https://doi.org/10.47734/regrasp.v11.01.p01-12

INSTITUTO FEDERAL
São Paulo
Campus São Paulo
REGRASP

Mecanismos regulatórios para infraestrutura digital brasileira: Entre a governança de redes e a proteção de sistemas críticos

Regulatory Mechanisms for Brazilian Digital Infrastructure: Between Network Governance and Critical System Protection

Larissa Maria Pinheiro de Lima
Graduanda em Gestão Pública
Instituto Federal de Educação, Ciência e Tecnologia de São Paulo campus Pirituba
https://orcid.org/0009-0004-8320-7994
larissa.pinheiro@aluno.ifsp.edu.br

Luana Oliveira do Nascimento
Graduanda em Gestão Pública
Instituto Federal de Educação, Ciência e Tecnologia de São Paulo campus Pirituba
https://orcid.org/0009-0002-0456-7306
luana.nascimento@aluno.ifsp.edu.br

Rebeca de Lima Saraiva Leão
Graduanda em Gestão Pública
Instituto Federal de Educação, Ciência e Tecnologia de São Paulo campus Pirituba
https://orcid.org/0009-0007-6269-1248
l.leao@aluno.ifsp.edu.br

Willian Ramalho Feitosa
Doutor em Administração de Empresas e Professor do IFSP- Campus Pirituba
EAESP FGV - Instituto Federal de Educação, Ciência e Tecnologia de São Paulo
https://orcid.org/0009-0004-8320-7994
wilian.feitosa@ifsp.edu.br

Nota editorial:
Este artigo é uma versão revisada de trabalho selecionado no *fast-track* do XI Congresso Internacional de Logística do IFSP (IFLOG) para publicação na Revista REGRASP.

Histórico do artigo
Recebido: 23 dez. 2025
Aprovado: 06 mar. 2026
Publicado: 12 mar. 2026

RESUMO

A expansão da digitalização no Brasil intensificou a dependência de setores essenciais como energia, saúde, transportes, finanças e serviços públicos, tornando a proteção da infraestrutura digital um tema central para a segurança nacional. Nesse contexto, crescem os desafios relacionados a ameaças cibernéticas e à necessidade de marcos regulatórios capazes de promover resiliência operacional. O presente artigo tem como objetivo analisar os mecanismos regulatórios brasileiros voltados à governança de redes e à proteção de sistemas críticos, identificando avanços, lacunas e perspectivas. Para isso, adotou-se uma revisão de literatura qualitativa e analítica, baseada em fontes acadêmicas, normativas e institucionais, interpretadas por meio da análise de conteúdo. Os resultados evidenciam que o país progrediu com instrumentos como o Marco Civil da Internet, a Lei Geral de Proteção de Dados e a Estratégia Nacional de Segurança Cibernética, mas ainda enfrenta fragmentação normativa, baixa capacidade institucional e desafios de integração entre Estado, setor privado e sociedade civil. Conclui-se que o fortalecimento da infraestrutura digital brasileira depende da consolidação de

uma governança multissetorial, de investimentos em capacitação técnica e de políticas coordenadas de segurança cibernética que promovam resiliência e confiança digital.
Palavras-chave: governança de redes; infraestrutura digital; sistemas críticos; segurança cibernética; políticas públicas.

ABSTRACT
The expansion of digitalization in Brazil has intensified the dependence of essential sectors such as energy, healthcare, transportation, finance, and public services, making the protection of digital infrastructure a central issue for national security. In this context, challenges related to cyber threats and the need for regulatory frameworks capable of promoting operational resilience have increased. This article aims to analyze Brazilian regulatory mechanisms focused on network governance and the protection of critical systems, identifying advances, gaps, and future perspectives. To this end, a qualitative and analytical literature review was conducted, based on academic, normative, and institutional sources, interpreted through content analysis. The results show that the country has made progress with instruments such as the Internet Civil Framework, the General Data Protection Law, and the National Cybersecurity Strategy, but it still faces normative fragmentation, low institutional capacity, and challenges in integrating the State, the private sector, and civil society. It is concluded that strengthening Brazil's digital infrastructure depends on consolidating multistakeholder governance, investing in technical capacity building, and implementing coordinated cybersecurity policies that promote resilience and digital trust.
Keywords: network governance; digital infrastructure; critical systems; cybersecurity; public policies.

Introdução

A crescente digitalização da sociedade e a interdependência das infraestruturas críticas tornaram a regulação e a proteção desses sistemas questões centrais no debate sobre segurança nacional e governança pública. Conforme Castells (2009, p. 89):

> "A revolução tecnológica baseada em tecnologias da informação não apenas transforma a economia, mas também reconfigura o poder, a cultura e as instituições, criando um novo paradigma de organização social em redes"

Esse novo paradigma está diretamente ligado à digitalização de setores como energia, transporte, saúde, finanças e serviços públicos, todos fortemente dependentes de sistemas digitais para garantir eficiência, acessibilidade e continuidade dos serviços.

No setor energético, a automação de redes de distribuição, o uso de sistemas inteligentes de monitoramento e a integração com tecnologias de energia renovável ampliam a eficiência, mas também expõem fragilidades. O ataque cibernético à rede elétrica da Ucrânia, em 2015, exemplifica a gravidade do problema ao deixar mais de 200 mil pessoas sem fornecimento de energia (RID, 2020). Esse caso reforça a necessidade de marcos regulatórios robustos que articulem segurança e resiliência.

O **setor de transportes** também se tornou dependente da integração digital. Segundo Silva e Pereira (2021, p. 44):

> "Os sistemas inteligentes de transporte, ao mesmo tempo em que oferecem ganhos de previsibilidade e gestão do fluxo urbano, também se tornam pontos frágeis de uma cadeia complexa, nos quais um ataque cibernético pode comprometer desde a segurança de passageiros até o funcionamento da economia"

A vulnerabilidade dos sistemas de mobilidade coloca em risco não apenas a logística nacional, mas também a vida cotidiana dos cidadãos.

Na área da **saúde**, hospitais e sistemas de gestão pública foram alvos recorrentes de ataques de ransomware. O episódio de 2017 com o ataque WannaCry no Reino Unido interrompeu consultas e cirurgias, expondo a fragilidade das infraestruturas críticas hospitalares. No Brasil, o ataque ao ConecteSUS, em 2021, revelou que até mesmo os serviços essenciais podem ser paralisados, impactando diretamente a vida da população. Como reforça Denardis (2020, p. 132):

> "Hospitais e redes de saúde são infraestruturas críticas que se encontram no cruzamento entre vulnerabilidades técnicas e consequências sociais graves, visto que um colapso digital pode custar vidas humanas"

O **sistema financeiro** é outro setor extremamente vulnerável, dada sua dependência de plataformas digitais para transações, investimentos e controle monetário. Zanatta (2019, p. 76) observa que:

> "A regulação de dados financeiros e da infraestrutura crítica associada ao sistema bancário deve ir além da mera proteção contra-ataques cibernéticos. É preciso criar ecossistemas normativos capazes de responder a novos padrões de crime digital, lavagem de dinheiro e manipulação algorítmica do mercado"

Por fim, os **serviços públicos digitais**, como cadastros sociais, emissão de documentos e plataformas de transparência, tornaram-se indispensáveis à cidadania, especialmente após a pandemia de COVID-19. Segundo a OCDE (2019, p. 52):

> "Os serviços digitais governamentais, quando mal protegidos, não apenas colocam em risco informações sensíveis dos cidadãos, como também podem abalar a confiança social no Estado e sua legitimidade perante a população"

A justificativa para este estudo, portanto, repousa na urgência de compreender os mecanismos regulatórios voltados à proteção da infraestrutura digital brasileira, situando-os no contexto da governança em rede. Trata-se de um desafio multidimensional que envolve a articulação entre Estado, setor privado e sociedade civil, exigindo soluções colaborativas, interdisciplinares e integradas.

Objetivos

Este artigo tem como objetivo realizar uma revisão de literária de caráter qualitativo e analítico sobre os mecanismos regulatórios da infraestrutura digital brasileira, com ênfase na governança em rede e na proteção de sistemas críticos. A pesquisa baseia-se em fontes científicas, normativas e institucionais reconhecidas, de modo a oferecer uma sistematização crítica das produções existentes e identificar as principais tendências e desafios do campo.

Os objetivos específicos são:

- Mapear os principais marcos normativos e regulatórios brasileiros sobre infraestrutura digital e segurança cibernética;
- Examinar a inserção dos setores de energia, transporte, saúde, finanças e serviços públicos nesse contexto;
- Discutir experiências internacionais de governança de sistemas críticos e suas lições para o Brasil;
- Avaliar os desafios e perspectivas futuras para a proteção da infraestrutura digital no país.

Referencial Teórico

Marcos regulatórios da infraestrutura digital no Brasil

Marco Civil da Internet (Lei nº 12.965/2014) consolidou-se como o "Constituição da Internet no Brasil" (DONEDA; MENDES, 2018, p. 22), pois estabelece princípios fundamentais como a proteção da privacidade, a neutralidade da rede, a guarda de registros de conexão ("logs") e a transparência dos provedores quanto aos termos de uso da internet (BRASIL, 2014). Esses elementos são relevantes para a proteção de infraestruturas críticas porque permitem rastreabilidade em incidentes, auxiliando em processos de recuperação e investigação e responsabilizando atores da rede. Contudo, como aponta Pinheiro (2020), o Marco Civil foi desenhado majoritariamente para disciplinar a relação entre provedores de internet e usuários, assegurando a liberdade de expressão e a proteção de dados, mas sem enfoque específico na segurança operacional de infraestruturas críticas. Assim, não impõe obrigações técnicas robustas para sistemas de controle industrial, redes de distribuição ou telecomunicações estratégicas. Em contextos de ataques cibernéticos ou falhas graves, o Marco Civil, isoladamente, não garante resiliência ou continuidade operacional — como redundâncias ou planos de recuperação — sendo necessária a complementação por regulamentações específicas (SILVA, 2021).

A Lei Geral de Proteção de Dados Pessoais (Lei nº 13.709/2018 – LGPD) representou um avanço normativo significativo, pois obriga os agentes de tratamento de dados a adotar medidas técnicas e administrativas de segurança para proteger informações contra acessos não autorizados, vazamentos ou qualquer forma de tratamento inadequado (BRASIL, 2018).

Tais medidas abrangem práticas como criptografia, controle de acesso e políticas de segurança da informação (MENDES; DONEDA; MONTEIRO, 2019). De acordo com Abreu (2023), a LGPD também introduz no Brasil a cultura de gestão de riscos e resposta a incidentes, estimulando a implementação de planos de recuperação para mitigar os impactos de ataques cibernéticos. No entanto, o diploma legal não estabelece padrões técnicos mínimos aplicáveis de forma universal a setores críticos, nem prevê certificações ou auditorias específicas para sistemas industriais (PINHEIRO, 2020). Outro desafio relevante, como observa Silva (2021), é que a lei presume que todos os agentes possuem capacidade técnica e recursos financeiros para a conformidade, o que não corresponde à realidade de organizações que ainda operam com sistemas legados e infraestrutura precária. Além disso, a LGPD restringe-se ao escopo de dados pessoais, não contemplando aspectos fundamentais de continuidade de negócios e resiliência operacional de serviços essenciais, como redes de energia ou sistemas de controle industrial.

Já a Estratégia Nacional de Segurança Cibernética (E-Ciber), instituída originalmente pelo Decreto nº 10.222/2020 e revisada pelo Decreto nº 12.573/2025, busca modernizar e ampliar as diretrizes de ciber segurança no Brasil (BRASIL, 2020; BRASIL, 2025). O documento apresenta como objetivos centrais a proteção de infraestruturas críticas, a coordenação entre órgãos públicos, setor privado e sociedade civil, além da promoção da confiança digital (NIC.BR, 2022). Tais diretrizes são indispensáveis à continuidade de negócios em setores estratégicos como água, energia, telecomunicações e saúde, assegurando que mantenham suas operações diante de ataques ou incidentes (ABREU, 2023). A versão mais recente reforça ainda a importância da capacitação profissional, da educação em segurança cibernética da governança integrada como pilares da resiliência digital. Contudo, sua efetividade depende de forte articulação institucional e da disponibilização de recursos, o que revela desigualdades entre diferentes setores e regiões do país (SILVA, 2021). Ademais, a E-Ciber não substitui a necessidade de um marco legal setorial, com obrigações detalhadas, padrões técnicos mínimos e penalidades claras para falhas de segurança que comprometam serviços críticos. Outro obstáculo identificado é a distância entre a formulação das diretrizes e sua implementação prática, sobretudo em organizações de menor porte ou em áreas com infraestrutura digital insuficiente, perpetuando desigualdades na execução da política nacional de segurança cibernética (NIC.BR, 2022).

Governança em redes e sua infraestrutura

A análise da infraestrutura digital brasileira exige compreender, o conceito de infraestruturas críticas se sua relação com a governança em rede e a regulação digital. Esse campo tem sido explorado tanto por autores clássicos das ciências sociais e políticas quanto por organismos internacionais que discutem a segurança cibernética em escala global.

Infraestruturas críticas e sociedade em rede

O termo “infraestruturas críticas” refere-se a sistemas, serviços e ativos essenciais ao funcionamento da sociedade, cuja interrupção ou falha pode causar impactos severos à segurança nacional, à economia e à vida da população. Segundo a OCDE (2019, p. 17):

> “Infraestruturas críticas compreendem não apenas setores como energia, transporte, comunicações e finanças, mas também serviços essenciais à vida cotidiana, cuja falha compromete a resiliência social e institucional de um país”

A interdependência digital amplia esses riscos. Castells (2009, p. 45) explica que:

> “A sociedade em rede é caracterizada por fluxos contínuos de informação e pela interconexão de atividades, instituições e pessoas em escala global. Essa interconexão,

> embora crie oportunidades, também gera novas formas de vulnerabilidade"

Dessa forma, a proteção das infraestruturas críticas no Brasil deve ser compreendida como parte de um movimento maior de reorganização global em torno da informação e da segurança digital.

Zanatta (2019, p. 72) destaca que a regulação deve acompanhar a velocidade das transformações digitais:

> "No Brasil, a regulação de dados e da infraestrutura digital ainda é marcada por fragmentação normativa e por uma baixa capacidade institucional de resposta a incidentes complexos"

Experiências internacionais

A União Europeia tem se destacado na consolidação de políticas de segurança para infraestruturas críticas. A Agência Europeia para segurança cibernética (ENISA, 2021) coordena diretrizes que obrigam Estados-membros a adotar planos nacionais de proteção, com protocolos comuns de resposta a incidentes.

Nos Estados Unidos, a segurança cibernética das infraestruturas críticas é tratada como questão de segurança nacional, com políticas coordenadas pelo Department of Homeland Security (DHS). Kello (2017, p. 96) observa que:

> "O ciberespaço emergiu como um novo domínio de conflito, comparável à terra, ao mar e ao ar. Proteger as infraestruturas críticas significa proteger a própria soberania nacional"

Essas experiências internacionais demonstram que a regulação da infraestrutura digital deve ser compreendida como um problema global, exigindo não apenas normas internas, mas também alinhamento às boas práticas multilaterais.

O caso brasileiro

No Brasil, os principais marcos regulatórios incluem o Marco Civil da Internet (Lei nº 12.965/2014), a Lei Geral de Proteção de Dados (Lei nº 13.709/2018) e o Decreto nº 9.573/2018, que institui a Política Nacional de Segurança da Informação. Mais recentemente, a Estratégia Nacional de Segurança Cibernética (E-Ciber, 2020) passou a orientar as ações do governo federal.

No entanto, como destacam Gama e Ribeiro (2022, p. 55):

> "Apesar dos avanços normativos, a ausência de padronização e de mecanismos de monitoramento contínuo fragiliza a proteção das infraestruturas críticas brasileiras, tornando-as suscetíveis a incidentes de grandes proporções"

A revisão de literatura evidencia, portanto, que o Brasil ainda enfrenta desafios relacionados à consolidação de uma governança integrada e à harmonização de normas e práticas de segurança cibernética.

Proteção de Sistemas Críticos

Sistemas críticos são infraestruturas essenciais, cuja falha poderia comprometer serviços fundamentais como energia, transporte, telecomunicações e finanças. A proteção desses sistemas deve combinar três dimensões:

1. Segurança física e lógica: envolve a proteção de equipamentos, servidores e redes contra ameaças cibernéticas e ataques físicos.

2. Resiliência operacional: planejamento de contingência, redundâncias e backup de dados para garantir continuidade de serviços em caso de incidentes.

3. Referenciais internacionais e frameworks de segurança: a adoção de modelos como o NIST,CyberSecurity, Framework e diretrizes da OCDE permite estruturar processos de gestão de riscos, auditorias e resposta a incidentes (OCDE, 2019).

O estudo de Schwab (2016) sobre a quarta revolução industrial destaca que a digitalização acelerada aumenta a complexidade dos sistemas críticos, tornando a coordenação entre múltiplos atores indispensáveis para proteger as infraestruturas contra ameaças cada vez mais sofisticadas.

Exemplos de vulnerabilidades incluem o ataque à rede elétrica ucraniana em 2015, que deixou centenas de milhares de pessoas sem energia (RID, 2020), e o ataque de ransomware WannaCry em hospitais do Reino Unido, que paralisou serviços essenciais em 2017 (Denardis, 2020). Esses casos mostram que falhas em sistemas críticos têm impacto direto na sociedade, reforçando a necessidade de governança integrada e resiliência digital.

Desafios e perspectivas da segurança cibernética

A segurança cibernética consolidou-se como um dos maiores desafios contemporâneos diante da crescente digitalização da economia, da administração pública e da vida cotidiana. Desde a expansão da internet comercial, nos anos 1990, especialistas já alertavam sobre os riscos de ataques digitais (CASTRO; SOUZA, 2021). Contudo, nas últimas duas décadas, o processo de transformação digital das empresas e governos, intensificado pela pandemia de Covid-19, ampliou de forma exponencial a superfície de ataques cibernéticos (WORLD ECONOMIC FORUM, 2023).

Esse cenário foi agravado pelo avanço da Internet das Coisas (IoT), da computação em nuvem, das redes 5G e da inteligência artificial, que, embora tragam ganhos de eficiência e inovação, também criam novos pontos de vulnerabilidade (SOUSA, 2022; OLIVEIRA, 2023).

1. Crescimento dos ataques cibernéticos sofisticados:

Casos como o ataque de ransomware ao Superior Tribunal de Justiça (STJ) em 2020 e à Secretaria de Saúde do Rio Grande do Sul em 2021 demonstram a vulnerabilidade de instituições públicas (UFPEL, 2021). O relatório Internet Crime Report 2022, do FBI, confirma que "phishing e ransomware estão entre os crimes digitais mais recorrentes e com maior impacto financeiro" (FBI, 2023).

Empresas privadas também enfrentam desafios relevantes. A Cielo adotou um conjunto integrado de soluções (Microsoft Defender XDR, Microsoft Sentinel e Intune) para centralizar monitoramento e automatizar respostas a incidentes. Segundo o Chief Information Security Officer da empresa, "o Microsoft Sentinel está no centro do trabalho da nossa equipe de resposta" (TI INSIDE, 2024).

2. Proteção de infraestruturas críticas:

Setores como energia e telecomunicações têm recebido atenção regulatória e técnica — a ANEEL publicou a Resolução Normativa nº 964/2021 para o setor elétrico, definindo políticas e conteúdo mínimo para segurança cibernética (ANEEL, 2021). Normas técnicas internacionais, como a IEC 62443, orientam práticas de segurança para sistemas de automação industrial (ABNT, 2021).

3. Fragmentação regulatória:

Apesar de marcos legais importantes, como o Marco Civil da Internet (BRASIL, 2014) e a LGPD (BRASIL, 2018), persiste a necessidade de integração normativa e institucional. A Estratégia Nacional de Ciber Segurança (Decreto nº 12.573/2025) atualiza a governança federal sobre o tema, mas sua implementação exige coordenação entre União, estados e setor privado (BRASIL, 2025).

4. Escassez de profissionais especializados:

Relatórios do (ISC) apontam lacunas no quadro global e na capacitação de profissionais em segurança cibernética; estimativas recentes indicam um déficit significativo de profissionais,

o que impacta a capacidade de resposta (ISC2, 2023). Empresas como a Cielo têm investido em treinamento interno para mitigar esse gap (MICROSOFT NEWS, 2024).

5. Dependência tecnológica externa:

A utilização majoritária de soluções estrangeiras implica riscos de cadeia de suprimentos e soberania tecnológica. Ao mesmo tempo, a adoção criteriosa dessas tecnologias, combinada com políticas internas robustas, pode reduzir exposição a riscos — como observou a Cielo ao integrar soluções Microsoft: "o Microsoft Defender XDR e o Microsoft Sentinel proporcionaram centralização do monitoramento e automação de processos, reduzindo custos e riscos operacionais" (MICROSOFT, 2024).

Perspectivas e tendências

Entre as tendências que moldam a agenda estão a adoção de IA generativa para defesa e ataque, os desafios colocados pela computação quântica à criptografia atual e a necessidade de normas e educação continuada (WORLD ECONOMIC FORUM, 2023; NIST, 2022). Organizações brasileiras como o CERT.br fornecem materiais educativos e boas práticas para usuários e instituições (CERT.br, 2021).

A segurança cibernética demanda uma ação coordenada entre instrumentos legais, técnicos, econômicos e sociais. A experiência de empresas privadas, como a Cielo, com políticas formais e investimentos em tecnologia e formação, ilustra práticas que podem apoiar a resiliência nacional.

Metodologia

O presente estudo fundamenta-se em uma revisão de literatura de caráter qualitativo e analítico, voltada à identificação, seleção e interpretação crítica de fontes acadêmicas, normativas e institucionais relacionadas à regulação da infraestrutura digital e à proteção de sistemas críticos no Brasil.

A revisão de literatura consiste em uma metodologia sistemática de levantamento e análise de publicações científicas, com o intuito de sintetizar o estado do conhecimento sobre determinado tema, promovendo uma leitura crítica e interpretativa das contribuições teóricas, das normas e dos documentos oficiais relevantes.

A abordagem metodológica adotada neste artigo se ancora na análise de conteúdo, conforme as proposições de Laurence Bardin (1977), e é interpretada sob a ótica relacional e crítica de Pierre Bourdieu (1983; 1990). Essa combinação permite compreender o conteúdo das fontes não apenas em seu aspecto descritivo, mas também como expressão das relações de poder, disputas simbólicas e dinâmicas institucionais presentes no campo da regulação digital.

A análise de conteúdo, segundo Bardin (1977), envolve um conjunto de procedimentos sistemáticos e objetivos de descrição do conteúdo das mensagens, com o propósito de inferir significados, estruturas e tendências. Sob a perspectiva bourdieusiana, tais mensagens — sejam leis, relatórios ou artigos científicos — são também produtos de campos sociais e instrumentos de construção simbólica, expressando interesses e capitais diversos (econômico, político e informacional).

A pesquisa foi estruturada em quatro etapas principais:

Delimitação do escopo

O recorte temporal compreendeu o período de 2009 a 2024, o qual marca a consolidação da literatura sobre governança em rede (CASTELLS, 2009) e o fortalecimento dos marcos regulatórios brasileiros, como o Marco Civil da Internet (Lei nº 12.965/2014) e a Lei Geral de Proteção de Dados Pessoais – LGPD (Lei nº 13.709/2018).

Também foram incorporados documentos internacionais que tratam da segurança de infraestruturas críticas e da resiliência digital, como relatórios e recomendações da

Organização para a Cooperação e Desenvolvimento Econômico (OCDE, 2019), além de publicações da União Europeia e da Organização das Nações Unidas (ONU).

Estratégias de busca

A coleta das fontes foi realizada em bases de dados acadêmicas e em repositórios oficiais, a fim de garantir credibilidade e diversidade informacional. Foram consideradas:

• Bases acadêmicas: SciELO, Google Acadêmico, Scopus e Web of Science, priorizando artigos revisados por pares e livros de referência na área.

• Periódicos especializados: Revista de Direito Civil Contemporâneo, Revista do Serviço Público, Revista de Direito, Estado e Telecomunicações, entre outras.

• Documentos institucionais nacionais, emitidos por órgãos e entidades diretamente envolvidos na regulação e segurança digital:

o Anatel (Agência Nacional de Telecomunicações) – responsável por regulamentar e fiscalizar o setor de telecomunicações no Brasil;

o ANPD (Autoridade Nacional de Proteção de Dados) – órgão encarregado de zelar pela proteção de dados pessoais e fiscalizar o cumprimento da LGPD;

o CGI.br (Comitê Gestor da Internet no Brasil) – instância multissetorial que coordena e integra as ações relacionadas à governança da Internet no país, estabelecendo princípios e diretrizes para seu uso e desenvolvimento.

• Organismos internacionais:

o OCDE (Organização para a Cooperação e Desenvolvimento Econômico) – instituição que elabora diretrizes internacionais sobre governança digital, proteção de dados e resiliência cibernética;

o União Europeia – especialmente por meio do European Union Agency for Cybersecurity (ENISA), que publica relatórios e recomendações sobre segurança de sistemas críticos;

o ONU (Organização das Nações Unidas) – cujas publicações abordam direitos digitais, governança global da Internet e segurança internacional no espaço cibernético.

Os descritores utilizados incluíram: infraestrutura digital, governança em rede, segurança cibernética, sistemas críticos, regulação digital Brasil, tanto em português quanto em inglês (digital infrastructure, cybersecurity, network governance, critical systems, digital regulation Brazil).

Critérios de seleção e exclusão

Foram incluídos:

• Artigos científicos publicados em periódicos revisados por pares;

• Livros e capítulos de referência reconhecida na área;

• Relatórios técnicos de organismos nacionais e internacionais;

• Legislação e normas brasileiras relacionadas ao tema.

Foram excluídos:

• Trabalhos sem revisão por pares ou consistência metodológica;

• Publicações anteriores a 2009 que não tivessem relevância histórica ou conceitual;

• Materiais sem relação direta com a infraestrutura digital ou segurança de sistemas críticos.

Análise e tratamento dos dados

A etapa de análise seguiu as três fases clássicas da análise de conteúdo (Bardin, 1977), associadas ao enfoque crítico de Bourdieu (1990):

1. Pré-análise (leitura exploratória):

Realizou-se uma leitura inicial do material coletado para identificar a pertinência das fontes, seu contexto de produção e as categorias preliminares de análise (governança em rede, infraestrutura crítica, segurança cibernética, regulação digital).

2. Exploração do material (leitura seletiva):

Nesta fase, as fontes foram classificadas e categorizadas segundo eixos temáticos e conceituais. Foram destacados os principais marcos legais, as abordagens teóricas dominantes e as relações entre atores institucionais (Estado, setor privado, organismos internacionais e sociedade civil).
3. Tratamento dos resultados e interpretação (síntese integrativa):
As informações categorizadas foram interpretadas à luz da análise de conteúdo e da teoria dos campos de Bourdieu, buscando identificar convergências, divergências e lacunas nas políticas e nas abordagens regulatórias. Essa etapa permitiu compreender como as estruturas normativas e discursivas refletem posições de poder e disputas simbólicas no campo da governança digital brasileira.
A interpretação foi guiada por um enfoque crítico-analítico, buscando articular os marcos normativos nacionais com as práticas internacionais, bem como avaliar os impactos da governança em rede na proteção de sistemas críticos.
Por se tratar de uma revisão de literatura, esta pesquisa não contempla coleta de dados empíricos. O trabalho fundamenta-se exclusivamente em fontes secundárias, reconhecendo como limitação a escassez de estudos empíricos recentes sobre a implementação prática das políticas de segurança cibernética no Brasil.

Considerações Finais

Discussão

A regulação da infraestrutura digital brasileira encontra-se em um momento de transição, no qual o avanço legislativo proporcionado pelo Marco Civil da Internet e pela Lei Geral de Proteção de Dados deve ser acompanhado por políticas públicas de implementação mais eficazes e integradas. Embora os marcos normativos representem conquistas significativas para a proteção de direitos no ambiente digital, ainda existem lacunas quanto à sua aplicabilidade diante da crescente sofisticação das ameaças cibernéticas.
Nesse cenário, a literatura aponta para a necessidade de fortalecer a articulação entre os diferentes atores envolvidos: governo, setor privado, sociedade civil e organismos internacionais. O Comitê Gestor da Internet (CGI.br) é frequentemente citado como exemplo de governança multissetorial, mas sua atuação precisa ser ampliada para incorporar a gestão de riscos associados a infraestruturas críticas.
A comparação com experiências internacionais demonstra que países que avançaram na regulação digital (como os membros da União Europeia) buscaram alinhar a proteção da privacidade à resiliência cibernética, especialmente com a Diretiva NIS (Network and Information Security). Já no Brasil, apesar de iniciativas como a Estratégia Nacional de Segurança Cibernética (E-Ciber), observa-se a ausência de um sistema mais abrangente de monitoramento e resposta a incidentes em tempo real.
Outro ponto relevante diz respeito à influência da economia digital globalizada. A dependência de plataformas estrangeiras e de serviços em nuvem controlados por grandes corporações transnacionais evidencia desafios de soberania digital. Nesse aspecto, os autores analisados (DENARDIS, 2014; FREITAS et al., 2021) defendem que a regulação deve equilibrar a inovação tecnológica com a autonomia estratégica do país.
Portanto, a discussão revela que, embora o Brasil tenha estabelecido bases regulatórias importantes, o desafio atual consiste em transformar esses instrumentos em ferramentas efetivas de governança e proteção, em um ambiente digital que se caracteriza pela constante mutação e pela interdependência global.

Conclusão

O estudo permitiu observar que o Brasil possui um conjunto de mecanismos regulatórios que avançaram na última década, especialmente com o Marco Civil da Internet e a LGPD, constituindo pilares para a proteção de dados e a governança digital. Contudo, a efetividade desses instrumentos ainda depende de maior articulação institucional, investimentos em resiliência tecnológica e alinhamento com padrões internacionais.

Verificou-se que a segurança cibernética continua sendo um dos pontos mais críticos, exigindo a construção de capacidades estatais e privadas para responder a incidentes, prevenir ataques e fortalecer a confiança digital. A ausência de integração entre órgãos reguladores e a dependência de soluções estrangeiras ampliam a vulnerabilidade da infraestrutura crítica nacional.

As reflexões desenvolvidas reforçam que o caminho para o fortalecimento da infraestrutura digital brasileira passa pela consolidação de uma governança multissetorial, pela ampliação da cooperação internacional e pelo investimento em inovação regulatória. Nesse sentido, o Brasil pode assumir papel protagonista ao integrar proteção de dados, liberdade digital e resiliência cibernética em um modelo que una desenvolvimento econômico e defesa da soberania digital.

Assim, este artigo contribui para o debate acadêmico e político ao evidenciar que a proteção da infraestrutura digital deve ser compreendida como prioridade estratégica da administração pública, pois dela dependem não apenas serviços essenciais, mas também a garantia de direitos fundamentais no século XXI.

Referências

ABNT. (2021). IEC 62443: Segurança de sistemas de automação industrial. https://www.normas.com.br

Abreu, J. C. (2023). Governança digital e cibersegurança no Brasil: Desafios e perspectivas. Revista de Políticas Públicas Digitais, 5(2), 44–61.

Agência Nacional de Energia Elétrica. (2021). Resolução Normativa nº 964, de 24 de agosto de 2021.

Bardin, L. (1977). Análise de conteúdo. Edições 70.

Bourdieu, P. (1983). Questões de sociologia. Marco Zero.

Bourdieu, P. (1990). O poder simbólico. Bertrand Brasil.

Brasil. (2014). Lei nº 12.965, de 23 de abril de 2014 (Marco Civil da Internet).

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

Brasil. (2020). Decreto nº 10.222, de 5 de fevereiro de 2020. Institui a Estratégia Nacional de Segurança Cibernética.

Brasil. (2025). Decreto nº 12.573, de 4 de agosto de 2025. Institui a Estratégia Nacional de Cibersegurança – E-Ciber.

Castells, M. (2009). A sociedade em rede (12ª ed.). Paz e Terra.

CERT.br. (2021). Cartilha de segurança para a internet. https://cartilha.cert.br

DeNardis, L. (2014). The global war for internet governance. Yale University Press.

DeNardis, L. (2020). The internet in everything: Freedom and security in a world with no off switch. Yale University Press.

Doneda, D., & Mendes, L. (2018). Proteção de dados e privacidade no Brasil. FGV Direito Rio.

FBI. (2023). Internet Crime Report 2022. https://www.ic3.gov

Freitas, L. C., Cervieri Guterres, E., Morais, L. E., Moura Filho, R. N., & Talouki, M. A. S. (2021). Regulamentação da segurança cibernética das telecomunicações no Brasil. Revista Latinoamericana de Economía y Sociedad Digital, (2).

Gama, J. R., & Ribeiro, M. A. (2022). Governança digital e proteção de infraestruturas críticas no Brasil. Revista Brasileira de Políticas Públicas, 12(1), 45–62.

ISC². (2023). Cybersecurity workforce study 2023. https://www.isc2.org

Kello, L. (2017). The virtual weapon and international order. Yale University Press.

Mendes, L., Doneda, D., & Monteiro, F. (2019). A LGPD e os desafios da segurança da informação. Revista Brasileira de Políticas Digitais, 2(1), 12–34.

Microsoft. (2024). Cielo speeds threat detection and response with Microsoft Defender XDR and Microsoft Sentinel. https://www.microsoft.com

NIC.br. (2022). Cibersegurança e proteção de infraestruturas críticas. Comitê Gestor da Internet no Brasil.

NIST. (2022). Post-quantum cryptography publications. https://csrc.nist.gov

OCDE. (2019). Good governance for critical infrastructure resilience. OECD Publishing. https://doi.org/10.1787/9789264276623-en

Pinheiro, P. (2020). Direito digital e segurança da informação. Thomson Reuters Brasil.

Schwab, K. (2016). A quarta revolução industrial. Edipro.

Silva, R. F. (2021). Cibersegurança e proteção de infraestruturas críticas no Brasil: Um estudo comparado. Revista Brasileira de Políticas Públicas, 11(3), 102–121.

Sousa, R. (2022). Transformação digital e novos riscos cibernéticos. Revista de Administração Pública Digital, 4(2), 33–49.

Souza, C. A., & Doneda, D. (2018). Proteção de dados pessoais e regulação no Brasil. Revista de Direito Civil Contemporâneo, 14, 51–74.

Souza Júnior, A. F., & Streit, R. E. (2017). Segurança cibernética: Política brasileira e experiência internacional. Revista do Serviço Público, 68(1), 107–130. https://doi.org/10.21874/rsp.v68i1.864

TI Inside. (2024). Cielo conta com ferramentas de cibersegurança para melhorar detecção e resposta a ameaças. https://tiinside.com.br

World Economic Forum. (2023). Global cybersecurity outlook 2023. https://www.weforum.org