DATA CENTERS, ENERGY AND REGULATION: LEGAL AND ECONOMIC CHALLENGES FOR DIGITAL INFRASTRUCTURE IN BRAZIL

CENTROS DE DADOS, ENERGIA E REGULAÇÃO: DESAFIOS JURÍDICOS E ECONÔMICOS PARA A INFRAESTRUTURA DIGITAL NO BRASIL

CENTROS DE DATOS, ENERGÍA Y REGULACIÓN: DESAFÍOS JURÍDICOS Y ECONÓMICOS PARA LA INFRAESTRUCTURA DIGITAL EN BRASIL

https://doi.org/10.56238/sevened2026.008-005

Daniel Amin Ferraz[1], Paulo Roberto Alonso Viegas[2]

ABSTRACT

This article analyzes the legal and economic challenges related to the installation and operation of data centers in Brazil, considering their nature as critical infrastructure and their growing importance in the digital economy. It examines energy demand, technological alternatives for continuous electricity supply, as well as environmental and regulatory impacts. Legislative initiatives in progress and public policy proposals aimed at consolidating a specific regulatory framework are evaluated. The thesis defended is that Brazil's competitiveness in the data economy depends on the creation of a stable regulatory environment, integrated with energy and environmental policies, capable of guaranteeing legal certainty and attracting long-term investments.

Keywords: Data Centers. Energy. Regulation. Critical Infrastructure. Economic Law.

RESUMO

O presente artigo analisa os desafios jurídicos e econômicos relacionados à instalação e operação de data centers no Brasil, considerando sua natureza de infraestrutura crítica e sua crescente importância na economia digital. Examina-se a demanda energética, as alternativas tecnológicas para suprimento contínuo de eletricidade, bem como os impactos ambientais e regulatórios. São avaliadas iniciativas legislativas em tramitação e propostas de política pública voltadas à consolidação de um marco regulatório específico. A tese defendida é a de que a competitividade do Brasil na economia de dados depende da criação de um ambiente regulatório estável, integrado às políticas energéticas e ambientais, capaz de garantir segurança jurídica e atrair investimentos de longo prazo.

Palavras-chave: Data Centers. Energia. Regulação. Infraestrutura Crítica. Direito Econômico.

[1] Dr. in International Business Law. Universidade de Valência. Spain. E-mail: daniel.amin@afctf.adv.br
[2] Master's degree in Economic Sciences. Universidade de Brasília (UnB). Brazil.
E-mail: Attorney-at-law; pviegas@senado.leg.br

RESUMEN
Este artículo analiza los desafíos jurídicos y económicos relacionados con la instalación y operación de centros de datos en Brasil, considerando su naturaleza como infraestructura crítica y su creciente importancia en la economía digital. Se examinan la demanda energética, las alternativas tecnológicas para el suministro continuo de electricidad, así como los impactos ambientales y regulatorios. Se evalúan iniciativas legislativas en curso y propuestas de políticas públicas orientadas a la consolidación de un marco regulatorio específico. La tesis defendida es que la competitividad de Brasil en la economía de los datos depende de la creación de un entorno regulatorio estable, integrado con las políticas energéticas y ambientales, capaz de garantizar seguridad jurídica y atraer inversiones a largo plazo.

Palabras clave: Centros de Datos. Energía. Regulación. Infraestructura Crítica. Derecho Económico.

1 INTRODUCTION

The increasing digitalization of the economy has amplified the relevance of data centers as essential elements of informational infrastructure. These facilities support financial, governmental, logistical, and communication systems, becoming indispensable components for the functioning of contemporary societies. The legal and administrative literature has recognized such structures as critical infrastructure, a term used in Decree No. 9,573 of 2018, which approves the National Policy for Critical Infrastructure Security (PNSIC), to designate services whose disruption severely affects the State and society.

This policy is set forth in the Annex to the aforementioned Decree, defining its essential content and aiming to ensure the security and resilience of the country's critical infrastructures, safeguarding the continuity of their services[3].

Critical infrastructures are understood as facilities, services, assets, and systems whose interruption or destruction, in whole or in part, may cause serious social, environmental, economic, political, or international impacts, or threaten the security of the State and society. The policy also defines concepts such as critical infrastructure security, interdependence among critical infrastructures, and resilience.

From a strictly legal standpoint, the investments in large data centers mentioned herein are not expressly contemplated in Brazilian regulations on "critical infrastructures." However, they may be classified as such should the Executive Branch so determine, given that the current legal regime is open, discretionary, and dependent on complementary administrative acts[4].

---

[3] The National Policy for Critical Infrastructure Security (PNSIC) is grounded in principles such as prevention and precaution based on risk analysis, integration among the Public Authorities, the business sector, and society, reduction of costs arising from security investments, and safeguarding the interests of national defense and security. Among its objectives are the prevention of interruptions in the activities of critical infrastructures or, if interruptions occur, the mitigation of their impacts; the establishment of guidelines and instruments for the protection of infrastructures essential to national security; the integration of data on threats and risks; the identification of interdependencies; and the development of awareness regarding the subject.
The policy also establishes guidelines for integration with other State policies, federative cooperation, coordination with the Brazilian Intelligence System, incentives for public– private partnerships and international cooperation, exchange of knowledge, continuous monitoring of infrastructures, and the permanent updating of security activities. As instruments, it establishes the National Strategy for Critical Infrastructure Security, the National Plan for Critical Infrastructure Security, and the Integrat ed Data System for Critical Infrastructure Security, defining their fundamental functions, as well as the competencies of the Foreign Affairs and National Defense Chamber of the Government Council and the Institutional Security Office of the Presidency of the Republic for the formulation, approval, and management of these instruments. See: BRASIL. Decreto nº 9.573, de 22 de novembro de 2018. Dispõe sobre a Política Nacional de Segurança de Infraestruturas Críticas. Diário Oficial da União: seção 1, Brasília, DF, 23 nov. 2018, p. 5–6.

[4] To date, there is no statute in the Brazilian legal system — in the sense of a law enacted by the Legislative Branch — that specifically addresses the subject of 'critical infrastructures' with the breadth and scope set forth in Decree No. 9,573 of 2018 (and its subsequent developments), a decree which, as previously noted, approved the National Policy for Critical Infrastructure Security (PNSIC). Instead, the regime governing the protection of critical infrastructures is regulated through infra-legal normative acts (administrative in nature, such as decrees). Subsequently, Decree No. 10,569 of 2020 approved the National Strategy for Critical Infrastructure Security, an instrument guiding the PNSIC; and, more recently, Decree No. 11,200 of 2022 approved the PLANSIC plan,

The central thesis of this article is to demonstrate the energy- related challenges associated with the expansion of data centers in Brazil and to assess whether the sustainable development of the sector in the country requires a coherent regulatory framework aligned with energy, environmental, and technological policies, in order to ensure legal certainty, economic predictability, and operational efficiency, based on an interdisciplinary analysis that integrates technical, economic, and legal aspects. In any event, as will be discussed, it is possible to infer that Brazil possesses the conditions to become a hub; however, its reliance on fossil- fuel thermal power generation and the intermittency of renewable sources call for specific regulatory reforms.

2 DATA CENTERS AS CRITICAL INFRASTRUCTURE: TECHNICAL AND LEGAL ASPECTS

Data centers are characterized by the continuous and large-scale processing of digital information, requiring redundant power supply systems, efficient cooling, and high-speed connectivity. International protection, environment, etc.), clear obligations applicable to private and public entities beyond the direct federal administration, and the establishment of

establishing operational guidelines, institutional-sectoral responsibilities, and governance mechanisms. In other words, the existing regulatory framework is based on decrees and public policies, not on ordinary or supplementary legislation.

This situation likely arises from several factors: (1) the fact that initiatives for the protection of critical infrastructure in Brazil historically developed within the Executive Branch through decrees and administrative orders, without the Legislative Branch having structured its own legal framework; (2) the fact that specialized public bodies in this area, such as the Institutional Security Office of the Presidency of the Republic (GSI-PR) and the Chamber of Foreign Affairs and National Defense (CREDEN), coordinate security actions by virtue of delegations contained in decrees, rather than by statute; and (3) findings of certain recent audits, which have identified gaps regarding institutionalization, governance structure, and inter-agency integration, thereby demonstrating weaknesses in the implementation of the policy — circumstances that reinforce the notion that a more robust and formal legal framework could be beneficial.

Therefore, the ‘critical infrastructure’ regime in Brazil depends on higher-order normative acts (decrees), and not on a law enacted by the National Congress, a situation that may generate normative fragility, particularly with respect to long-term predictability, compatibility with other laws (energy, telecommunications, data protection, environment, etc.), clear obligations applicable to private and public entities beyond the direct federal administration, and the establishment of a uniform sanctioning framework.

a uniform sanctioning framework studies[5] show that hyperscale facilities may exceed 100 MW of installed load, demonstrating their reliance on uninterrupted energy supply[6].

In Brazil, estimates indicate the existence of data center structures of varying sizes, still insufficient to meet the growth associated with the expected expansion in the use of artificial intelligence[7]. The dependence of these facilities on complex and interdependent systems — such as electricity, telecommunications, and cooling — reinforces their legal characterization as critical infrastructure, subject to specific public policies and high-stability regulatory requirements.

Moreover, the strategic nature of these environments demands legal certainty regarding environmental licensing, access to electricity, and installation in areas compatible with water availability and network infrastructure. The absence of a systematized regulatory framework creates uncertainty for investors, consistent with warnings raised in the economic law literature[8].

The development of a regulatory framework for the data center sector in Brazil requires a comprehensive normative approach capable of ensuring legal certainty, economic efficiency, personal data protection, operational stability, and environmental sustainability.

---

[5] According to the IEA, hyperscale data center facilities rank among the largest individual energy consumers in the digital sector, frequently exceeding 100 MW of installed load— a level comparable to that of medium-sized industrial units. The IEA emphasizes that these facilities operate continuously and are highly sensitive to interruptions or fluctuations in voltage and frequency, which requires stable, redundant, and high-quality electricity supply. The magnitude of this demand poses significant challenges for energy planning, particularly regarding the need for dedicated substations, transmission reinforcement, and integration with high-voltage networks. Moreover, the expansion of these centers — driven by artificial intelligence applications and high-performance computing — puts pressure on generation capacity and raises questions about the compatibility between uninterrupted consumption and the intermittency of renewable sources. In this context, the observation that hyperscale installations may exceed 100 MW demonstrates not only their structural dependence on continuous supply but also the strategic nature of this sector for national power-system planning and security. International Energy Agency (IEA). Electricity 2023. Paris, 2023, p. 45-51.

[6] It is noted that hyperscale infrastructures already exceed 200 MW in a few cases, with a growing trend. INTERNATIONAL ENERGY AGENCY (IEA). Data Centres and Data Transmission Networks 2023. Paris: IEA, 2023. p. 23–25; ver também: McKINSEY & COMPANY. The Data Center Opportunity. New York: McKinsey, 2023. p. 11–13; UNITED STATES. Department of Energy (DOE). Energy Consumption in Data Centers. Washington, D.C.: DOE, 2022. p. 9–10.

[7] Some analyses highlight the accelerated increase in the use of artificial intelligence by Brazilian companies, the consequent rise in demand for processing capacity, the fact that data centers dedicated to AI training remain, to a large extent, located outside the country, and the projections for the expansion of installed data center capacity in Brazil (from approximately 740 MW in 2024 to 1,210 MW in 2029). These elements underscore the need to expand existing infrastructure in order to keep pace with AI-driven growth. MOODY'S LOCAL BRASIL. Setor de data centers no Brasil: fundamentos, perspectivas e tendências. São Paulo: Moody's Local Brasil, 1 abr. 2025, p. 6 e 7.

[8] According to Richard Posner, the central function of law is to promote efficiency by reducing social and transactional costs. The author argues that legal uncertainty increases transaction costs, discourages investment, and reduces the market's ability to allocate resources efficiently, whereas clear and predictable rules lower the cost of economic decision-making—hence why efficient legal systems tend to generate greater investment and growth. Moreover, ventures such as large data centers involve extremely high CAPEX with long-term returns—a classic type of activity in which, according to Posner, legal certainty is a condition for economic rationality. After all, for this author, environments characterized by uncertainty lead investors to demand higher risk premiums. POSNER, Richard. Economic Analysis of Law. 2007, p. 120-123.

This is a capital -, energy -, and technology-intensive sector, strategic for the country's digital infrastructure, including applications in cloud computing, artificial intelligence, essential public services, and high-capacity communications.

Accordingly, regulation must establish clear parameters for the installation, operation, and oversight of such facilities, in order to harmonize private, collective, and governmental interests.

Initially, it is necessary to define data centers in legal terms, along with their modalities — such as hyperscale, colocation, edge, and public, private, or hybrid clouds — with classification criteria based on size, energy capacity, and level of criticality. From these categories, it becomes possible to regulate environmental and urban licensing, establishing zoning rules, land-use requirements, construction standards, noise limits, and physical security parameters, while observing the particularities of facilities dedicated to processing sensitive data or providing public-interest services.

Another central axis concerns energy infrastructure, given that data centers depend on continuous and stable electrical power. The regulatory framework must include rules for grid connection, energy procurement in the regulated or free markets, the use of renewable sources, efficiency mechanisms (such as PUE[9], WUE[10], and CUE[11] indicators), and redundancy requirements. These measures help ensure operational continuity and encourage the adoption of sustainable cooling, energy- storage, and thermal-management technologies.

In the field of cybersecurity and data protection, the framework must align with the General Data Protection Law (LGPD) and the guidelines of the National Data Protection Authority (ANPD), while also engaging with international technical standards such as ISO

[9] PUE is the most widely used indicator for measuring the energy efficiency of a data center. It expresses the ratio between 'Total Energy' divided by 'Energy Consumed Exclusively by IT Equipment.' The indicator measures how much energy is spent on auxiliary systems (cooling, UPS, lighting, etc.) relative to effective processing. UNITED STATES. Department of Energy. Energy Efficiency in Data Centers: Best Practices Guide. Washington, D.C.: DOE, 2022. p. 14–17.

[10] WUE measures the water efficiency of a data center and is expressed as 'Water Consumed in the Data Center (liters/year)' divided by 'Energy Consumed by IT Equipment (kWh).' The indicator seeks to capture the water impacts of cooling systems, particularly in facilities that use cooling towers, adiabatic cooling, or evaporative free cooling". THE GREEN GRID. Water Usage Effectiveness (WUE™): A Green Grid Data Center Sustainability Metric. Beaverton: The Green Grid, 2011.p. 4–7.

[11] CUE quantifies the carbon impact associated with a data center's energy consumption and is calculated by dividing the facility's 'Annual CO_2 Emissions' by the 'Energy Consumed by IT Equipment (kWh).' This indicator depends on the local electricity mix, as indirect emissions vary according to the energy source (coal, gas, hydropower, solar, nuclear, etc.). INTERNATIONAL ENERGY AGENCY (IEA). Data Centres and Data Transmission Networks 2023. Paris: IEA, 2023. p. 14–18.

27001[12], ISO 27701[13], and NIST[14]. It is essential to establish obligations for incident prevention and notification, auditing mechanisms, business continuity plans, operational redundancy, and specific requirements for processing governmental data and critical infrastructures, thereby ensuring the integrity, confidentiality, and availability of information.

Environmental sustainability constitutes another essential element. Given the high demand for energy and water, particularly for cooling, the framework must establish criteria for water management, energy efficiency, emissions inventories, sustainable construction standards, and recycling of electronic equipment. These parameters promote responsible practices and align the sector with national and international environmental goals.

Connectivity regulation is also relevant, particularly in coordination with the National Telecommunications Agency (Anatel), to address network requirements, link redundancy, service-quality metrics (latency, availability), and compatibility with 5G and 6G policies and edge computing[15]. Addressing these aspects is fundamental to ensure interoperability and high availability of the services provided.

---

[12] ISO 27001 is the leading international standard for information security management, establishing requirements for creating, implementing, maintaining, and continually improving an Information Security Management System (ISMS). Its purpose is to: protect the confidentiality, integrity, and availability of information; establish security controls (technical, administrative, and physical); and standardize cybersecurity risk governance. INTERNATIONAL ORGANIZATION FOR STANDARDIZATION; INTERNATIONAL ELECTROTECHNICAL COMMISSION. ISO/IEC 27001:2022 — Information security, cybersecurity and privacy protection — Information security management systems — Requirements. Geneva: ISO/IEC, 2022. p. v–vi, 1–5.

[13] ISO 27701 is an extension of ISO 27001 focused on privacy and the protection of personal data, establishing the Privacy Information Management System (PIMS). The purpose of this standard is to: operationalize requirements inspired by data protection laws (such as the LGPD and GDPR); guide measures for data governance, minimization, retention, and privacy controls; define the roles of controller and processor; and enable privacy audits. INTERNATIONAL ORGANIZATION FOR STANDARDIZATION; INTERNATIONAL ELECTROTECHNICAL COMMISSION. ISO/IEC 27701:2019 — Security techniques — Extension to ISO/IEC 27001 and ISO/IEC 27002 for privacy information management — Requirements and guidelines. Geneva: ISO/IEC, 2019. p. 1–8, 15–18.

[14] NIST is not a standard, but rather a United States federal agency responsible for producing technical standards and guidelines widely used in cybersecurity, risk management, and digital infrastructure. The most relevant documents issued by the agency include: the NIST Cybersecurity Framework (NIST CSF), a global reference model for cybersecurity risk management; NIST SP 800-53, a catalog of security controls for information systems; NIST SP 800-171, which establishes requirements for protecting sensitive information in non-governmental environments; and the NIST AI Risk Management Framework (2023), which provides guidelines for governance and risk mitigation in artificial intelligence systems. NIST is today the principal international reference in the field of cybersecurity and, in Brazil as well, its guidelines influence IT practices, public policies, audits, and internal corporate standard. NIST Cybersecurity Framework (CSF) - NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY. The NIST Cybersecurity Framework (CSF) 2.0. Gaithersburg, MD: NIST, 2024. p. 1–7, 11–15; NIST SP 800-53 – Catálogo de controles de segurança - NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY. Security and Privacy Controls for Information Systems and Organizations (NIST SP 800-53, Revision 5). Gaithersburg, MD: NIST, 2020. p. 1–13; NIST AI Risk Management Framework - NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY. Artificial Intelligence Risk Management Framework (AI RMF 1.0). Gaithersburg, MD: NIST, 2023. p. 1–10, 13–18.

[1515] Policies for 5G and 6G refer to the set of governmental and sectoral strategies, regulations, and initiatives aimed at guiding the development, deployment, security, and use of emerging technologies. They are crucial because 5G and 6G (the successor to 5G) , as well as edge computing policy, are not merely technological enhancements; rather, they constitute foundational digital infrastructures that reshape the economy, national

The regulatory framework must also consider mechanisms for economic incentives and regional development, such as tax regimes conditioned on efficiency and sustainability targets, the creation of digital- interest zones, and the promotion of technological hubs. In addition, it must provide guidelines for attracting foreign investment, fostering technological partnerships, and supporting research and development in emerging fields such as quantum computing and advanced cooling.

Nonetheless, it is important to emphasize that institutional governance must be clearly structured, defining the competencies of regulatory and supervisory bodies and inspection procedures carried out by the Ministry of Mines and Energy, the Ministry of the Environment and Climate Change, among others. Only through coherent coordination among these institutions will it be possible to ensure the effectiveness of the regulatory framework, avoiding overlaps, gaps, and legal uncertainty.

3 ENERGY, SUSTAINABILITY, AND REGULATORY CHALLENGES

The continuous operation of data centers imposes a high energy demand, with loads exceeding several tens of megawatts. The adoption of renewable sources — solar and wind — faces limitations arising from the natural intermittency of these resources, which compromises the continuous supply required for critical infrastructures.

Although energy storage technologies may mitigate such variability, their cost still represents a significant obstacle[16].

---

security, and social life. The 5G strategy corresponds to the fifth generation of mobile technology, whereas 6G refers to the sixth generation, encompassing more advanced standards for mobile broadband networks. The expression ‘Edge Computing’ refers to a distributed computing model that brings data processing and storage closer to the source that generated them (referred to as the ‘edge’ of the network), instead of sending them to a centralized data center or to the cloud. Its advantages include: drastically reducing latency and required bandwidth, being essential for real-time applications such as autonomous vehicles, remote surgery, and industrial automation; promoting the development of regional micro–data centers; establishing interoperability standards; ensuring the security and privacy of data processed locally; and fostering business models based on edge services. INTERNATIONAL TELECOMMUNICATION UNION (ITU). IMT-2020: Framework and overall objectives of the future development of IMT for 2020 and beyond (ITU-R M.2083-0). Geneva: ITU, 2015. p. 11–25. INTERNATIONAL TELECOMMUNICATION UNION (ITU). IMT-2030 Framework for 6G (Draft Technical Report). Geneva: ITU, 2023. p. 7–22, 28–35. EUROPEAN UNION AGENCY FOR CYBERSECURITY (ENISA). Edge Computing: Benefits, Risks and Best Practices. Athens: ENISA, 2021. p. 9–23, 31–35. 16 According to Edenhofer, the integration of high and continuous electrical loads—such as those of data centers—faces structural challenges when dependent on intermittent renewable sources, whose variable output does not, by itself, meet the requirements of uninterrupted operation. The report acknowledges that storage technologies may reduce such variability; however, it emphasizes that their costs remain high, limiting large-scale adoption. Thus, the reliability of critical infrastructures depends on technological combinations and energy arrangements capable of ensuring stable and secure supply. EDENHOFER, Ottmar. Climate Change 2014: Mitigation of Climate Change. Cambridge, 2014, p. 879-882.

[16] According to the IAEA, SMRs represent a significant evolution in nuclear technology, characterized by reduced power output, modularity, and the possibility of standardized manufacturing in an industrial environment. This approach allows for lower capital costs, accelerated deployment, and greater siting flexibility, including in regions with limited electrical infrastructure. These reactors incorporate enhanced passive safety features, reducing the need for human intervention and increasing operational robustness. Moreover, they can operate in a stable load regime, making them suitable for supporting electric systems with high penetration of renewables. However,

In this context, other alternatives are evaluated, such as biofuels, whose viability depends on regional logistics; thermal generation, which carries non-negligible environmental impacts; Small Modular Reactors (SMRs)[17], still in a phase of technological maturation[18]; and direct connection to the National Interconnected Power System (SIN), viewed as a more stable solution[19].

These options entail legal challenges related to energy policy, decarbonization goals, and environmental licensing, requiring sophisticated regulatory capacity on the part of the State.

In this scenario, the State must also assess the issue of water- based cooling, which, when adopted, tends to rely on closed-loop systems so as to minimize losses. Current examples indicate optimized levels of losses below 2% per year[20], thereby reducing environmental pressure associated with water use.

4 LEGISLATIVE INITIATIVES AND PUBLIC POLICIES UNDER DEVELOPMENT

their commercial development depends on regulatory advances, international standardization, and demonstration of economic viability at scale. INTERNATIONAL ATOMIC ENERGY AGENCY (IAEA). Advances in Small Modular Reactor Technology. Viena, 2020, p.29- 37.

[17] According to Edenhofer, the integration of high and continuous electrical loads—such as those of data centers—faces structural challenges when dependent on intermittent renewable sources, whose variable output does not, by itself, meet the requirements of uninterrupted operation. The report acknowledges that storage technologies may reduce such variability; however, it emphasizes that their costs remain high, limiting large-scale adoption. Thus, the reliability of critical infrastructures depends on technological combinations and energy arrangements capable of ensuring stable and secure supply. EDENHOFER, Ottmar. Climate Change 2014: Mitigation of Climate Change. Cambridge, 2014, p. 879-882.

[18] According to Nayar et al., technological consolidation in the data center sector is directly related to advances in high-power energy storage systems, which are essential for ensuring continuity, stability, and operational efficiency. The authors highlight that data centers require fast response times, high reliability, and the capacity to withstand sudden load variations—factors that drive the adoption of technologies such as lithium-ion batteries, supercapacitors, and flywheels. These solutions have been undergoing a maturation phase, with improvements in energy density, durability, safety, and cost per cycle. Nayar et al. note that intelligent integration among storage, thermal management, and power-quality systems constitutes a central element of this consolidation phase, enabling greater autonomy, emissions reduction, and compatibility with intermittent renewable sources. However, they emphasize that cost and scalability challenges still limit full adoption in large-scale projects. NAYAR, Chemmangot V. et al. High-Power Energy Storage Systems. London, 2020, p. 303-320.

[19] Direct connection to the SIN system constitutes, for facilities classified as critical, the most stable and predictable alternative for electricity supply. The SIN offers greater capacity to respond to demand fluctuations; reduced risk of interruptions due to the interconnection of multiple sources and regions; operational standardization through unified quality and safety criteria; and structural redundancy, which mitigates local or regional failures. TRIBUNAL DE CONTAS DA UNIÃO (TCU). Relatório de Auditoria Operacional sobre Infraestrutura Crítica. 2021, p. 58-60.

[20] According to ASHRAE, liquid cooling systems in data centers require careful technical and regulatory assessment, particularly regarding the use of natural resources and compliance with environmental standards. The organization emphasizes that closed-loop systems are the recommended practice, as they significantly reduce water consumption, achieving losses of less than 2% per year in optimized facilities. These systems enhance thermal efficiency but require appropriate infrastructure, continuous monitoring, and compliance with environmental and safety regulations—factors that pose regulatory challenges for authorities responsible for licensing and energy policy. ASHRAE – American Society of Heating, Refrigerating and Air-Conditioning Engineers. ASHRAE Datacom Series – Liquid Cooling Guidelines for Datacom Equipment Centers. Atlanta: ASHRAE, 2016. p. 56–62, 103–105.

Brazil currently has no federal statute—meaning a law enacted by the Legislative Branch—that specifically regulates investments in large data centers or establishes a dedicated legal framework for this type of enterprise. What exists today are scattered sectoral norms — concerning telecommunications, electricity, data protection, tax incentives, or innovation — that affect the deployment and operation of data centers but do not constitute a legal regime dedicated to the sector.

Examples of such legislation include the General Telecommunications Law (Law No. 9,472 of 1997), the Brazilian Internet Bill of Rights (Law No. 12,965 of 2014), the General Data Protection Law – LGPD (Law No. 13,709 of 2018), as well as the Electricity Law and related statutes (such as Laws No. 9,074 of 1995 and 9,427 of 1996, among others). None of these laws treat data centers as a distinct regulatory category. They apply indirectly, but none creates obligations, benefits, or specific regulatory treatment for the installation, operation, or attraction of large data centers.

Nevertheless, there are relevant infra-legal norms, although none directed toward investment. In these cases, data centers appear only as essential infrastructure or strategic equipment within certain administrative instruments, such as decrees on digital strategy, cybersecurity, and critical infrastructure (although they do not expressly classify data centers as critical). Norms issued by ANEEL and the electricity system—governing grid access, self-generation, and transmission and distribution tariffs—affect energy costs; resolutions of the National Data Protection Authority (ANPD) govern information security and data governance, but not physical investment; and telecommunications rules from Anatel apply mainly when the data center integrates communication networks. None of these norms establishes incentives, special licensing categories, or a distinct legal status for the sector.

Regarding federal tax incentives, there is no specific or permanent program aimed at major data center investments. Brazil does not, for instance, have a federal policy to attract hyperscalers, unlike Ireland, Chile, the United States, Singapore, or the United Arab Emirates[21].

[21] According to ASHRAE, liquid cooling systems in data centers require careful technical and regulatory assessment, particularly regarding the use of natural resources and compliance with environmental standards. The organization emphasizes that closed-loop systems are the recommended practice, as they significantly reduce water consumption, achieving losses of less than 2% per year in optimized facilities. These systems enhance thermal efficiency but require appropriate infrastructure, continuous monitoring, and compliance with environmental and safety regulations—factors that pose regulatory challenges for authorities responsible for licensing and energy policy. ASHRAE – American Society of Heating, Refrigerating and Air-Conditioning Engineers. ASHRAE Datacom Series – Liquid Cooling Guidelines for Datacom Equipment Centers. Atlanta: ASHRAE, 2016. p. 56–62, 103–105. According to ASHRAE, liquid cooling systems in data centers require careful technical and regulatory assessment, particularly regarding the use of natural resources and compliance with environmental standards. The organization emphasizes that closed-loop systems are the recommended practice, as they significantly reduce water consumption, achieving losses of less than 2% per year in optimized facilities. These systems enhance thermal efficiency but require appropriate infrastructure, continuous

However, certain Brazilian states—particularly São Paulo, Ceará, Rio Grande do Sul, Minas Gerais, and the Federal District—grant ICMS tax benefits for such investments, though these incentives arise from state-level technology promotion programs.

Therefore, it can be said that no federal law exists to regulate investments in large data centers in Brazil, whether as an economic sector, as strategic infrastructure, or as a matter of State policy.

Even so, several bills are currently under consideration— especially those related to digital sovereignty, classification of critical infrastructure, artificial intelligence policy, and the creation of technological zones—which touch upon the need to treat data centers as a strategic sector. Moreover, Congress is presently examining proposals that aim to establish specific rules for data centers, although none has yet been enacted.

Senate Bill No. 3,018 of 2024 addresses data centers dedicated to artificial intelligence, while House Bill No. 2,080 of 2025 creates the National Policy for Energy Efficiency and Socio-environmental Sustainability for Data Centers. Both measures signal a growing awareness of the need for sector-specific regulation.

In parallel, the Executive Branch is preparing the National Data Center Policy (Redata), in the form of a Provisional Measure, providing for tax exemptions, regional development incentives, renewable energy targets, and the reservation of computing capacity for the domestic market. International literature indicates that stable regulatory environments and fiscal incentives play a decisive role in consolidating digital hubs, as demonstrated by the cases of Ireland and Singapore[22].

From a legal standpoint, these policies raise issues related to fiscal responsibility, constitutionality of incentives, distribution of competences among federal entities, and integration with sectoral policies— particularly energy and the environment.

Thus, the lack of a specific regulatory framework for large data centers in Brazil results in an environment marked by significant legal uncertainty. Investors seeking to establish or expand such enterprises lack clear normative parameters regarding essential elements such as environmental and urban licensing, energy access and procurement, applicable tax

monitoring, and compliance with environmental and safety regulations—factors that pose regulatory challenges for authorities responsible for licensing and energy policy. ASHRAE – American Society of Heating, Refrigerating and Air-Conditioning Engineers. ASHRAE Datacom Series – Liquid Cooling Guidelines for Datacom Equipment Centers. Atlanta: ASHRAE, 2016. p. 56–62, 103–105.

[22] According to O'Riain, Ireland's consolidation as a digital hub resulted from a combination of regulatory stability, coordinated industrial policies, and aggressive tax incentives, which attracted major technology companies and fostered strong integration with global value chains. The author shows that legal predictability and an investment- friendly environment were decisive for the establishment of data centers and digital operations in the country. Similar policies appear in other international hubs, such as Singapore, demonstrating that stable regulation and economic incentives are structural factors for the development of competitive digital ecosystems. O'RIAIN, Sean. The Rise and Fall of Ireland's Celtic Tiger. Cambridge, 2014, p. 215-231.

regimes, minimum redundancy requirements, and mandatory technical standards. Even though investments have occurred under these conditions (from companies such as Ascenty, Equinix, Scala, etc.), the volume could be greater if the regulatory environment were more structured. This normative gap increases uncertainty and hinders the planning of capital- and infrastructure-intensive projects.

The situation is worsened by excessive administrative discretion. In the absence of uniform guidelines, critical decisions depend on local interpretations—often divergent—by environmental, energy, or urban management authorities, resulting in regulatory asymmetry between regions and undermining the predictability required for long-term investments. Furthermore, the lack of a legal classification of data centers as critical infrastructure prevents their formal prioritization in policies related to energy supply, public security, and civil protection, even though such facilities are essential for the continuity of banking, governmental, telecommunications, and artificial intelligence services. This lack of definition increases the risk of litigation, as the absence of unified legal standards facilitates administrative and judicial challenges, especially in large-scale projects.

From an economic and strategic perspective, the effects are equally significant. Countries with consolidated regulatory frameworks— such as Ireland, Singapore, the United States, and EU member states—have been preferred by major global operators due to legal predictability and the existence of specific incentive regimes. The absence of normative discipline in Brazil results in loss of international competitiveness and higher capital costs, as regulatory risk increases the weighted average cost of capital (WACC) and makes new facilities more expensive to implement. Additionally, there is systemic risk: interruptions in data centers may affect essential sectors, compromising the operation of cloud- and AI-based systems. The lack of a structured national framework also tends to intensify external dependence, as an increasing volume of computational load is transferred abroad, which has implications for Brazilian digital sovereignty.

From an institutional perspective, the situation is concerning. There is no clearly defined sectoral regulatory authority, resulting in coordination failures among bodies such as the Ministry of Mines and Energy (MME), the ANPD, Anatel, the Institutional Security Office (GSI), and other federal and subnational entities. National energy planning does not incorporate a specific methodology for large data centers. Moreover, the absence of a dedicated tariff classification prevents appropriate price signaling and limits incentives for energy efficiency.

Given this scenario, it is concluded that the absence of a regulatory framework constitutes a significant risk to the public interest, national security, and the business

environment. It is therefore recommended that a federal law be enacted addressing the following elements: classification of data centers as critical infrastructure; creation of a specific legal regime for licensing, resilience, data protection, and energy; establishment of Special Digital Infrastructure Zones; implementation of regulatory and tariff incentives conditioned on efficiency and security targets; and the development of integrated federal planning in coordination with states and municipalities.

5 PROPOSALS FOR A COHERENT REGULATORY FRAMEWORK

The construction of a regulatory framework for data centers in Brazil must rest upon three fundamental dimensions, without which it is impossible to establish a legal environment capable of attracting investment, ensuring operational continuity, and promoting national technological development. The first dimension is legal certainty, which requires the formulation of clear and uniform rules regarding environmental licensing, access to networks and energy sources, and the instruments of promotion and economic incentives applicable to the sector. The absence of objective and predictable parameters undermines decision-making by private actors, increases regulatory risk, and raises the cost of capital, particularly in a sector characterized by large-scale undertakings and long-term return horizons.

The second dimension concerns economic efficiency. Data centers are highly energy - and technology-intensive facilities, which is why the regulatory framework must provide tariff rationality, mechanisms for energy procurement compatible with the needs of predictability and continuity of supply, as well as incentives for innovation, adoption of emerging technologies, and continuous performance improvement. Economic efficiency also demands that the regulatory framework harmonize systemic costs, risks of network congestion, and strategies for expanding digital infrastructure, allowing investments to be allocated rationally and in line with market dynamics.

The third essential dimension is environmental sustainability, which must guide the rational use of natural resources — especially water and energy — and establish clear targets for emissions reduction and the promotion of a low-carbon economy. Considering that large data centers play an increasingly significant role in global energy demand, it is imperative that the regulatory framework incorporate mechanisms that encourage efficiency, minimum standards for energy performance, and support for research and development of technological solutions capable of reducing the environmental footprint of these facilities. The incorporation of environmental criteria is not merely a requirement of public policy but an element of international competitiveness, particularly in a market in which major operators prioritize regulatory environments that align with global decarbonization commitments.

The economic law literature consistently records that capital- intensive sectors — such as the data center industry — depend on high levels of regulatory predictability for long-term investment decisions[23]. The absence of a stable regulatory framework hinders cost forecasting, the execution of energy supply contracts, and the formulation of corporate strategies, all of which negatively affect the country's attractiveness. Likewise, contemporary regulatory theories highlight the importance of governance models that are flexible, transparent, and evidence-based, capable of responding to rapid technological transformations and disruptive innovations characteristic of the digital economy[24]. Regulation, in this context, must be dynamic, coordinated, and guided by regulatory impact assessment, ensuring that norms evolve at the same pace as the technologies they seek to govern, without imposing excessive costs or unjustified barriers to economic activity[25].

6 FINAL COMMENTS

Brazil possesses relevant conditions to consolidate itself as a hub of digital infrastructure in Latin America, notably due to its availability of renewable energy sources, strategic geographic position, and the growth of the digital services market. However, the absence of an integrated regulatory framework limits the predictability required to attract large-scale investments.

It follows that the consolidation of the sector depends on: (a) legal certainty and regulatory stability; (b) an energy policy aligned with the needs of data centers; (c) robust environmental and technological governance; and (d) incentive mechanisms compatible with energy transition goals and digital sovereignty.

---

[23] According to Bercovici, capital-intensive sectors require stable regulatory frameworks capable of reducing uncertainties and guiding long-term investment decisions. The author emphasizes that normative predictability is a condition for economic efficiency, as it lowers transaction costs, increases the confidence of private actors, and facilitates coordination between the State and the market. Without regulatory stability, structural investments—such as those required for digital or industrial infrastructure—tend to be postponed or become more costly, thereby undermining development. Thus, clear and consistent regulation is a central element of economic policy in sectors of high complexity and substantial CAPEX. BERCOVICI, Gilberto. Direito Econômico. São Paulo: Malheiros, 2018,p77-85.

[24] According to Bercovici, capital-intensive sectors require stable regulatory frameworks capable of reducing uncertainties and guiding long-term investment decisions. The author emphasizes that normative predictability is a condition for economic efficiency, as it lowers transaction costs, increases the confidence of private actors, and facilitates coordination between the State and the market. Without regulatory stability, structural investments—such as those required for digital or industrial infrastructure—tend to be postponed or become more costly, thereby undermining development. Thus, clear and consistent regulation is a central element of economic policy in sectors of high complexity and substantial CAPEX. BERCOVICI, Gilberto. Direito Econômico. São Paulo: Malheiros, 2018,p77-85.

[25] It must be considered, however, that the existence of the National Interconnected Power System (SIN) is itself a means of mitigating the limitations of each generation source — in other words, the SIN already performs the function of managing the intermittency of It must be considered, however, that the existence of the National Interconnected Power System (SIN) is itself a means of mitigating the limitations of each generation source — in other words, the SIN already performs the function of managing the intermittency of

A coherent regulatory system will enable Brazil to compete globally, strengthen its critical infrastructure, and expand its capacity for innovation.

REFERENCES

American Society of Heating, Refrigerating and Air-Conditioning Engineers. (2016). ASHRAE Datacom Series: Liquid cooling guidelines for datacom equipment centers. ASHRAE.

Baldwin, R., Cave, M., & Lodge, M. (2012). Understanding regulation. Oxford University Press.

Bercovici, G. (2018). Direito econômico. Malheiros.

Brasil. (2018). Decreto nº 9.573, de 22 de novembro de 2018. Dispõe sobre a Política Nacional de Segurança de Infraestruturas Críticas. Diário Oficial da União, seção 1, Brasília, DF.

Edenhofer, O. (2014). Climate change 2014: Mitigation of climate change. Cambridge University Press.

European Union Agency for Cybersecurity. (2021). Edge computing: Benefits, risks and best practices. ENISA.

International Telecommunication Union. (2015). IMT-2020: Framework and overall objectives of the future development of IMT for 2020 and beyond (ITU-R M.2083-0).

International Telecommunication Union. (2023). IMT-2030 framework for 6G (Draft Technical Report).

Moody's Local Brasil. (2025). Setor de data centers no Brasil: Fundamentos, perspectivas e tendências.

International Atomic Energy Agency. (2020). Advances in small modular reactor technology.

International Energy Agency. (2023a). Data centres and data transmission networks 2023.

International Energy Agency. (2023b). Electricity 2023.

International Organization for Standardization; International Electrotechnical Commission. (2022). ISO/IEC 27001:2022: Information security, cybersecurity and privacy protection — Information security management systems — Requirements.

International Organization for Standardization; International Electrotechnical Commission. (2019). ISO/IEC 27701:2019: Security techniques — Extension to ISO/IEC 27001 and ISO/IEC 27002 for privacy information management — Requirements and guidelines.

McKinsey & Company. (2023). The data center opportunity.

Nayar, C. V., et al. (2020). High-power energy storage systems.

National Institute of Standards and Technology. (2023). Artificial Intelligence Risk Management Framework (AI RMF 1.0).

National Institute of Standards and Technology. (2024). The NIST Cybersecurity Framework (CSF) 2.0.

National Institute of Standards and Technology. (2020). Security and privacy controls for information systems and organizations (NIST SP 800-53, Revision 5).

O'Riain, S. (2014). The rise and fall of Ireland's Celtic Tiger. Cambridge University Press.

Pereira, A. L. C., Araújo, L. A. B., & Giambiagi, F. (Orgs.). (2020). O setor elétrico brasileiro: Desafios e oportunidades. Elsevier.

The Green Grid. (2011). Water Usage Effectiveness (WUE™): A Green Grid data center sustainability metric.

Tolmasquim, M. T. (2016). Matriz energética brasileira: Formação, desafios e perspectivas (2ª ed.). Elsevier.

Tribunal de Contas da União. (2021). Relatório de auditoria operacional sobre infraestrutura crítica.

United States. Department of Energy. (2022a). Energy consumption in data centers.

United States. Department of Energy. (2022b). Energy efficiency in data centers: Best practices guide.

United States Government Accountability Office. (2021). Federal data centers: Optimization, consolidation, and security.