública externa e mandou avaliar residência de dados, jurisdição e retenção de comandos nas ferramentas (BRASIL, 2026b). A Portaria SGD/MGI nº 5.921/2026, de 22 de julho, ampliou de 14 para 20 os perfis profissionais de referência nas contratações de operação de infraestrutura, criou o de especialista em infraestrutura de IA e, desde 1º de setembro de 2026, exige autorização expressa para que a contratada use ferramentas de IA, sem constituir regulação geral do uso de IA pela administração (BRASIL, 2026a; CARDOSO, 2026).

No plano legislativo, o Projeto de Lei nº 2.338/2023 foi aprovado pelo Senado em dezembro de 2024 e tramita na Câmara dos Deputados, de modo que, em outubro de 2026, o país ainda não dispõe de lei geral de IA (BRASIL, 2023b).

4.5 Fortaleza como nó de infraestrutura

O arranjo tem uma dimensão territorial. Fortaleza abriga 17 cabos submarinos e concentra, segundo a Anatel, mais de 90% do fluxo internacional de dados do país, e a Operação Tridente, exercício interagências de novembro de 2025, mobilizou 385 militares e 23 meios navais, com a participação de órgãos de segurança, da Anatel e de empresas do setor (RIBEIRO; MOREIRA, 2026). Esse trabalho anterior mostrou que a concentração em um ponto é, a um só tempo, vantagem geopolítica e vulnerabilidade,

o que reforça a leitura de Farrell e Newman (2019) sobre nós centrais. Aqui interessa apenas a lição de política: a soberania em IA depende também de infraestrutura física e de coordenação entre Forças Armadas, reguladores e empresas.

4.6 Antecedentes do setor de inteligência e de defesa: dados e compartilhamento

Trabalhos anteriores do autor oferecem três antecedentes brasileiros para o arranjo descrito. O primeiro é o compartilhamento de dados no Sistema Brasileiro de Inteligência (Sisbin), que reunia 48 órgãos em 2021. Um levantamento com 137 servidores de 13 órgãos do sistema mostrou que 98% dos que opinaram consideravam fundamentais o controle do fluxo de comunicação e o uso da gestão de riscos para decidir sobre a nuvem, mas apenas 38% julgavam a plataforma então usada capaz de atender ao critério de oportunidade (RIBEIRO; NUNES; ALBUQUERQUE, 2022; RIBEIRO, 2023). Os resultados não são reapresentados aqui; importa que a demanda por controle e por rastreabilidade veio de quem opera o sistema, antes das normas de 2026.

O segundo antecedente é o limite jurídico imposto pelo Supremo Tribunal Federal ao compartilhamento estatal de dados. Na ADI nº 6529, a Corte decidiu que os órgãos do Sisbin só podem fornecer dados à Abin quando comprovado o interesse público, mediante decisão motivada, que dados de comunicações telefônicas ou sujeitos à reserva de jurisdição não podem ser compartilhados e que é imprescindível haver procedimento formal e sistemas eletrônicos de segurança e de registro de acesso, inclusive para responsabilização por omissão, desvio ou abuso. Em 2020, o Tribunal já suspendera a Medida Provisória nº 954, que previa o compartilhamento de dados de usuários de telefonia com o IBGE, e reconhecera um direito autônomo à proteção de dados pessoais (ADI nº 6387, 6388, 6389, 6390 e 6393) (RIBEIRO, 2023). A jurisprudência atua, assim, como salvaguarda do cidadão justamente onde a LGPD não alcança o tratamento para fins de defesa e segurança do Estado.

O terceiro antecedente é o da soberania de operação em nuvem. Segundo análise anterior do autor, as normas complementares do GSI/PR já exigiam que as

contratações de nuvem previssem a residência dos dados e informações exclusivamente em território nacional, incluindo réplicas e cópias de segurança, e que serviços de TIC capazes de comprometer a segurança nacional fossem contratados junto a órgãos da administração federal ou operados como serviços próprios, sem compartilhamento ou contratação de terceiros (RIBEIRO, 2023). O país tem ainda uma base de criptografia de Estado: a Plataforma Criptográfica Portátil, desenvolvida pelo Centro de Pesquisa e Desenvolvimento para a Segurança das Comunicações (Cepesc) da Abin, está em uso desde o fim de 2007 (RIBEIRO, 2023). Esses elementos mostram que a ideia de soberania sobre dados e chaves não é nova na política brasileira; os atos de 2026 a estendem à IA generativa. As referências às normas e às decisões do Supremo são feitas aqui por meio do trabalho citado e devem ser conferidas nos textos primários.

No plano da fronteira, o Sistema Integrado de Monitoramento de Fronteiras (Sisfron), que cobre 16.885 quilômetros e dez países vizinhos, foi analisado como caso de compartilhamento de dados e de uso dual entre Forças Armadas, segurança pública e empresas privadas, com potencial para fomentar tecnologias de defesa de aplicação comercial (RIBEIRO et al., 2023).

Quadro 1 – Síntese do arranjo brasileiro por dimensão (2021–2026)

Dimensão	Instrumentos	Lógica de soberania	Lacuna
Investimento e infraestrutura	PBIA; supercomputador no RN; infraestrutura no RJ; Nuvem Brasileira	Capacidade pública de computação com parceiros externos	Acesso de órgãos pequenos a serviços compartilhados
Cibersegurança e segurança da informação	Decretos 11.856/2023, 12.572 e 12.573/2025; PPSI 2.0; IN GSI/PR 5/2021	Soberania como eixo e como valor de programa	Falta de instrumento que gradue exigências por tipo de dado
Proteção de dados	LGPD; Res. CD/ANPD 19/2024	Custo jurídico para transferência internacional	Exceção de defesa e segurança do Estado na LGPD
Regulação de IA	PL 2.338/2023 em tramitação	A definir	Ausência de lei geral
Normas setoriais de 2026	Portarias MGI 3.485, CHEC-MD 3.742 e SGD/MGI 5.921	Classificação do dado define onde a IA pode operar	Não indicam como processar dado protegido com IA em ambiente controlado

Fonte: Autor (2026)

5 TRÊS TENSÕES DO ARRANJO

5.1 Soberania jurisdicional e soberania do cidadão

Mügge (2024) alerta que a soberania jurisdicional do Estado pode deslocar a soberania dos cidadãos sobre seus dados. No arranjo brasileiro, a tensão aparece em dois pontos. O primeiro é a exceção da LGPD para tratamento com fins exclusivos de defesa, segurança do Estado e segurança pública, de modo que as salvaguardas que a lei dá ao titular deixam de valer justamente onde o poder do Estado sobre os dados é maior. O segundo é que as normas de 2026 protegem a informação do Estado contra provedores externos, mas pouco dizem sobre como o cidadão pode verificar o que o próprio Estado faz com a IA. O centro nacional de transparência algorítmica anunciado em 2026 aponta nessa direção, e a ANPD tem papel natural na fiscalização. A decisão do Supremo na ADI nº 6529, que exige procedimento formal, motivação e registro de acesso para o compartilhamento de dados de inteligência, indica o tipo de salvaguarda equivalente que a política pode generalizar (seção 4.6). Sem essas salvaguardas, a soberania apenas transfere o risco de um operador estrangeiro para um operador nacional.

5.2 Autonomia e interdependência

O arranjo brasileiro combina metas de autonomia e parcerias externas: o supercomputador do Rio Grande do Norte exige transferência de tecnologia, mas depende de fornecedores globais; a infraestrutura do Rio de Janeiro envolve fornecedores chineses; a Nuvem Brasileira é público-privada. Há ainda o custo da dependência: Malagon et al. (2025) mostram que tarifas de importação de GPUs, energia e câmbio pesam no custo da capacidade soberana. O caso brasileiro mostra que a pergunta pertinente é como gerir a interdependência, com diversificação de fornecedores, verificação independente e controle nacional de dados e chaves, e não como eliminá-la. É a interdependência gerenciada de Singh e Sengupta (2025) aplicada à política pública.

5.3 Política declaratória e capacidade operacional

Anúncios de investimento e normas de classificação não bastam se quem opera a segurança na ponta não tem pessoas, orçamento e ciclos de compra compatíveis. Em encontro nacional de profissionais de TIC de um sistema de conselhos profissionais, realizado em 2026, os palestrantes e os participantes relataram que a coordenação de infraestrutura e segurança do conselho federal contava com dois analistas, que as compras levavam de seis meses a mais de um ano, que ferramentas de IA eram adotadas sem conhecimento da área de TI e que conselhos regionais pequenos não alcançavam firewalls de nova geração com IA (comunicação oral). Esses relatos, não verificados de forma independente, coincidem com dados de mercado: a IBM estimou o custo médio de uma violação no Brasil em R$ 7,19 milhões em 2025 e em R$ 7,44 milhões em 2026, e em 2025 apontou acréscimo de cerca de R$ 591 mil associado ao uso não autorizado de IA e de R$ 725 mil à complexidade das ferramentas de segurança, além de que apenas 29% das organizações brasileiras usavam tecnologia de governança de IA (IBM, 2025; 2026). A Portaria SGD/MGI nº 5.921/2026 mostra que um instrumento pode alcançar o operador, ao exigir autorização para o uso de IA por contratadas. A tensão, portanto, é de desenho: normas que exigem salvaguardas devem vir acompanhadas de serviços compartilhados e de instrumentos de compra que as tornem viáveis para os órgãos menores.

6 COMPARAÇÃO INTERNACIONAL DAS ESTRATÉGIAS DE SOBERANIA

O Quadro 2 compara, de modo qualitativo, a estratégia dominante em cada jurisdição, os instrumentos principais e a lição para o Brasil. A comparação não classifica países: busca identificar tipos de estratégia e o lugar da cooperação em cada um.

Quadro 2 – Estratégias de soberania em IA e lições para o Brasil

Jurisdição	Estratégia dominante	Instrumentos	Lição para o Brasil
União Europeia	Soberania avaliável e usada em compras	Cloud Sovereignty Framework v1.2.1 (out. 2025), com oito objetivos, 48 critérios e níveis SEAL 0 a 4, sendo o nível global o do objetivo mais fraco; Regulamento (UE) 2024/1689; Gaia-X	Níveis explícitos de soberania podem orientar a compra pública
Índia	Capacidade pública e infraestrutura digital	IndiaAI Mission; infraestrutura pública digital; lei de proteção de dados de 2023, com transferências livres exceto para países notificados	Combinar capacidade pública e regras de transferência
China	Controle territorial	Leis de Cibersegurança (2017; alterada em out. 2025), de Segurança de Dados (2021) e de Proteção de Informações Pessoais (2021)	Modelo que coloca a cooperação em segundo plano; contraponto, não referência
Japão	Segurança econômica e nuvem avaliada	Lei de Promoção da Segurança Econômica (2022); programa ISMAP; Lei de promoção de IA (aprovada em 28 mai. 2025, em vigor em 4 jun. 2025), sem sanções	Avaliação de nuvem governamental e regulação leve de IA
Coreia do Sul	Regulação de IA e modelos nacionais	AI Basic Act (promulgada em 21 jan. 2025; em vigor em 22 jan. 2026); iniciativas de modelos nacionais	Regulação e capacidade de modelos andam juntas
Canadá	Capacidade pública de computação	Estratégia de Computação Soberana em IA (dez. 2024), com C$ 2 bilhões em cinco anos	Investimento público em computação como base
Austrália	Certificação de hospedagem por controle	Hosting Certification Framework (mar. 2021), com níveis Certified Strategic e Certified Assured	Certificar por condições de propriedade e controle, não por nacionalidade
Nigéria	Soberania linguística	Modelo N-ATLAS (2025), construído sobre um modelo aberto externo	Soberania linguística não elimina a dependência do modelo-base
Brasil	Arranjo misto, declaratório e de classificação	PBIA; E-Ciber; PPSI 2.0; atos de 2026	Falta graduação por tipo de dado e indicadores públicos

Fonte: Autor (2026)

Nota: Sobre as normas de outros países citadas no Quadro 2: UNIÃO EUROPEIA, **Regulamento (UE)** 2024/1689, https://eur-lex.europa.eu/eli/reg/2024/1689/oj; **ÍNDIA**, Digital Personal Data Protection Act, 2023, https://www.indiacode.nic.in/bitstream/123456789/22037/2/a2023-22.pdf; **CHINA**, Data Security Law, https://digichina.stanford.edu/work/translation-data-security-law-of-the-peoples-republic-of-china, e Personal Information Protection Law, https://digichina.stanford.edu/work/translation-personal-information-protection-law-of-the-peoples-republic-of-china-effective-nov-1-2021/; **JAPÃO**, Lei nº 53 de 2025, https://www.japaneselawtranslation.go.jp/en/laws/view/5066/en; **COREIA DO SUL**, Framework Act on the Development of Artificial Intelligence and the Creation of a Foundation for Trust, https://www.law.go.kr/LSW/eng/engLsInfoR.do?lsiSeq=268543.

Quatro padrões emergem:

Primeiro, as estratégias mais maduras separam o que o Estado precisa controlar do que pode comprar: a Austrália e a União Europeia certificam o provedor por condições de propriedade, operação e controle, e não por nacionalidade (COMISSÃO EUROPEIA, 2025; AUSTRALIAN GOVERNMENT, 2021);

Segundo, a capacidade pública de computação é comum a economias avançadas e emergentes, como Canadá, Índia e Brasil (GOVERNMENT OF CANADA, 2024; SINGH; SENGUPTA, 2025);

Terceiro, a soberania linguística, como no caso nigeriano, dá autonomia cultural, mas pode manter a dependência do modelo-base (NCAIR, 2025);

Quarto, os modelos de controle territorial, como o chinês, colocam a cooperação em segundo plano, o que os distingue da abordagem aqui defendida. O Brasil tem elementos dos três primeiros, mas ainda não tem o instrumento que a União Europeia e a Austrália adotaram: níveis explícitos de exigência, ligados a critérios verificáveis.

7 SOBERANIA COOPERATIVA E DIRETRIZES DE POLÍTICA PÚBLICA

7.1 A cooperação como habilitadora da soberania

A soberania computacional não deve ser lida como autarquia tecnológica. As infraestruturas digitais são interconectadas, e os avanços em computação confidencial, segurança de IA, projeto de semicondutores, criptografia pós-quântica e sistemas multiagentes seguros emergem cada vez mais de colaboração científica internacional. O objetivo de uma IA soberana não é eliminar dependências internacionais, mas garantir que a cooperação não comprometa o controle nacional sobre dados sensíveis, chaves criptográficas, governança operacional e decisões estratégicas. Nesse sentido, parcerias entre governos, universidades, centros de pesquisa e indústria são complementares à soberania: pesquisa conjunta, padrões de interoperabilidade, iniciativas abertas de segurança e validação colaborativa de tecnologias confiáveis aceleram a inovação e preservam a autonomia sobre infraestruturas críticas.

Há programas que tratam a segurança de IA como esforço conjunto entre governo, academia e indústria. O Instituto Nacional de Padrões e Tecnologia dos Estados Unidos conduziu, em processo aberto, a padronização de algoritmos de criptografia pós-quântica, concluída em 2024 (NIST, 2024). A DARPA e a National Science Foundation lançaram em 2026 o AI Forge, que reúne universidades, indústria e governo em pesquisa pré-competitiva sobre interpretabilidade, controle e robustez de IA, ainda que o programa seja de segurança nacional e aberto a universidades norte-americanas, de modo que ilustra um modelo de governança, e não participação internacional (DARPA; NSF, 2026). Seis agências nacionais de cibersegurança, entre elas as dos Estados Unidos, do Reino Unido, do Canadá, da Austrália e da Nova Zelândia, publicaram em 2026 a primeira orientação conjunta sobre o uso seguro de agentes de IA (CISA et al., 2026), e o protocolo A2A de comunicação entre agentes passou à governança neutra da Linux Foundation (LINUX FOUNDATION, 2025).

A soberania cooperativa se sustenta pela governança e pelo controle: o Estado compartilha pesquisa, código aberto, referências de avaliação e contribuições a padrões, e retém as chaves criptográficas, os dados críticos, o controle das instalações e as decisões operacionais. O modelo é aplicável a qualquer democracia, do Sul Global a economias avançadas; o Brasil é um caso, e não uma premissa. No caso brasileiro, há base institucional para a retenção de chaves e para a criptografia de Estado, como a Plataforma Criptográfica Portátil do Cepesc/Abin (RIBEIRO, 2023), que a cooperação internacional pode complementar sem substituir.

7.2 Sete diretrizes

A análise do arranjo, das tensões e da comparação sugere sete diretrizes.

D1. Graduar as exigências pela classificação do dado. Estender a política federal a lógica dos atos de 2026, com níveis que vão do dado público ao classificado, e ligar a cada nível exigências de infraestrutura, operação e controle de chaves, em vez de proibições uniformes.

D2. Abrir um caminho técnico e normativo para processar dado protegido com IA em ambiente controlado. Os atos de 2026 dizem onde o dado protegido não pode ir, mas não como pode ser processado com IA dentro de ambiente institucional. Cabe à política indicar padrões técnicos nacionais para esse caso, a serem detalhados por órgãos de padronização.

D3. Oferecer serviços compartilhados e instrumentos de compra aos órgãos menores. Catálogos padronizados, compras centralizadas e serviços federados reduzem o custo marginal das salvaguardas e respondem à tensão entre norma e capacidade.

D4. Publicar indicadores de dependência. Indicadores abertos, com metodologia transparente e comparáveis no tempo, permitem decidir o que repatriar e o que manter com salvaguardas, em linha com a abordagem objetivo a objetivo da União Europeia.

D5. Diversificar fornecedores e exigir verificação independente. A soberania se protege com pluralidade de origem, certificação por controle e verificação por terceiros, e não com a escolha de um único fornecedor, nacional ou estrangeiro.

D6. Proteger o cidadão do uso estatal da IA. Auditoria independente, transparência algorítmica e fiscalização pela ANPD devem valer também onde a LGPD não se aplica, com salvaguardas equivalentes.

D7. Participar ativamente de pesquisa, padrões e validação internacionais. O Brasil deve integrar fóruns de padronização e programas colaborativos, mantendo governança nacional sobre chaves, dados críticos e decisões operacionais, e propor uma agenda internacional de pesquisa em computação confidencial, IA confiável, sistemas multiagentes seguros, criptografia pós-quântica e métodos de avaliação de IA soberana.

8 CONSIDERAÇÕES FINAIS

O Brasil avançou, entre 2021 e 2026, em estratégia, infraestrutura e normas: tem um plano nacional de IA, investimentos em supercomputação e nuvem, uma estratégia de cibersegurança com eixo de soberania, um programa federal que trata a soberania como valor e atos setoriais que ligam o uso de IA à classificação da informação. O arranjo, contudo, apresenta três tensões: entre a soberania jurisdicional do Estado e a soberania do cidadão, entre a meta de autonomia e a interdependência com fornecedores estrangeiros e entre a política declaratória e a capacidade operacional dos órgãos menores. A comparação internacional mostra que outros países resolveram parte dessas tensões com níveis explícitos de exigência, certificação por controle e capacidade pública de computação.

O artigo defende a soberania cooperativa como orientação de política: reter a capacidade de decidir sobre dados, chaves, operações e escolhas estratégicas e, ao mesmo tempo, cooperar em pesquisa, padrões e validação. As sete diretrizes concretizam essa orientação. Como limites, o estudo é documental e não avalia a implementação dos instrumentos, depende em parte de fontes secundárias para outros países e não esgota a literatura. Como agenda, propõem-se estudos de implementação dos atos de 2026, a construção de indicadores públicos de dependência e a comparação sistemática de estratégias de soberania em países do Sul Global.

REFERÊNCIAS

ANPD. **Resolução CD/ANPD nº 19, de 23 de agosto de 2024**. Aprova o Regulamento de Transferência Internacional de Dados. Brasília: ANPD, 2024.

AP NEWS. **Trump's sanctions on ICC prosecutor have halted tribunal's work**. 2025. Disponível em: https://apnews.com/article/icc-trump-sanctions-karim-khan-court-a4b4c02751ab84c09718b1b95cbd5db3. Acesso em: 2 nov. 2026.

AUSTRALIAN GOVERNMENT. Digital Transformation Agency. **Hosting Certification Framework**. Canberra: DTA, mar. 2021. Disponível em: https://www.dta.gov.au/our-projects/hosting-strategy/hosting-certification-framework. Acesso em: 2 nov. 2026.

BELLI, L. How are BRICS countries building AI sovereignty? Introduction to thematic section. **African Journal of Information and Communication**, n. 35, p. 1-4, 2025. DOI: 10.23962/ajic.i35.23192.

BRASIL. **Decreto nº 11.856, de 26 de dezembro de 2023**. Institui a Política Nacional de Cibersegurança. Brasília, 2023a.

BRASIL. Senado Federal. **Projeto de Lei nº 2.338, de 2023**. Dispõe sobre o uso da inteligência artificial. Aprovado pelo Senado em 10 dez. 2024; em tramitação na Câmara dos Deputados. Brasília, 2023b.

BRASIL. **Instrução Normativa GSI/PR nº 5, de 30 de agosto de 2021**. Requisitos mínimos de segurança da informação para o uso de computação em nuvem pela administração pública federal. Brasília, 2021.

BRASIL. **Lei nº 13.709, de 14 de agosto de 2018**. Lei Geral de Proteção de Dados Pessoais (LGPD). Brasília, 2018.

BRASIL. **Decreto nº 12.573, de 4 de agosto de 2025**. Institui a Estratégia Nacional de Cibersegurança (E-Ciber). Brasília, 2025a.

BRASIL. **Decreto nº 12.572, de 4 de agosto de 2025**. Governança da segurança da informação nos órgãos da administração pública federal. Brasília, 2025b.

BRASIL. Ministério da Gestão e da Inovação em Serviços Públicos. **Portaria SGD/MGI nº 9.511, de 28 de outubro de 2025**. Institui o Programa de Privacidade e Segurança da Informação 2.0 (PPSI 2.0). Diário Oficial da União, Brasília, 28 out. 2025. Disponível em: https://www.in.gov.br/en/web/dou/-/portaria-sgd/mgi-n-9.511-de-28-de-outubro-de-2025-665815455. Acesso em: 2 nov. 2026.

BRASIL. Ministério da Gestão e da Inovação em Serviços Públicos. **Portaria SGD/MGI nº 5.921, de 22 de julho de 2026**. Diário Oficial da União, Brasília, 24 jul. 2026. Disponível em: https://www.in.gov.br/web/dou/-/portaria-sgd/mgi-n-5.921-de-22-de-julho-de-2026-721095205. Acesso em: 2 nov. 2026.

BRASIL. Ministério da Defesa. **Portaria GAB CHEC-MD nº 3.742, de 13 de julho de 2026**. Diário Oficial da União, Brasília, 14 jul. 2026. Disponível em: https://www.in.gov.br/web/dou/-/portaria-gab-chec-md-n-3.742-de-13-de-julho-de-2026-718721093. Acesso em: 2 nov. 2026.

BRASIL. Ministério da Gestão e da Inovação em Serviços Públicos. **Portaria MGI nº 3.485, de 24 de abril de 2026**. Política de Governança de Inteligência Artificial do MGI. Diário Oficial da União, Brasília, 28 abr. 2026. Disponível em: https://www.in.gov.br/web/dou/-/portaria-mgi-n-3.485-de-24-de-abril-de-2026-702070785. Acesso em: 2 nov. 2026.

CARDOSO, A. G. Inteligência artificial em contratos com a Administração Pública Federal: exigências da Portaria SGD/MGI nº 5.921/2026. **Informativo Eletrônico**, Justen, Pereira, Oliveira e Talamini, ed. 235, set. 2026. Disponível em: https://justen.com.br/artigo_pdf/inteligencia-artificial-em-contratos-com-a-administracao-publica-federal-exigencias-da-portaria-sgd-mgi-no-5-921-2026/. Acesso em: 2 nov. 2026.

CISA; NSA; ASD's ACSC; CANADIAN CENTRE FOR CYBER SECURITY; NCSC-NZ; NCSC-UK. **Careful adoption of agentic AI services**. Orientação conjunta, 1 maio 2026. Disponível em: https://cyber.gc.ca/en/news-events/joint-guidance-careful-adoption-agentic-artificial-intelligence-services. Acesso em: 2 nov. 2026.

COMISSÃO EUROPEIA. **Cloud Sovereignty Framework**. Versão 1.2.1. Bruxelas: DG DIGIT, out. 2025. Disponível em: https://commission.europa.eu/document/download/2ad80a48-166f-4c77-a513-80c53ca2a128_en. Acesso em: 2 nov. 2026.

CONVERGÊNCIA DIGITAL. **Reportagem sobre a política de governança de IA do Ministério da Gestão e da Inovação (Portaria MGI nº 3.485/2026)**. 2026. Disponível em: https://convergenciadigital.com.br/?p=51474. Acesso em: 2 nov. 2026.

COULDRY, N.; MEJIAS, U. A. **The costs of connection**: how data is colonizing human life and appropriating it for capitalism. Stanford: Stanford University Press, 2019.

DARPA; NSF. **AI Forge**. 2026. Disponível em: https://www.darpa.mil/research/programs/ai-forge. Acesso em: 2 nov. 2026.

FARRELL, H.; NEWMAN, A. L. Weaponized interdependence: how global economic networks shape state coercion. **International Security**, v. 44, n. 1, p. 42-79, 2019.

FERREIRA, J. R.; PINCOVSCY, J. A.; RIBEIRO, C. de M.; CANEDO, E. D.; MENDONÇA, F. L. L. de. Mitigação dos riscos à privacidade através da anonimização de dados. **RISTI – Revista Ibérica de Sistemas e Tecnologias de Informação**, n. E49, p. 573-585, abr. 2022.

FLORIDI, L. The fight for digital sovereignty: what it is, and why it matters, especially for the EU. **Philosophy & Technology**, v. 33, n. 3, p. 369-378, 2020.

GARTNER. **Gartner identifies the top strategic technology trends for 2026**. Comunicado de imprensa, 20 out. 2025.

GOVERNMENT OF CANADA. **Canadian Sovereign AI Compute Strategy**. Ottawa: Innovation, Science and Economic Development Canada, 2024. Disponível em: https://ised-isde.canada.ca/site/ised/en/node/271. Acesso em: 2 nov. 2026.

IBM. **Cost of a Data Breach Report 2025**. Armonk: IBM Security, 2025.

IBM. **Cost of a Data Breach Report 2026**. Armonk: IBM Security, 2026.

LEHDONVIRTA, V.; WÚ, B.; HAWKINS, Z. Compute North vs. Compute South: the uneven possibilities of compute-based AI governance around the globe. **Proceedings of the AAAI/ACM Conference on AI, Ethics, and Society**, v. 7, n. 1, p. 828-838, 2024. DOI: 10.1609/aies.v7i1.31683.

LINUX FOUNDATION. **Linux Foundation launches the Agent2Agent protocol project to enable secure, intelligent communication between AI agents**. Comunicado de imprensa, 23 jun. 2025.

MALAGON, S. et al. The feasibility of training sovereign language models in the Global South: a study of Brazil and Mexico. **arXiv**, 2510.19801, 2025.

MCTI. **Plano Brasileiro de Inteligência Artificial 2024-2028**. Brasília: Ministério da Ciência, Tecnologia e Inovação, 2024.

MOVIMENTO ECONÔMICO. **Supercomputador de R$ 1 bi no RN segue plano de soberania digital e IA no Brasil**. 20 ago. 2026. Disponível em: https://movimentoeconomico.com.br/tecnologia/2026/08/20/supercomputador-de-r-1-bi-no-rn-segue-plano-de-soberania-digital-e-ia-no-brasil/. Acesso em: 2 nov. 2026.

MÜGGE, D. EU AI sovereignty: for whom, to what end, and to whose benefit? **Journal of European Public Policy**, v. 31, n. 8, p. 2200-2225, 2024. DOI: 10.1080/13501763.2024.2318475.

NCAIR. **N-ATLAS multilingual language model**. Abuja: National Centre for Artificial Intelligence and Robotics, 2025. Disponível em: https://ncair.nitda.gov.ng/llm. Acesso em: 2 nov. 2026.

NIST. **FIPS 203, 204 e 205**: padrões de criptografia pós-quântica. Gaithersburg: National Institute of Standards and Technology, ago. 2024.

POHLE, J.; THIEL, T. Digital sovereignty. **Internet Policy Review**, v. 9, n. 4, 2020. DOI: 10.14763/2020.4.1532.

RIBEIRO, C. de M. **Uma proposta de otimização da comunicação sigilosa no Sisbin com o uso da computação em nuvem privada**. 2023. Dissertação (Mestrado Profissional em Engenharia Elétrica) – Faculdade de Tecnologia, Universidade de Brasília, Brasília, 2023.

RIBEIRO, C. de M.; ALBUQUERQUE, R. de O.; MENDES, F. F.; NUNES, R. R. O compartilhamento de dados e o uso dual do Sistema Integrado de Fronteiras do Exército Brasileiro. **RISTI – Revista Ibérica de Sistemas e Tecnologias de Informação**, n. E62, p. 130-142, out. 2023.

RIBEIRO, C. de M.; NUNES, R. R.; ALBUQUERQUE, R. de O. Um diagnóstico sobre o processo de comunicação sigilosa entre os órgãos do Sistema Brasileiro de Inteligência. **RISTI – Revista Ibérica de Sistemas e Tecnologias de Informação**, n. E49, p. 169-183, abr. 2022.

RIBEIRO, C.; MOREIRA, N. A. Cabos submarinos em Fortaleza: soberania digital e o papel do Exército Brasileiro. **InterAção**, Santa Maria, v. 17, n. 3, e97783, 2026. DOI: 10.5902/2357797597783.

SINGH, S. K.; SENGUPTA, S. Sovereign AI: rethinking autonomy in the age of global interdependence. **arXiv**, 2511.15734, 2025.

STRANGE, S. **States and markets**. London: Pinter, 1988.

TECHZINE. **Microsoft denies having suspended any services to ICC**. 2025. Disponível em: https://www.techzine.eu/news/privacy-compliance/131996/microsoft-denies-having-suspended-any-services-to-icc/. Acesso em: 2 nov. 2026.

THE REGISTER. **Microsoft admits it 'cannot guarantee' data sovereignty**. 25 jul. 2025. Disponível em: https://www.theregister.com/2025/07/25/microsoft_admits_it_cannot_guarantee/. Acesso em: 2 nov. 2026.

Autoria

1 Cileno de Magalhães Ribeiro

Formação militar em Comunicações pela Academia Militar das Agulhas Negras; Especialista em Telecomunicações e Guerra Eletrônica; Mestre em Operações Militares pela Escola de Aperfeiçoamento de Oficiais; Mestre em Engenharia Elétrica com concentração em Segurança Cibernética pela Universidade de Brasília; Assessor da Presidência da República, no Gabinete de Segurança Institucional e na Secretaria de Assuntos Estratégicos; Chefe do 52º Centro de Telemática

https://orcid.org/0000-0002-9329-1243 • cilenomag@gmail.com

Como citar este artigo

RIBEIRO, C. M. Soberania cooperativa em inteligência artificial: o arranjo brasileiro (2021–2026) e as lições do Sul Global. **InterAção**, Santa Maria, v. 17, n. 3, e99717, p. 1-21, 2026. DOI 10.5902/2357797599717. Disponível em: https://dx.doi.org/10.5902/2357797599717. Acesso em: dia mês abreviado. ano.

DECLARAÇÃO DE CONFLITO DE INTERESSES

O autor é oficial do Exército Brasileiro e chefia um centro de telemática do Exército que aparece em trabalho anterior sobre cabos submarinos. As opiniões são do autor e não expressam posição do Exército Brasileiro nem do Ministério da Defesa.