

Desafios Estruturais da Nuvem de Governo para a Autonomia Tecnológica na Administração Pública Federal

Renato César Oliveira Viana¹, Robson de Oliveira Albuquerque¹

¹Universidade de Brasília (UnB)

Programa de Pós-Graduação Profissional em Engenharia Elétrica (PPEE)

Especialização em Privacidade e Segurança da Informação

renato.viana@aluno.unb.br, robson@redes.unb.br

Resumo: *Este artigo discute a Nuvem de Governo na Administração Pública Federal brasileira, examinando seus arranjos normativos e institucionais e os desafios estruturais à autonomia tecnológica. Adota-se abordagem qualitativa, fundamentada em revisão bibliográfica e análise documental de normas, atos institucionais, fiscalizações e comunicações oficiais. A decorrente análise documental evidencia que a Nuvem de Governo visa fortalecer a capacidade estatal de governança, ampliar a coordenação institucional e padronizar a prestação de serviços de computação em nuvem, contribuindo para ampliar a capacidade estatal de gestão sobre os ativos informacionais nela processados e armazenados. Entretanto, persistem desafios estruturais relacionados à dependência de tecnologias críticas, às cadeias globais de suprimentos, à crescente integração de serviços baseados em inteligência artificial, aos mecanismos de aprisionamento tecnológico, aos provedores globais de serviços digitais e ao fortalecimento das capacidades estatais necessárias para enfrentar essas dependências. Conclui-se que a Nuvem de Governo fortalece a capacidade estatal de governança sobre ambientes digitais estratégicos, sem eliminar os condicionantes estruturais da autonomia tecnológica, evidenciando que sua ampliação depende do desenvolvimento contínuo de capacidades estatais e da gestão estratégica dos riscos associados às dependências tecnológicas.*

Palavras-chave: *Nuvem de Governo. Autonomia Tecnológica. Governança Digital. Computação em Nuvem. Administração Pública Federal.*

Abstract: *This article discusses the Government Cloud initiative in the Brazilian Federal Public Administration, examining its regulatory and institutional arrangements and the structural challenges to technological autonomy. A qualitative approach was adopted, based on a literature review and documentary analysis of regulations, institutional acts, audit reports, and official communications. The documentary analysis indicates that the Government Cloud aims to strengthen the State's governance capacity, enhance institutional coordination, and standardize the provision of cloud computing services, thereby improving the State's ability to manage the information assets processed and stored within these environments. Nevertheless, structural challenges remain, including dependence on critical technologies, global supply chains, the increasing integration of artificial intelligence-based services, vendor lock-in mechanisms, global digital service*

providers, and the strengthening of State capabilities required to address these dependencies. It is concluded that the Government Cloud enhances the State's governance capacity over strategic digital environments without eliminating the structural constraints on technological autonomy, indicating that its further development depends on the continuous strengthening of State capabilities and the strategic management of risks associated with technological dependencies.

Keywords: *Government Cloud. Technological Autonomy. Digital Governance. Cloud Computing. Brazilian Federal Public Administration.*

1. Introdução

A implementação da Nuvem de Governo integra o conjunto de iniciativas voltadas ao fortalecimento da governança da computação em nuvem na Administração Pública Federal. Ao concentrar a prestação de serviços digitais em sua infraestrutura, o Estado brasileiro busca ampliar sua capacidade de gestão sobre esses serviços e sobre os ativos informacionais nela processados e armazenados. Contudo, sua operacionalização permanece apoiada, em parte, em plataformas, tecnologias e serviços desenvolvidos por grandes fornecedores globais, mantendo a Administração Pública Federal dependente de infraestruturas, softwares e ecossistemas tecnológicos controlados por terceiros.

Essa dependência impõe desafios à autonomia tecnológica do Estado, relacionados à concentração do mercado de tecnologias digitais, aos mecanismos de aprisionamento tecnológico (vendor lock-in), às limitações à portabilidade entre plataformas, à crescente integração de serviços baseados em inteligência artificial e à incidência de regimes jurídicos extraterritoriais sobre provedores internacionais. Mesmo com o fortalecimento da governança sobre ambientes digitais e a ampliação do controle estatal sobre a localização e a gestão dos dados, permanecem limitações estruturais relacionadas ao domínio das tecnologias, infraestruturas e plataformas que sustentam esses serviços [Mitchell e Samlidis 2021; Bellanova et al. 2022; Gu 2024; Silva et al. 2025].

Nesse contexto, a Nuvem de Governo constitui uma resposta institucional voltada ao fortalecimento da capacidade estatal de coordenar e supervisionar a infraestrutura e os serviços que a integram. Para esse fim, estrutura-se sobre um arranjo normativo e institucional que estabelece diretrizes para a classificação das cargas de trabalho, define a Nuvem de Governo como infraestrutura de nuvem privada ou comunitária gerida exclusivamente por órgãos ou empresas públicas e é complementado por Acordos de Cooperação Técnica que atribuem responsabilidades relacionadas à operação dos serviços, à segurança da informação, ao monitoramento contínuo e à governança dos ambientes computacionais [Brasil 2023; Brasil 2024a; Brasil 2024b; Brasil 2024c; Brasil 2024d].

A coexistência entre o fortalecimento da governança promovido pela Nuvem de Governo e a persistência das dependências tecnológicas torna relevante examinar em que medida essa iniciativa contribui para ampliar a capacidade estatal de governança sobre ambientes digitais estratégicos e quais são seus limites frente aos ecossistemas

digitais contemporâneos. Com esse propósito, este estudo analisa os arranjos normativos e institucionais que estruturam a Nuvem de Governo, por meio de abordagem qualitativa fundamentada em revisão bibliográfica e análise documental. Como principal contribuição, o trabalho oferece uma análise integrada da Nuvem de Governo sob a perspectiva da autonomia tecnológica, articulando dimensões normativas, institucionais, tecnológicas e geopolíticas para compreender seus avanços e limites.

O artigo está organizado em cinco seções. Após esta introdução, a primeira seção apresenta os fundamentos teóricos relacionados à soberania digital, à computação em nuvem e à Nuvem de Governo, bem como o contexto normativo e institucional que estrutura sua implementação. A segunda examina os limites estruturais da Nuvem de Governo, abrangendo limites tecnológicos; limites geopolíticos e capacidades estatais. A terceira desenvolve uma análise crítica da Nuvem de Governo, articulando seus avanços institucionais à gestão estratégica dos riscos associados às dependências tecnológicas e às suas implicações para o fortalecimento da autonomia tecnológica estatal. Por fim, são apresentadas as considerações finais do estudo.

2. Fundamentação Teórica

Esta seção apresenta os fundamentos teóricos necessários à análise da Nuvem de Governo no contexto da Administração Pública Federal brasileira. Inicialmente, são discutidos os conceitos de soberania digital e computação em nuvem. Em seguida, apresenta-se a Nuvem de Governo e seu marco normativo e institucional, estabelecendo a base teórica para a análise de seus impactos sobre a governança digital e a autonomia tecnológica.

2.1. Soberania digital

A soberania digital, embora apresente diferentes definições na literatura, fundamenta-se na capacidade de exercer controle sobre ambientes digitais em três camadas interdependentes: a camada física (infraestruturas, recursos e dispositivos); a camada de código (representada, neste estudo, por softwares, plataformas e demais componentes lógicos que estruturam os ambientes digitais); e a camada da informação (dados e conteúdos digitais) [Falkner et al. 2024]. Essa capacidade envolve a possibilidade de influenciar o desenvolvimento, o uso e os resultados das tecnologias digitais, de modo a preservar modelos específicos de governança [Falkner et al. 2024].

Essa compreensão também encontra respaldo em Roberts et al. (2021), que observam que o conceito de soberania digital passou a ocupar posição central na formulação das políticas digitais da União Europeia, embora permaneça empregado de forma heterogênea por diferentes instituições. Nessa perspectiva, para os autores, a soberania digital está associada à capacidade de o Estado exercer autoridade legítima sobre dados, softwares, serviços, padrões técnicos e demais infraestruturas digitais, preservando sua capacidade de implementar escolhas regulatórias, ainda que em um contexto de interdependências tecnológicas.

No contexto contemporâneo, o controle exercido sobre essas diferentes camadas não se restringe a aspectos técnicos, assumindo também dimensões políticas, econômicas e geopolíticas. O exercício desse poder manifesta-se na definição de regras, na coordenação de infraestruturas e plataformas digitais e na utilização dessas tecnologias como instrumentos de regulação, coordenação e segurança pelo Estado [Bellanova et al. 2022].

A crescente concentração de capacidades digitais em grandes corporações transnacionais ampliou os desafios ao exercício da soberania digital, uma vez que infraestrutura, plataformas e capacidades de inovação passaram a se concentrar em um número reduzido de fornecedores globais [Floridi 2020; Farrand e Carrapico 2022]. Como consequência, parcela significativa da evolução dos ambientes digitais passa a ser condicionada por decisões tomadas fora da esfera de atuação dos Estados, ampliando assimetrias na definição de padrões tecnológicos, funcionalidades e ciclos de inovação [Floridi 2020; Rone 2024].

Nesse contexto, a incorporação da inteligência artificial aos ecossistemas digitais amplia esses desafios, ao reforçar a necessidade de que os Estados desenvolvam capacidades estatais para governar tecnologias digitais estratégicas, além do controle sobre dados e infraestruturas [Roberts et al. 2021; Gu 2024]. Sob essa perspectiva, a inteligência artificial reforça a necessidade de que a soberania digital contemple a capacidade estatal de definir, implementar e supervisionar políticas públicas em ambientes digitais cada vez mais influenciados por essas tecnologias [Roberts et al. 2021; Floridi 2020].

No Brasil, a discussão sobre soberania digital insere-se no processo de transformação digital da Administração Pública e na crescente utilização de tecnologias providas por fornecedores globais. Conforme observam Silva et al. (2025), esse cenário evidencia que a construção da soberania digital não se restringe à proteção de dados ou à segurança da informação, envolvendo também a capacidade do Estado de desenvolver, coordenar e preservar competências institucionais, tecnológicas e produtivas que reduzam dependências externas em infraestruturas e serviços digitais considerados estratégicos.

No ambiente de computação em nuvem, essas dependências manifestam-se de forma particularmente intensa. A adoção de arquiteturas distribuídas e ecossistemas tecnológicos complexos dificulta o exercício do controle direto sobre componentes estratégicos e desloca a gestão da informação para componentes lógicos frequentemente intermediados por plataformas, softwares e serviços externos [von Scherenberg et al. 2024]. Para Estados em desenvolvimento, esse cenário evidencia os desafios de converter autoridade normativa em capacidade efetiva de coordenação tecnológica sobre ambientes digitais estratégicos [Gu 2024].

2.2. Computação em nuvem

A computação em nuvem constitui um modelo que permite o acesso sob demanda, por meio da rede, a um conjunto compartilhado e configurável de recursos computacionais, os quais podem ser rapidamente provisionados e liberados com mínimo esforço de gerenciamento ou interação com o provedor de serviços [NIST 2011; Cloud Security

Alliance 2024]. Esse modelo caracteriza-se pelo compartilhamento de recursos, rápida elasticidade e disponibilização de capacidade computacional conforme a demanda dos usuários, além de possibilitar a mensuração do consumo dos recursos utilizados. Também promove elevado nível de abstração da infraestrutura física, transferindo ao provedor parte significativa da responsabilidade pela operação, manutenção e gerenciamento do ambiente computacional, reduzindo o controle direto do usuário sobre a infraestrutura subjacente [NIST 2011; Cloud Security Alliance 2024].

Embora tecnicamente fundamentada em arquiteturas distribuídas, a computação em nuvem consolidou-se no mercado por meio de grandes provedores transnacionais, cujas plataformas passaram a desempenhar papel central na operação de infraestruturas estatais que suportam a governança de dados públicos estratégicos [Pierucci 2025; Jansen et al. 2023]. Essa concentração do mercado intensificou dependências tecnológicas estruturais, reduzindo a capacidade dos Estados de exercer controle sobre componentes críticos das infraestruturas digitais e fortalecendo as discussões contemporâneas sobre soberania digital e autonomia tecnológica [Pohle e Thiel 2020; Silva et al. 2025].

Ainda no campo conceitual, o National Institute of Standards and Technology (NIST) propôs uma classificação da computação em nuvem baseada em modelos de serviço e de implantação, que se consolidou como a principal referência da literatura especializada. Embora originalmente publicada em 2011, essa classificação continua sendo adotada por documentos técnicos recentes, como o Security Guidance v5 da Cloud Security Alliance (2024), além de permanecer compatível com os modelos descritos na norma ISO/IEC 22123-2:2023, que estabelece os conceitos fundamentais da computação em nuvem. As Tabelas 1 e 2 apresentam uma síntese desses modelos.

Tabela 1. Modelos de serviço
Fonte: NIST

Modelo	Descrição
Infraestrutura como Serviço	Disponibiliza recursos computacionais, como processamento, armazenamento e redes, permitindo ao usuário gerenciar sistemas operacionais e aplicações.
Plataforma como Serviço	Disponibiliza um ambiente para desenvolvimento, implantação e execução de aplicações, cabendo ao provedor gerenciar a infraestrutura subjacente.
Software como Serviço	Disponibiliza aplicações prontas para uso por meio da internet, sendo toda a infraestrutura e manutenção administradas pelo provedor.

Tabela 2. Modelos de implantação
Fonte: NIST

Modelo	Descrição
Nuvem pública	Infraestrutura disponibilizada ao público em geral e operada por um provedor de serviços.
Nuvem privada	Infraestrutura destinada ao uso exclusivo de uma única organização.
Nuvem comunitária	Infraestrutura compartilhada por organizações que possuem requisitos comuns de missão, segurança ou conformidade regulatória.
Nuvem híbrida	Combinação de dois ou mais modelos de implantação, mantendo interoperabilidade entre os ambientes.

Dentre os modelos de implantação, as nuvens privadas e comunitárias assumem especial relevância para este estudo, uma vez que a regulamentação da Nuvem de Governo estabelece que sua implementação ocorra nesses ambientes. Nessas infraestruturas, podem ser ofertados os diferentes modelos de serviço apresentados na Tabela 1, conforme as necessidades dos órgãos e entidades. Essas características constituem a base tecnológica que fundamenta a Nuvem de Governo, cuja estrutura normativa e institucional é apresentada na seção seguinte.

2.3. Nuvem de Governo

No contexto da Administração Pública Federal brasileira, a Nuvem de Governo consiste em uma infraestrutura de computação em nuvem destinada à hospedagem, ao processamento e à disponibilização de informações e serviços digitais considerados estratégicos para o Estado [Mitchell e Samlidis 2021; Serpro 2026]. Nos termos da Portaria SGD/MGI nº 5.950/2023, sua implementação ocorre em infraestrutura de nuvem privada ou comunitária, gerida exclusivamente por órgãos ou empresas públicas. Essa medida visa estruturar um ambiente de computação em nuvem capaz de atender requisitos específicos de segurança da informação, governança e proteção de dados [Brasil 2023; Brasil 2024a; Brasil 2024b; Brasil 2024c; Brasil 2024d].

A gestão exclusiva por órgãos ou empresas públicas constitui um elemento central desse arranjo, ao concentrar no Estado a responsabilidade pela governança, coordenação e supervisão da Nuvem de Governo. Todavia, essa exclusividade refere-se à responsabilidade pela gestão e não implica domínio sobre as tecnologias e plataformas que sustentam sua infraestrutura. Assim, embora a Nuvem de Governo fortaleça a capacidade estatal de governança sobre os serviços digitais e os ativos informacionais nela processados, sua implementação permanece condicionada às tecnologias empregadas e às cadeias globais de suprimentos das quais elas dependem sobre as quais o Estado não exerce controle pleno. [Mitchell e Samlidis 2021; Falkner et al. 2024; Gu 2024].

No caso da implementação da Nuvem de Governo pelo SERPRO, o Catálogo de Serviços descreve uma solução composta por infraestruturas de computação em nuvem baseadas em múltiplas *stacks* tecnológicas, hospedadas em centros de processamento de dados localizados em território nacional e geridas pela entidade, que atua como provedora dos serviços de computação em nuvem. Nessa implementação, a infraestrutura é estruturada para operar sob jurisdição brasileira, buscando assegurar que informações e cargas de trabalho sensíveis, confidenciais ou estratégicas permaneçam em conformidade com os requisitos legais relacionados à segurança da informação, à proteção de dados e à disponibilidade dos serviços [Serpro 2026].

2.4. Marco normativo e institucional da Nuvem de Governo

No caso brasileiro, a implementação da Nuvem de Governo insere-se em um marco institucional e regulatório voltado à proteção de dados, à segurança da informação e à transformação digital na Administração Pública Federal. Esse conjunto de diretrizes e instrumentos busca fortalecer a governança estatal sobre informações e serviços digitais

estratégicos, estabelecendo requisitos mais restritivos para o tratamento de dados sensíveis em ambientes de nuvem.

No plano regulatório, destacam-se normas que disciplinam a contratação e a gestão de serviços em nuvem sob critérios mais rigorosos de governança e supervisão. Nesse contexto, a Portaria SGD/MGI nº 5.950/2023 institui modelo obrigatório para a contratação de software e de serviços de computação em nuvem no âmbito do Sistema de Administração dos Recursos de Tecnologia da Informação (SISP), na Administração Pública Federal, com ênfase na padronização procedimental e no fortalecimento dos mecanismos de gestão dessas soluções [Brasil 2023].

Adicionalmente, o arcabouço normativo recente fortaleceu a governança da computação em nuvem na Administração Pública Federal ao combinar diretrizes para contratação, utilização e gestão desses serviços com requisitos específicos para segurança da informação, privacidade e tratamento de informações classificadas. A Instrução Normativa SGD/ME nº 5/2021 disciplina a adoção de serviços de computação em nuvem pelos órgãos públicos, e a Instrução Normativa GSI/PR nº 8/2025 estabelece requisitos diferenciados de segurança conforme o grau de sigilo das informações tratadas [Brasil 2021; Brasil 2025a]. Complementarmente, a Portaria SGD/MGI nº 9.511/2025 institui o Programa de Privacidade e Segurança da Informação (PPSI) no âmbito do SISP, estabelecendo um framework de governança voltado à privacidade, à segurança da informação e à gestão de riscos [Brasil 2025b]. Em conjunto, esses instrumentos ampliam os mecanismos institucionais de governança, proteção de dados e gestão de riscos aplicáveis à utilização de ambientes de computação em nuvem [Brasil 2021; Brasil 2025a; Brasil 2025b].

No plano institucional, a Nuvem de Governo materializa-se na atuação coordenada entre o Ministério da Gestão e da Inovação em Serviços Públicos (MGI), o Serviço Federal de Processamento de Dados (Serpro) e a Empresa de Tecnologia e Informações da Previdência Social (Dataprev), com a assinatura de Acordos de Cooperação Técnica [Brasil 2024a; Brasil 2024b; Brasil 2024c; Brasil 2024d]. Esse arranjo institucional organiza a atuação conjunta das instituições responsáveis pela oferta e governança dos serviços de computação em nuvem, definindo competências e responsabilidades.

3. Limites estruturais da Nuvem de Governo

Esta seção examina os principais limites estruturais da Nuvem de Governo para o fortalecimento da autonomia tecnológica da Administração Pública Federal. A análise está organizada em dois eixos complementares, que totalizam cinco categorias de limites. O primeiro aborda os limites tecnológicos associados às três camadas da soberania digital: física, de código e da informação. O segundo examina dois conjuntos de limitações: as vulnerabilidades decorrentes do contexto geopolítico e das cadeias globais de suprimentos, e as capacidades institucionais e materiais que condicionam a autonomia tecnológica do Estado

3.1. Limites tecnológicos das camadas da soberania digital

As primeiras limitações examinadas neste capítulo correspondem às camadas da soberania digital propostas por Falkner et al. (2024): física, de código e da informação. Para fins de organização da discussão, cada uma dessas camadas é abordada separadamente, destacando os fatores tecnológicos que condicionam a capacidade do Estado de exercer controle sobre infraestruturas, componentes computacionais e ativos informacionais utilizados pela Nuvem de Governo.

3.1.1. Camada física

A primeira limitação estrutural da Nuvem de Governo situa-se em sua base material. Embora o Estado possa ampliar o controle institucional e operacional sobre o ambiente de processamento e armazenamento, a infraestrutura física que sustenta esse arranjo permanece apoiada em hardware e componentes tecnológicos críticos produzidos em cadeias globais de fornecimento, incluindo equipamentos de rede, controladoras, *firmware* e demais componentes necessários à sua operação.

Essa dependência adquire maior complexidade quando analisada a partir do ciclo de vida da infraestrutura. O incremento da autoridade estatal sobre os dados processados não implica, automaticamente, domínio sobre a fabricação, a manutenção e a substituição dos componentes que sustentam a operação do ambiente tecnológico [Floridi 2020]. Mesmo em arranjos submetidos a maior jurisdição nacional, a continuidade operacional desses ambientes permanece vinculada a fornecedores e ecossistemas tecnológicos externos [Floridi 2020; Bellanova et al. 2022].

Essa condição também se reflete na configuração concreta da infraestrutura estatal. Em comunicações institucionais, a Nuvem de Governo é apresentada como iniciativa baseada na disponibilização de infraestrutura computacional em *data centers* de empresas públicas, associada à utilização de soluções e serviços tecnológicos fornecidos por provedores externos, como, por exemplo: Amazon Web Services; Google Distributed Cloud; Huawei Cloud Stack e Oracle Exadata Cloud@Customer.

3.1.2. Camada de código

A limitação da Nuvem de Governo não se restringe à base material da infraestrutura, mas alcança também a camada de código. Mesmo quando o processamento ocorre em ambiente estatal, a operação da nuvem permanece significativamente dependente de arquiteturas proprietárias, softwares críticos e ecossistemas tecnológicos desenvolvidos por grandes fornecedores globais. Essa vinculação tecnológica pode ser observada, de forma mais ampla, na recorrente incorporação de conjuntos tecnológicos e serviços associados a grandes provedores globais em ambientes digitais estratégicos da Administração Pública [Silva et al. 2025].

Essa dinâmica também pode ser compreendida à luz de estudos que demonstram que os processos de digitalização alteram as formas de coordenação e controle em ambientes digitais. A digitalização amplia dependências relacionadas a sistemas digitais e cadeias tecnológicas [Martin et al. 2023], introduzindo desafios adicionais à

supervisão estatal de infraestruturas e serviços essenciais [Bellanova et al. 2022]. Aplicada à Nuvem de Governo, essa interpretação evidencia que a incorporação de arquiteturas proprietárias, serviços gerenciados e componentes críticos de software amplia limitações relacionadas à auditoria, à adaptação e à gestão do ambiente digital.

Essas relações de dependência elevam barreiras técnicas e organizacionais à migração entre ambientes digitais e à substituição de componentes críticos. A operação desses ambientes permanece condicionada por regimes de licenciamento, suporte especializado, compatibilidade técnica e ciclos de atualização definidos por fornecedores externos. Como consequência, ampliam-se os custos de migração tecnológica e os desafios de interoperabilidade, dificultando a reconfiguração autônoma de funções críticas sem comprometimento da continuidade operacional ou aumento da complexidade técnica [Silva et al. 2025].

3.1.3. Camada da informação

A camada da informação refere-se aos dados e conteúdos digitais que circulam, são armazenados e utilizados nos ambientes computacionais, constituindo os ativos informacionais sobre os quais incidem requisitos de proteção, disponibilidade, integridade e confidencialidade [Falkner et al. 2024]. No contexto da Nuvem de Governo, a ampliação do controle estatal sobre fluxos informacionais e serviços digitais fortalece os mecanismos de proteção desses ativos, especialmente por meio da definição de requisitos de segurança e governança aplicáveis ao tratamento das informações.

De acordo com Falkner et al. (2024), a camada da informação integra um núcleo tridimensional indissociável das camadas física e de código. Sob essa perspectiva, o controle sobre a informação não se esgota na regulação jurídica dos dados, mas depende também da capacidade de influenciar e controlar as infraestruturas e os componentes lógicos que sustentam seu processamento. Essa compreensão converge com Hummel et al. (2021), para quem a soberania dos dados envolve o exercício de controle significativo sobre os dados e sobre as condições técnicas e institucionais que permitem sua governança. [Falkner et al. 2024; Hummel et al. 2021; Pierucci 2025].

No plano operacional, a segurança das informações depende da adoção de mecanismos técnicos, como criptografia de dados em repouso e em trânsito, gestão de chaves criptográficas e controles de acesso. Embora essenciais para reduzir riscos associados ao tratamento, ao armazenamento e à transmissão de dados, essas medidas não eliminam os riscos e as dependências associados às infraestruturas e plataformas que sustentam os ambientes de computação em nuvem. Essa perspectiva também encontra respaldo na fiscalização que deu origem ao Acórdão TCU nº 949/2026, que destaca a importância da integridade, da rastreabilidade, da qualidade e da governança dos dados para a confiabilidade da solução de computação em nuvem objeto da auditoria [Brasil 2026].

3.2. Limites geopolíticos e capacidades estatais

Os limites estruturais da Nuvem de Governo não decorrem apenas de fatores tecnológicos relacionados às camadas da soberania digital. A capacidade do Estado de

exercer controle sobre infraestruturas e serviços digitais estratégicos também é condicionada por fatores geopolíticos, econômicos e institucionais. Nesse contexto, este tópico discute as vulnerabilidades decorrentes do cenário geopolítico e das cadeias globais de suprimentos, bem como as capacidades institucionais e materiais necessárias ao fortalecimento da autonomia tecnológica

3.2.1. Vulnerabilidades geopolíticas e a cadeia global de suprimentos

As vulnerabilidades geopolíticas da Nuvem de Governo decorrem, em grande medida, da inserção da Administração Pública em cadeias globais de suprimentos tecnológicos altamente concentradas. Em um cenário de crescente disputa por infraestruturas e capacidades tecnológicas estratégicas, no qual grandes potências buscam ampliar sua influência e liderança tecnológica, a dependência de plataformas e serviços externos amplia desafios institucionais e operacionais ao exercício da autonomia tecnológica [Broeders et al. 2023; Farrand e Carrapico 2022].

Glasze et al. (2023) destacam que iniciativas de soberania digital frequentemente se articulam à ampliação do controle estatal sobre dados, infraestruturas e serviços considerados estratégicos. Rone (2024), por sua vez, observa que a efetividade dessas iniciativas permanece condicionada à existência de capacidades tecnológicas compatíveis e à estrutura do mercado digital. Sob essa perspectiva, a autonomia tecnológica não depende apenas da autoridade regulatória do Estado, mas também da concentração das capacidades tecnológicas, da definição de padrões e do controle sobre recursos estratégicos.

Esse cenário torna-se particularmente evidente na produção de componentes que sustentam os ambientes digitais contemporâneos. Semicondutores, equipamentos avançados de processamento, soluções de armazenamento e segmentos relevantes da infraestrutura de rede integram cadeias produtivas de alta complexidade, concentradas em poucos polos industriais e sujeitas a disputas comerciais, restrições regulatórias e assimetrias geopolíticas [Silva et al. 2025; Gu 2024]. Nesses casos, a continuidade tecnológica da Nuvem de Governo pode permanecer exposta a limitações de fornecimento, atrasos logísticos e restrições de atualização nem sempre controladas pelo Estado.

A rápida incorporação de recursos de inteligência artificial aos serviços de computação em nuvem amplia essa dinâmica de dependência tecnológica. Conforme observa Gu (2024), a crescente utilização de inteligência artificial fortalece a posição das *Big Techs* ao concentrar capacidades computacionais, desenvolvimento algorítmico e grandes volumes de dados, tornando esses atores cada vez mais relevantes para a provisão de tecnologias digitais estratégicas. Nesse contexto, a competição internacional pela liderança em inteligência artificial reforça a dimensão geopolítica da computação em nuvem, uma vez que a disponibilidade dessas capacidades passa a influenciar diretamente a autonomia dos Estados na adoção e evolução de infraestruturas digitais críticas [Gu 2024; Broeders et al. 2023].

Em reconhecimento a esses riscos, o arcabouço normativo brasileiro passou a incorporar salvaguardas específicas relacionadas ao uso de inteligência artificial em serviços de computação em nuvem. A Instrução Normativa GSI/PR nº 5/2021

estabelece, entre os requisitos de segurança aplicáveis aos provedores de serviços de nuvem, a proibição do uso de informações dos órgãos e entidades para otimização de mecanismos de inteligência artificial. No mesmo sentido, a Portaria SGD/MGI nº 5.950/2023 reproduz essa exigência em seu modelo de contratação, reforçando a proteção dos ativos informacionais da Administração Pública Federal e restringindo a utilização de dados governamentais para finalidades alheias à execução contratual.

Para além das limitações decorrentes da concentração tecnológica, a atuação de provedores globais de serviços de computação em nuvem também introduz condicionantes de natureza jurídica e geopolítica [Bellanova et al. 2022; Mitchell e Samlidis 2021]. Embora submetidos às exigências regulatórias brasileiras, esses provedores permanecem simultaneamente vinculados aos ordenamentos jurídicos e às autoridades competentes de seus países de origem. Em determinadas circunstâncias, normas de alcance extraterritorial, como o US CLOUD Act, podem produzir efeitos sobre dados sob posse, custódia ou controle de provedores sujeitos à jurisdição dos Estados Unidos, ainda que armazenados em infraestrutura localizada em território brasileiro [von Scherenberg et al. 2024; Silva et al. 2025]. Esse cenário evidencia que o exercício do controle estatal sobre ativos informacionais pode sofrer limitações decorrentes da incidência simultânea de regimes jurídicos distintos, ampliando os desafios para o fortalecimento da autonomia tecnológica [Gu 2024; Jansen et al. 2023; Floridi 2020].

Em contextos de elevada concentração tecnológica e baixa capacidade de substituição de fornecedores estratégicos, a dependência de ecossistemas externos pode ampliar a exposição do Estado a alterações unilaterais de preços, condições de licenciamento, regimes de suporte e ciclos de atualização tecnológica. Mesmo sem rupturas geopolíticas explícitas, esses fatores podem afetar a continuidade operacional, a previsibilidade orçamentária e a sustentabilidade de estratégias digitais estatais. Sob essa perspectiva, a robustez da Nuvem de Governo também depende da capacidade de mitigar assimetrias econômicas e de governança associadas à concentração de capacidades tecnológicas em atores externos.

3.2.2. Capacidades institucionais e materiais para a autonomia tecnológica

A viabilidade da Nuvem de Governo no longo prazo depende da existência de capacidades institucionais e materiais compatíveis com sua implantação, operação, manutenção e evolução contínua. Ainda que a infraestrutura estatal avance na ampliação do controle sobre dados e serviços digitais, sua consolidação depende de investimentos contínuos, coordenação organizacional e competências técnicas especializadas. Nesse sentido, a autonomia tecnológica não se resume à implantação da infraestrutura, mas envolve a capacidade de mantê-la de forma resiliente, escalável e tecnicamente qualificada ao longo do tempo.

A sustentabilidade econômica constitui um dos principais fatores que condicionam a viabilidade da Nuvem de Governo no longo prazo. A consolidação de uma infraestrutura de computação em nuvem sob maior controle estatal exige investimentos contínuos em recursos computacionais, conectividade, segurança e modernização tecnológica. Em contraste com grandes provedores globais, que operam sob economias de escala e ampla diversificação de serviços, a infraestrutura estatal

precisa sustentar esses investimentos em contextos institucionais e orçamentários mais restritos, o que pode limitar sua expansão e resiliência [Silva et al. 2025].

A disponibilidade de capacidades técnico-operacionais constitui outro fator determinante para a consolidação da Nuvem de Governo. A operação de infraestruturas de nuvem em alta disponibilidade exige equipes especializadas, monitoramento contínuo, resposta a incidentes e competências específicas em áreas como virtualização, redes, automação e cibersegurança. Nesse cenário, a formação e a retenção de profissionais qualificados tornam-se fatores centrais, especialmente porque a complexidade dos ambientes digitais e a rápida evolução das soluções tecnológicas podem dificultar a capacidade estatal de acompanhar os avanços técnicos e operacionais dos ecossistemas tecnológicos externos [Martin et al. 2023; Cloud Security Alliance 2024].

4. Análise Crítica

Os limites estruturais identificados ao longo deste estudo evidenciam que a implementação da Nuvem de Governo representa um avanço relevante para o fortalecimento da governança sobre ambientes digitais estratégicos, sem, contudo, eliminar os fatores que condicionam a autonomia tecnológica do Estado. Partindo dessa constatação, este capítulo desenvolve uma análise crítica da Nuvem de Governo, examinando, inicialmente, os avanços institucionais promovidos por esse arranjo; em seguida, os limites que persistem para a autonomia tecnológica da Administração Pública Federal; e, por fim, o papel da gestão estratégica de riscos na administração das dependências inerentes aos ecossistemas digitais contemporâneos.

4.1. Aspectos fortalecidos pela Nuvem de Governo

A principal contribuição da Nuvem de Governo reside no fortalecimento da governança sobre os ambientes de computação em nuvem por ela abrangidos. Mais do que ampliar a disponibilidade de infraestrutura tecnológica, esse arranjo institucional fortalece mecanismos permanentes de coordenação, supervisão e definição de responsabilidades sobre os serviços digitais e os ativos informacionais processados e armazenados nesse ambiente. Esses mecanismos reforçam a capacidade estatal de governança sobre os ambientes digitais estratégicos, especialmente nos aspectos relacionados à coordenação institucional, à supervisão e à gestão das informações [Brasil 2023; Mitchell e Samlidis 2021].

Esse avanço decorre da atuação coordenada da Secretaria de Governo Digital do MGI e da atribuição de competências específicas às empresas públicas responsáveis pela gestão da Nuvem de Governo. Os Acordos de Cooperação Técnica estabelecem responsabilidades relacionadas à gestão da infraestrutura, ao monitoramento da prestação dos serviços, ao suporte técnico aos órgãos usuários e à elaboração de catálogos padronizados, contribuindo para reduzir a fragmentação administrativa e promover maior uniformidade na implementação da Nuvem de Governo entre os órgãos da Administração Pública Federal [Brasil 2024a; Brasil 2024b; Brasil 2024c; Brasil 2024d].

Outro aspecto fortalecido consiste na definição de critérios uniformes para a alocação das cargas de trabalho entre os diferentes ambientes de computação em nuvem. Essa classificação busca compatibilizar o nível de proteção das informações com as características de cada ambiente computacional, fortalecendo a governança sobre os ativos informacionais. Nos termos da Portaria SGD/MGI nº 5.950/2023, devem ser mantidas em ambiente de Nuvem de Governo, exceto se expressamente determinado pelo Comitê de Governança Digital ou instância equivalente do órgão ou entidade, as cargas de trabalho que tratem informações com restrição de acesso prevista na legislação, como aquelas protegidas pelos sigilos fiscal, bancário, comercial, empresarial, contábil, de segredo industrial, de direito autoral, de propriedade intelectual, industrial, policial, processual civil, processual penal e disciplinar administrativa [Brasil 2023].

A adoção desses critérios promove maior uniformidade na aplicação dos requisitos de segurança da informação e reduz a heterogeneidade das decisões administrativas relacionadas à utilização dos diferentes ambientes de computação em nuvem. Em conjunto, esses mecanismos reforçam a capacidade estatal de coordenar e supervisionar os ambientes digitais abrangidos pela Nuvem de Governo e criam condições institucionais mais favoráveis para a gestão das dependências tecnológicas discutidas nas seções anteriores, bem como para o desenvolvimento contínuo das capacidades institucionais e organizacionais necessárias à evolução da infraestrutura digital estatal [Brasil 2023; Cloud Security Alliance 2024; Martin et al. 2023; Silva et al. 2025].

4.2. Desafios que permanecem para a autonomia tecnológica

Os avanços proporcionados pela Nuvem de Governo não eliminam os fatores estruturais que condicionam a autonomia tecnológica do Estado. Permanecem desafios relacionados à dependência de fornecedores estratégicos e ao fortalecimento das capacidades estatais necessárias para reduzir, de forma progressiva, as vulnerabilidades inerentes aos ecossistemas digitais contemporâneos.

4.2.1. Persistência da dependência de fornecedores estratégicos

A persistência da dependência de fornecedores estratégicos constitui um dos principais desafios à consolidação da autonomia tecnológica da Administração Pública Federal. A elevada concentração do mercado global de serviços e plataformas de computação em nuvem faz com que parcela significativa das soluções digitais utilizadas pelo Estado permaneça vinculada a ecossistemas tecnológicos controlados por um número reduzido de grandes provedores internacionais. Essa concentração também se reflete nas contratações públicas federais. Silva et al. (2025) estimam que, entre 2014 e 2025, o setor público brasileiro tenha despendido ao menos R\$ 23 bilhões com tecnologias estrangeiras, evidenciando a relevância econômica desses fornecedores para a sustentação dos ambientes digitais governamentais. A Tabela 3 apresenta um recorte desses dispêndios, elaborado pelos autores a partir de dados extraídos do Comprasnet e do Portal Nacional de Contratações Públicas (PNCP).

Tabela 3. Recorte de dispêndios públicos federais com grandes fornecedores internacionais de tecnologia

Fonte: Adaptado de Silva et al. (2025)

Empresa	Valor	Período	Fonte
Microsoft	R\$ 1.571.599.915,02	2021 a 2025	PNCP
	R\$ 3.274.233.113,08	2014 a 2025	Comprasnet
Oracle	R\$ 1.022.836.447,10	2021 a 2025	PNCP
	R\$ 742.814.513,19	2014 a 2025	Comprasnet
Google	R\$ 938.842.693,82	2021 a 2025	PNCP
	R\$ 133.270.423,40	2014 a 2025	Comprasnet
Red Hat	R\$ 909.225.269,72	2021 a 2025	PNCP
	R\$ 295.340.141,20	2014 a 2025	Comprasnet

No plano tecnológico, essa dependência também se manifesta por meio da utilização de plataformas e serviços proprietários, que podem ampliar mecanismos de aprisionamento tecnológico (*vendor lock-in*) e dificultar a substituição de fornecedores ou a migração entre ambientes digitais. Essa preocupação é corroborada pelo Acórdão TCU nº 949/2026, que, ao examinar a infraestrutura digital de órgão público baseada em serviços de computação em nuvem, identificou riscos relacionados à dependência de fornecedor único e à ausência de mecanismos robustos de portabilidade tecnológica, recomendando medidas para sua mitigação [Brasil 2026].

Em conjunto, esses elementos indicam que o fortalecimento da governança sobre ambientes digitais não elimina os limites estruturais anteriormente identificados. Permanecem, em especial, aqueles relacionados às camadas física e de código da soberania digital e à organização das cadeias globais de suprimentos, dos quais decorrem as dependências de fornecedores estratégicos e os desafios associados à substituição de tecnologias críticas ao longo do tempo.

4.2.2. Capacidades estatais como condição para a autonomia tecnológica

As limitações relacionadas às capacidades institucionais e materiais, discutidas na Seção 3.2.2, evidenciam que o fortalecimento da autonomia tecnológica não depende exclusivamente da ampliação da infraestrutura digital estatal. A capacidade de desenvolver, operar, manter e evoluir tecnologias estratégicas constitui requisito igualmente relevante para reduzir vulnerabilidades associadas à utilização de plataformas e ecossistemas tecnológicos externos. Nesse contexto, investimentos contínuos em pesquisa, inovação, desenvolvimento tecnológico e fortalecimento da base produtiva nacional representam condições estruturantes para fortalecer a capacidade estatal de desenvolver, controlar e sustentar tecnologias estratégicas, reduzindo progressivamente as vulnerabilidades associadas à dependência de ecossistemas tecnológicos externos [Martin et al. 2023; Silva et al. 2025].

Nesse sentido, a superação gradual dessas limitações também requer a formação e a retenção de profissionais qualificados, capazes de projetar, implementar, operar e manter infraestruturas digitais críticas. O fortalecimento das capacidades estatais, por

meio do desenvolvimento contínuo de competências técnicas, mecanismos de inovação e aprendizagem organizacional, amplia a capacidade de reduzir dependências tecnológicas ao longo do tempo e de exercer maior controle sobre a evolução dos ambientes digitais. Nessa perspectiva, a Nuvem de Governo deve ser compreendida como um instrumento de fortalecimento contínuo das capacidades institucionais e materiais do Estado, e não como uma solução suficiente, por si só, para assegurar a autonomia tecnológica [Cloud Security Alliance 2024; Martin et al. 2023; Silva et al. 2025].

4.3. Gestão de riscos e autonomia tecnológica

As análises desenvolvidas neste trabalho evidenciam que a autonomia tecnológica não deve ser compreendida como uma condição de autossuficiência absoluta. No contexto da economia digital contemporânea, caracterizada pela elevada concentração do mercado de tecnologias digitais, por cadeias globais de suprimentos altamente integradas e pela distribuição internacional das capacidades de inovação, a eliminação completa das dependências tecnológicas mostra-se inviável. Sob essa perspectiva, a autonomia tecnológica deve ser entendida como um processo contínuo de ampliação progressiva da autonomia decisória do Estado sobre infraestruturas, serviços e ativos informacionais estratégicos, reduzindo vulnerabilidades e administrando estrategicamente os riscos decorrentes das dependências tecnológicas que não possam ser eliminadas [Jansen et al. 2023; Martin et al. 2023; Pierucci 2025].

Nesse contexto, a principal contribuição da Nuvem de Governo consiste em criar condições institucionais para que o Estado administre, de forma mais coordenada, os riscos associados aos ambientes de computação em nuvem utilizados para o processamento de informações estratégicas. Ao institucionalizar mecanismos de coordenação, supervisão e definição de responsabilidades, a estratégia fortalece a capacidade estatal de identificar vulnerabilidades, responder de maneira mais consistente aos riscos e apoiar decisões relacionadas à gestão desses ambientes [Brasil 2023; Brasil 2024a; Brasil 2024b; Martin et al. 2023].

Entretanto, a efetividade da Nuvem de Governo permanece condicionada a fatores que extrapolam seu escopo institucional. O gerenciamento dos riscos associados a Nuvem de Governo deve considerar aspectos tecnológicos, jurídicos e geopolíticos que vão além dos mecanismos de governança nela previstos. Da mesma forma, a localização da infraestrutura e dos dados em território nacional, embora fortaleça a proteção das informações estratégicas, não elimina condicionantes decorrentes da concentração internacional das capacidades tecnológicas nem das jurisdições às quais permanecem submetidos provedores e tecnologias que sustentam esses ambientes. Nesse contexto, a ampliação da autonomia tecnológica depende da capacidade do Estado de identificar, avaliar e administrar estrategicamente esses condicionantes, reduzindo seus impactos sobre a continuidade, a segurança e a evolução dos serviços digitais estratégicos [Mitchell e Samlidis 2021; Bellanova et al. 2022; Gu 2024; Silva et al. 2025].

5. Considerações Finais

A análise dos arranjos normativos e institucionais relacionados à Nuvem de Governo demonstra que sua implementação se estrutura por meio de um modelo de governança destinado a organizar a atuação dos órgãos e empresas públicas responsáveis por sua gestão. Os mecanismos de definição de responsabilidades, padronização de procedimentos e estabelecimento de requisitos de segurança da informação e proteção de dados, aplicáveis a uma infraestrutura gerida por órgãos ou empresas públicas e localizada em território nacional, evidenciam a finalidade de ampliar a capacidade estatal de gestão sobre os serviços digitais e os ativos informacionais processados e armazenados nesse ambiente.

O fortalecimento institucional decorrente desse arranjo, entretanto, não elimina os desafios estruturais que limitam a autonomia tecnológica da Administração Pública Federal. As análises desenvolvidas evidenciam que permanecem limitações relacionadas ao controle sobre as tecnologias que sustentam a infraestrutura, ao uso de plataformas e códigos proprietários, aos mecanismos de controle e circulação dos dados, além das restrições decorrentes da organização global das cadeias produtivas. Nesse cenário, a ampliação da governança sobre a infraestrutura digital fortalece a capacidade estatal de coordenação, supervisão e gestão desse ambiente, sem conferir domínio pleno sobre as tecnologias, plataformas e dados que o sustentam.

A persistência dessas limitações torna a gestão de riscos um elemento central para a preservação da capacidade decisória do Estado diante das interdependências que caracterizam os ecossistemas digitais contemporâneos. As análises realizadas indicam que, no contexto da Nuvem de Governo, a ampliação da autonomia tecnológica não decorre da eliminação dessas dependências, mas da capacidade estatal de administrá-las estrategicamente. A gestão de riscos constitui, nesse sentido, um dos instrumentos por meio dos quais o Estado busca preservar sua capacidade de decisão e reduzir sua exposição às vulnerabilidades associadas à utilização de tecnologias externas.

A efetividade dessa estratégia, entretanto, depende de um processo contínuo de desenvolvimento de capacidades estatais. Isso envolve investimentos em infraestrutura, inovação, formação e retenção de profissionais especializados, bem como o aperfeiçoamento permanente dos instrumentos de governança. Em um ambiente marcado por rápidas transformações tecnológicas e geopolíticas, a sustentabilidade desse processo exige que o Estado desenvolva capacidades institucionais, técnicas e organizacionais capazes de adaptar continuamente a atuação da Administração Pública Federal às novas vulnerabilidades e desafios dos ecossistemas digitais.

Como desdobramento deste artigo, futuras pesquisas podem aprofundar a análise dos riscos associados às tecnologias que compõem a Nuvem de Governo, por meio do levantamento das contratações dos serviços e ferramentas utilizados pela Administração Pública Federal, identificando as dependências tecnológicas, os riscos inerentes a cada solução e as estratégias de mitigação adotadas. Também podem ser explorados os impactos da crescente integração entre computação em nuvem e inteligência artificial, especialmente diante das transformações geopolíticas relacionadas à concentração de capacidades tecnológicas e seus reflexos sobre a autonomia tecnológica do Estado.

Referências bibliográficas

- Bellanova, R.; Carrapico, H.; Duez, D. (2022). Digital/sovereignty and European security integration: an introduction. *European Security*, v. 31, n. 3, p. 337–355. DOI: 10.1080/09662839.2022.2101887.
- Broeders, D.; Cristiano, F.; Kaminska, M. (2023). In Search of Digital Sovereignty and Strategic Autonomy: Normative Power Europe to the Test of Its Geopolitical Ambitions. *JCMS: Journal of Common Market Studies*, v. 61, n. 5, p. 1261–1280. DOI: 10.1111/jcms.13462.
- Brasil. (2021). Gabinete de Segurança Institucional da Presidência da República. Instrução Normativa GSI/PR nº 5, de 30 de agosto de 2021. Dispõe sobre os requisitos mínimos de segurança da informação para utilização de soluções de computação em nuvem pelos órgãos e entidades da Administração Pública Federal. *Diário Oficial da União*, Brasília, DF.
- Brasil. (2023). Ministério da Gestão e da Inovação em Serviços Públicos. Portaria SGD/MGI nº 5.950, de 26 de outubro de 2023. Institui a Estratégia Nacional de Computação em Nuvem da Administração Pública Federal direta, autárquica e fundacional – Estratégia de Nuvem de Governo. *Diário Oficial da União*, Brasília, DF.
- Brasil. (2024a). Acordo de Cooperação Técnica nº 141/2024, celebrado entre a União, por intermédio do Ministério da Gestão e da Inovação em Serviços Públicos, e a Empresa de Tecnologia e Informações da Previdência – Dataprev. Brasília: Ministério da Gestão e da Inovação em Serviços Públicos.
- Brasil. (2024b). Acordo de Cooperação Técnica nº 142/2024, celebrado entre a União, por intermédio do Ministério da Gestão e da Inovação em Serviços Públicos, e o Serviço Federal de Processamento de Dados – Serpro. Brasília: Ministério da Gestão e da Inovação em Serviços Públicos.
- Brasil. (2024c). Plano de Trabalho referente ao Acordo de Cooperação Técnica MGI nº 141/2024, firmado entre o Ministério da Gestão e da Inovação em Serviços Públicos e a Empresa de Tecnologia e Informações da Previdência – Dataprev. Brasília: Ministério da Gestão e da Inovação em Serviços Públicos.
- Brasil. (2024d). Plano de Trabalho referente ao Acordo de Cooperação Técnica MGI nº 142/2024, firmado entre o Ministério da Gestão e da Inovação em Serviços Públicos e o Serviço Federal de Processamento de Dados – Serpro. Brasília: Ministério da Gestão e da Inovação em Serviços Públicos.
- Brasil. (2025a). Gabinete de Segurança Institucional da Presidência da República. Instrução Normativa GSI/PR nº 8, de 19 de março de 2025. Estabelece requisitos complementares de segurança da informação para utilização de serviços de computação em nuvem pela Administração Pública Federal.
- Brasil. (2025b). 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 (PPSI) no âmbito do Sistema de Administração dos Recursos de Tecnologia da Informação (SISP).

- Brasil. (2026). Tribunal de Contas da União. Acórdão nº 949/2026 – Plenário. Relator: Ministro Jorge Oliveira. Brasília: Tribunal de Contas da União.
- Cloud Security Alliance. (2024). Security Guidance v5 for Critical Areas of Focus in Cloud Computing. Cloud Security Alliance. Disponível em: <https://cloudsecurityalliance.org/artifacts/security-guidance-v5/>. Acesso em: 2 jul. 2026.
- Falkner, G.; Heidebrecht, S.; Obendiek, A.; Seidl, T. (2024). Digital sovereignty – Rhetoric and reality. *Journal of European Public Policy*, v. 31, n. 8, p. 2099–2120. DOI: 10.1080/13501763.2024.2358984.
- Farrand, B.; Carrapico, H. (2022). Digital sovereignty and taking back control: From regulatory capitalism to regulatory mercantilism in EU cybersecurity. *European Security*, v. 31, n. 3, p. 435–453. DOI: 10.1080/09662839.2022.2102896.
- Floridi, L. (2020). The Fight for Digital Sovereignty: What It Is, and Why It Matters, Especially for the EU. *Philosophy & Technology*, v. 33, p. 369–378. DOI: 10.1007/s13347-020-00423-6.
- Glasze, G.; Cattaruzza, A.; Douzet, F.; Dammann, F.; Bertran, M.-G.; Bômout, C.; Braun, M.; Danet, D.; Desforges, A.; Géry, A.; Grumbach, S.; Hummel, P.; Limonier, K.; Münßinger, M.; Nicolai, F.; Pétiniaud, L.; Winkler, J.; Zanin, C. (2023). Contested Spatialities of Digital Sovereignty. *Geopolitics*, v. 28, n. 2, p. 919–958. DOI: 10.1080/14650045.2022.2050070.
- Gu, H. (2024). Data, Big Tech, and the New Concept of Sovereignty. *Journal of Chinese Political Science*, v. 29, n. 4, p. 591–612. DOI: 10.1007/s11366-023-09855-1.
- Hummel, P.; Braun, M.; Tretter, M.; Dabrock, P. (2021). Data Sovereignty: A Review. *Big Data & Society*, Jan.–Jun., p. 1–17. DOI: 10.1177/2053951720982012.
- Jansen, B.; Kadenko, N.; Broeders, D.; van Eeten, M.; Borgolte, K.; Fiebig, T. (2023). Pushing boundaries: An empirical view on the digital sovereignty of six governments in the midst of geopolitical tensions. *Computers & Security*, v. 135, Article 103528. DOI: 10.1016/j.cose.2023.103528.
- Martin, A.; Sharma, G.; de Souza, S. P.; Taylor, L.; van Eerd, B.; McDonald, S. M.; Marelli, M.; Cheesman, M.; Scheel, S.; Dijstelbloem, H. (2023). Digitisation and Sovereignty in Humanitarian Space: Technologies, Territories and Tensions. *Geopolitics*, v. 28, n. 3, p. 1362–1397. DOI: 10.1080/14650045.2022.2047468.
- Mitchell, A. D.; Samlidis, T. (2021). Cloud services and government digital sovereignty in Australia and beyond. *International Journal of Law and Information Technology*, v. 29, n. 4, p. 364–394. DOI: 10.1093/ijlit/eaac003.
- NIST. (2011). Guidelines on Security and Privacy in Public Cloud Computing. NIST Special Publication 800-144. Gaithersburg: National Institute of Standards and Technology. DOI: 10.6028/NIST.SP.800-144.
- Pierucci, F. (2025). Sovereignty in the Digital Era: Rethinking Territoriality and Governance in Cyberspace. *Digital Society*, v. 4, Article 27. DOI: 10.1007/s44206-025-00189-4.

- Pohle, J.; Thiel, T. (2020). Digital sovereignty. *Internet Policy Review*, v. 9, n. 4. DOI: 10.14763/2020.4.1532.
- Roberts, H.; Cows, J.; Casolari, F.; Morley, J.; Taddeo, M.; Floridi, L. (2021). Safeguarding European values with digital sovereignty: An analysis of statements and policies. *Internet Policy Review*, v. 10, n. 3. DOI: 10.14763/2021.3.1575.
- Rone, J. (2024). ‘The sovereign cloud’ in Europe: Diverging nation state preferences and disputed institutional competences in the context of limited technological capabilities. *Journal of European Public Policy*, v. 31, n. 8, p. 2343–2369. DOI: 10.1080/13501763.2024.2348618.
- SERPRO. (2026). Catálogo de Serviços ACT nº 142/2024 – Nuvem de Governo. Versão 1.1, 30 jun. 2026. Brasília: Serviço Federal de Processamento de Dados. Disponível em: <https://mais.serpro.gov.br/index.php/s/TBzmL9dDBtWn625?path=%2F&openfile=18532495>. Acesso em: 2 jul. 2026.
- Silva, E. C. de M.; Rocha, I.; Vaz, J. C.; Veneziani, J. R. de A.; Modanez, C. de C. (2025). Entre licenças bilionárias e nuvens internacionais: um mapeamento sistemático de contratos do setor público brasileiro com fornecedores internacionais de tecnologias. *InterAção*, v. 16, n. 4, e93697. DOI: 10.5902/2357797593697.
- von Scherenberg, F.; Hellmeier, M.; Otto, B. (2024). Data Sovereignty in Information Systems. *Electronic Markets*, v. 34, Article 15. DOI: 10.1007/s12525-024-00693-4.