Localizar o servidor no Brasil não é suficiente para soberania digital

03/03/2026

Em outubro de 2025, a Anatel (Agência Nacional de Telecomunicações) publicou o *White Paper Data Centers*, consolidando estudos do seu Comitê de Infraestrutura ao longo de dois anos. Pela primeira vez, o regulador brasileiro trata a infraestrutura de processamento e armazenamento de dados como componente estratégico do ecossistema digital — e não apenas como apêndice das redes de telecomunicações.

Governo Federal

A preocupação central do *White Paper* é legítima: aproximadamente 60% da carga digital brasileira é processada em data centers no exterior, sobretudo nos Estados Unidos. Uma interrupção nessa dependência poderia paralisar o Pix, comprometer prontuários do SUS e derrubar sistemas de controle do transporte aéreo.

A resposta proposta é expandir a capacidade nacional, criar incentivos fiscais — o Redata, instituído pela MP nº 1.318/2025 —, elaborar um Plano Nacional de Data Centers e fortalecer a articulação entre Anatel, ANPD e GSI.

Tudo isso é necessário. Mas é insuficiente. E a insuficiência não é periférica — é estrutural. O White Paper protege o continente, mas não o conteúdo. Cuida de onde o servidor está, mas não de quem pode acessar o que nele se encontra. Dados estratégicos de empresas brasileiras de todos os perfis — estatais, beneficiárias de recursos públicos para inovação e empresas privadas — podem ser acessados por governos estrangeiros sem que o Brasil seja sequer notificado. E o ordenamento jurídico brasileiro não possui resposta para isso.

Quem está exposto e como

A exposição de dados estratégicos brasileiros ao acesso por governos estrangeiros não é hipótese acadêmica. É consequência direta de escolhas de infraestrutura que o mercado faz diariamente — e que o ordenamento brasileiro ainda não aprendeu a regular. Três categorias concentram o risco.

Empresas públicas e sociedades de economia mista operam em setores estratégicos — energia, defesa, saneamento, saúde, financeiro — e processam dados sensíveis em infraestruturas de nuvem com nexo jurisdicional nos Estados Unidos. Isso significa que esses dados estão ao alcance da *Cloud Act*, a lei que permite ao governo americano exigir de empresas com nexo jurisdicional americano o fornecimento de dados armazenados em qualquer jurisdição do mundo. A ordem é dirigida ao provedor. A estatal brasileira não é notificada. O Poder Executivo

não é consultado.

> *Uma estatal pode ter seu data center em São Paulo e ainda assim ter seus dados acessíveis ao governo americano — porque o provedor de nuvem que contratou é americano.*

O problema se agrava no ecossistema de inovação. O Brasil investe dezenas de bilhões de reais por ano em P&D por meio de fundos setoriais, subvenções e agências de fomento. Os resultados — dados experimentais, modelos de IA, segredos industriais pré-competitivos, pedidos de patente em sigilo — são armazenados majoritariamente em nuvem estrangeira.

Spacca

A Lei de Inovação, a Lei do Bem e os regulamentos das agências de fomento não impõem qualquer exigência sobre onde esses dados devem estar, quem pode acessá-los ou o que fazer se um governo estrangeiro os solicitar ao provedor. Dinheiro público brasileiro financia conhecimento que pode ser transferido a jurisdição estrangeira sem ciência do Brasil.

A exposição não se limita a quem recebe recursos do Estado. Qualquer empresa privada que contrate infraestrutura com nexo jurisdicional estrangeiro está sujeita ao mesmo risco. O risco jurídico é idêntico; varia a relevância estratégica dos dados. O mercado não resolveu o problema sozinho porque o risco é difuso e os custos de mitigação são imediatos. É exatamente para isso que existe regulação — e é exatamente isso que a política brasileira de data centers ainda não propõe.

O que o Brasil já tem. E por que não é suficiente

O Brasil construiu instrumentos relevantes. O Marco Civil da Internet (Lei nº 12.965/2014) afirma a aplicação da legislação brasileira a operações de tratamento de dados de brasileiros, mas não possui mecanismos de *enforcement* quando a ordem de acesso parte de governo estrangeiro dirigida ao provedor, e não à empresa brasileira. A LGPD (Lei nº 13.709/2018) protege dados pessoais em relações entre agentes privados e titulares, mas não alcança dados estratégicos não pessoais — segredos industriais, modelos de IA, dados de P&D — nem transferências coercitivas determinadas por governo estrangeiro. O R-Ciber (Resolução Anatel nº 767/2024) e a Resolução nº 780/2025 avançam na segurança cibernética de data centers vinculados a telecomunicações, mas não alcançam a maioria das empresas que contratam infraestrutura para outros fins.

O Redata (MP nº 1.318/2025) reduziu a carga tributária sobre data centers de 52% para 18%, mas suas contrapartidas são voltadas a sustentabilidade e P&D geral — nenhuma exige controle nacional efetivo sobre a infraestrutura ou proteção de dados estratégicos. A Lei de Inovação e a

Lei do Bem não condicionam recursos públicos a qualquer exigência de proteção dos dados gerados. A Estratégia Nacional de Cibersegurança (Decreto nº 10.222/2020) estabelece diretrizes para infraestruturas críticas, mas sem densidade normativa para impor obrigações concretas a operadores privados de data center.

> *O Brasil possui arcabouço normativo razoável para proteger dados pessoais em contextos relacionais entre privados. Não possui instrumentos adequados para proteger dados estratégicos — pessoais ou não — diante de ordens de governos estrangeiros dirigidas a provedores de infraestrutura.*

As lacunas que o White Paper não endereçou

Compreendido o problema concreto e avaliado o arcabouço existente, é possível identificar com precisão o que o White Paper deveria ter proposto — e não propôs.

Controle efetivo versus domicílio formal

O White Paper ancora a soberania digital na localização física da infraestrutura. Essa premissa ignora que a localização do servidor não determina quem controla as decisões sobre os dados nele armazenados. Uma empresa formalmente brasileira, pertencente a grupo multinacional, permanece alcançável pela legislação de seu controlador. Da mesma forma, uma empresa 100% brasileira que contrate provedor americano submete seus dados à jurisdição americana, porque é o provedor — e não ela — quem os detém fisicamente.

A solução não é proibir capital estrangeiro. É exigir, para operadores de infraestrutura crítica, autonomia decisória local demonstrável: gestão operacional independente, custódia nacional das chaves criptográficas, obrigação contratual de não cumprir ordens estrangeiras sem autorização judicial brasileira e governança que impeça interferência externa. É o mecanismo de ring-fencing que o Brasil já aplica em subsidiárias de bancos estrangeiros — e que ainda não transpôs para infraestrutura digital.

Regime específico para dados estratégicos de inovação

A Lei de Inovação, a Lei do Bem e os regulamentos das agências de fomento não condicionam recursos públicos a qualquer exigência de proteção dos dados gerados. Essa lacuna precisa ser preenchida com: obrigatoriedade de armazenamento em infraestrutura soberana ou com certificação de isolamento; criptografia com chaves custodiadas por entidade nacional; protocolo de notificação obrigatória às agências de fomento e ao INPI em caso de ordem estrangeira; e vedação de acesso remoto por entidades estrangeiras sem autorização judicial. Os modelos existem: o Health Data Hub francês e a Gaia-X Sovereign Cloud alemã demonstram que é possível construir ambientes computacionais soberanos para projetos financiados com recursos públicos.

Escudo jurisdicional contra ordens estrangeiras

O ordenamento brasileiro não possui mecanismo que obrigue operadores de data center a notificar autoridades nacionais ao receber ordens estrangeiras, nem que permita ao Estado contestá-las antes de seu cumprimento. O Brasil precisa de instrumento equivalente ao blocking statute europeu — o Regulamento (CE) nº 2271/96, que proíbe o cumprimento de decisões judiciais ou administrativas estrangeiras especificadas, sob pena de sanção —: cláusulas contratuais obrigatórias em contratos de data center para setores críticos, que imponham notificação imediata e não cumprimento de ordens estrangeiras sem autorização judicial brasileira. Esse instrumento não viola obrigações internacionais — é exercício legítimo de soberania jurisdicional.

Governança algorítmica para sistemas de inteligência artificial

O White Paper trata data centers como infraestrutura de armazenamento e processamento, sem abordar que essa infraestrutura é crescentemente utilizada para operar sistemas de IA de alto impacto sobre dados nacionais. O AI Act europeu, em vigor desde agosto de 2024, com implementação escalonada, demonstra que a regulação da IA como uso da infraestrutura é tão importante quanto a regulação da infraestrutura em si. O Brasil não possui regime específico de governança algorítmica: não exige documentação técnica de modelos de IA, não impõe logs auditáveis, não veda o uso de dados sensíveis brasileiros para treino de modelos controlados por entidades estrangeiras e não estabelece requisitos de portabilidade. O PL 2.338/2023, em tramitação no Senado como marco regulatório da IA, tampouco endereça a dimensão de infraestrutura soberana — lacuna que precisará ser suprida se o Brasil quiser que a governança algorítmica tenha efetividade material.

Prevenção de nova concentração de mercado

Se as beneficiárias do Redata forem predominantemente as grandes plataformas globais de nuvem, o Brasil terá substituído dependência geográfica por dependência estrutural. A Política Nacional de Data Centers precisa incorporar: limites à participação de mercado de um único provedor em infraestrutura crítica, obrigações de interoperabilidade e portabilidade para prevenir vendor *lock-in*, e regras de separação estrutural entre operadores de infraestrutura e prestadores de serviços — à semelhança do unbundling já praticado nos setores elétrico e de telecomunicações.

Direito e tecnologia: dois déficits que se alimentam

O Brasil sabe onde quer que os dados estejam — em solo nacional —, mas ainda não decidiu quem pode acessá-los, em que condições, sob qual lei e com quais garantias de resistência a ordens estrangeiras. O Marco Civil afirma a soberania, mas não a defende quando o vetor de acesso é o provedor estrangeiro.

A LGPD não alcança dados estratégicos não pessoais nem ordens transnacionais. O R-Ciber não se estende ao setor de data centers em geral. O Redata não condiciona incentivos a controle nacional efetivo. A Lei de Inovação não protege o conhecimento que financia. Nenhum desses instrumentos, isoladamente ou em conjunto, é suficiente.

Mas há uma segunda camada: a soberania digital tem um teto tecnológico. O Brasil tem capacidade real em software e governança — o Serpro, a Dataprev, a RNP e o PIX demonstram isso. A dependência é estrutural na camada de hardware: o país não produz semicondutores avançados nem GPUs.

Mesmo a nuvem soberana francesa opera sobre componentes não europeus. O teto existe independentemente da sofisticação do regime jurídico.

> *Qualquer regime jurídico de soberania de dados tem um teto tecnológico. Enquanto o Brasil não tiver capacidade de produção doméstica de componentes críticos, esse teto será definido por outros.*

A Política Nacional de Data Centers é a oportunidade de integrar as duas agendas que tramitam em paralelo sem se conversar: a jurídica — controle efetivo, escudo jurisdicional, governança algorítmica — e a de política industrial — capacidade doméstica em semicondutores, diversificação de suprimento tecnológico, produção nacional de componentes críticos.

O Redata exige contrapartidas em P&D, mas exigir investimento em pesquisa não é o mesmo que exigir desenvolvimento de capacidade tecnológica soberana. O Brasil tem capacidade jurídica e tecnológica parcial para construir soberania digital real. O que falta é a compreensão de que Direito e tecnologia são duas faces do mesmo problema — e que avançar em apenas uma delas é insuficiente.

Referências normativas e documentais

ANATEL. White Paper Data Centers. Brasília: Anatel, 2025.

BRASIL. Lei nº 10.973, de 2 de dezembro de 2004. Lei de Inovação.

BRASIL. Lei nº 11.196, de 21 de novembro de 2005. Lei do Bem.

BRASIL. Lei nº 12.965, de 23 de abril de 2014. Marco Civil da Internet.

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

BRASIL. Decreto nº 10.222, de 5 de fevereiro de 2020. Estratégia Nacional de Cibersegurança (E-Ciber).

BRASIL. Resolução Anatel nº 767, de 19 de dezembro de 2024. Regulamento de Segurança Cibernética (R-Ciber).

BRASIL. Resolução Anatel nº 780, de 2025.

BRASIL. Medida Provisória nº 1.318, de 17 de setembro de 2025. Regime Especial de Tributação para Serviços de Datacenter (Redata).

EUA. Clarifying Lawful Overseas Use of Data Act (CLOUD Act). Pub. L. 115-141, 2018.

EUA. CHIPS and Science Act. Pub. L. 117-167, 2022.

EUA. Executive Order 14117, de 28 de fevereiro de 2024. Regulamentada pela regra final do DOJ (Federal Register, 8 de janeiro de 2025).

UNIÃO EUROPEIA. Regulamento (UE) 2024/1689 (Artificial Intelligence Act). 13 de junho de 2024.

UNIÃO EUROPEIA. Regulamento (CE) nº 2271/96 do Conselho (Blocking Statute). 22 de novembro de 1996.

Fonte: https://conjur.jumps.com.br/2026-mar-03/localizar-o-servidor-no-brasil-nao-e-suficiente-para-soberania-digital/