
FOREIGN INVESTMENT IN AI DATA CENTRES IN INDIA: BALANCING INVESTOR PROTECTION, DIGITAL SOVEREIGNTY AND ENVIRONMENTAL REGULATORY AUTONOMY

Pragya Sharma¹ & Prachi Tripathi²

ABSTRACT

The expansion of artificial intelligence is creating a new class of digital infrastructure in India: high-density data centres designed to provide large-scale computing, storage, networking and cooling capacity. These facilities attract foreign capital and can support digital services, employment, cloud computing and national AI ambitions, but they also raise difficult questions concerning investor protection, control over data and environmental resource allocation. This paper examines the interaction between India's foreign investment regime, digital-data governance and environmental regulation through the lens of international investment law. It argues that the central challenge is not whether India should protect investors or regulate data centres, but how it can preserve regulatory space while maintaining predictability and non-discrimination. The paper evaluates fair and equitable treatment, legitimate expectations, expropriation and national treatment alongside India's data-governance and environmental powers. It also compares regulatory approaches in the European Union, China, Singapore, the UAE and Brazil. The paper proposes a coordinated framework based on transparent approval criteria, technology-neutral sustainability standards, risk-based data governance, regulatory-impact assessment and carefully drafted investment treaties. Such an approach can attract long-term investment without converting legitimate digital and environmental regulation into an avoidable source of investment disputes.

Keywords: Artificial Intelligence; AI Data Centres; Foreign Investment; Digital Sovereignty; Environmental Regulatory Autonomy; International Investment Law.

¹ CB&IL LLM, Amity Law School, Amity University, Noida

² CB&IL LLM, Amity Law School, Amity University, Noida

1. Introduction

1.1 Background and Context

Data centres have moved from being relatively invisible components of information technology infrastructure to becoming strategic assets of the digital economy. The development of generative AI, large language models, advanced analytics and high-performance computing has intensified this transformation.³ AI workloads require dense computational infrastructure, sophisticated networking and substantial cooling capacity. Consequently, an AI data centre is not merely a warehouse for servers; it is an energy-intensive infrastructure project with implications for electricity planning, water availability, land use, telecommunications, cybersecurity and economic policy. India is becoming a significant destination for data-centre investment because of its large digital economy, expanding internet and cloud markets, availability of technical talent, improving connectivity and government support for digital infrastructure. Official information indicates that India's total data-centre capacity increased from approximately 375 MW in 2020 to around 1,500 MW by 2025 (Ministry of Electronics and Information Technology, 2026). The same official material records the deployment of thousands of GPUs under India's AI compute-capacity initiatives. These figures illustrate the speed with which computational infrastructure is becoming an element of national economic strategy.⁴

Foreign capital is particularly important because hyperscale and AI data-centre projects require very large upfront expenditure. International investors may finance land acquisition or leasing, buildings, power infrastructure, cooling systems, servers, fibre connectivity and renewable-energy arrangements. At the same time, the State has a legitimate interest in ensuring that foreign investment does not undermine national security, personal-data protection, electricity reliability, water security or environmental objectives. The resulting legal problem is therefore multidimensional: a measure designed to protect one public interest may affect the economic assumptions underlying another. India's policy architecture reflects this complexity. The Department for Promotion of Industry and Internal Trade describes India's FDI regime as liberal, with foreign investment up to 100 percent permitted under the automatic route in most sectors and activities, subject to applicable conditions (DPIIT, 2025). Data centres, however,

³ International Energy Agency, 2025; Ministry of Electronics and Information Technology, 2026

⁴ International Energy Agency, 2025; Ministry of Electronics and Information Technology, 2026

operate within a wider regulatory environment. The Foreign Exchange Management Act, 1999, information-technology legislation, data-protection rules, electricity regulation, environmental statutes, building requirements and state-level policies can all influence the feasibility and cost of a project.⁵

The environmental dimension is becoming more significant as AI computing expands. Electricity is required not only for computing equipment but also for cooling and ancillary systems. Water may be consumed by particular cooling technologies, while land and grid capacity may become scarce in locations attractive to data-centre developers. In August 2026, the Ministry of Environment, Forest and Climate Change explained that AI data centres do not, merely by being AI data centres, automatically require environmental clearance under the Environmental Impact Assessment Notification, 2006; clearance can nevertheless be required where the project falls within specified building and construction or township and area-development categories. The Ministry also referred to water balance, freshwater availability, recycling and reuse as relevant considerations for projects requiring clearance (Ministry of Environment, Forest and Climate Change, 2026).⁶

1.2 Research Problem

The principal research problem lies in balancing three competing objectives: protecting foreign investors through a stable and predictable regulatory environment; preserving India's digital sovereignty over data and strategic digital infrastructure; and maintaining the State's authority to regulate energy, water, emissions, land and environmental impacts. While these objectives can coexist, regulatory changes after investment may create uncertainty and potential conflicts under international investment law.

Although investment treaties do not generally provide immunity from regulation, arbitrary or discriminatory measures, serious procedural unfairness, frustrated legitimate expectations or measures amounting to indirect expropriation may give rise to investor claims. This concern is particularly relevant to AI data centres because they involve substantial, long-term capital commitments and significant technological and environmental requirements.

⁵ Department for Promotion of Industry and Internal Trade, 2025; Government of India, 1999; Ministry of Electronics and Information Technology, 2023

⁶ Ministry of Environment, Forest and Climate Change, 2026

The study therefore examines whether India's existing framework provides sufficient regulatory certainty to attract foreign investment while preserving regulatory autonomy, and whether future investment treaties and domestic policies should provide clearer safeguards, public-interest exceptions and transition mechanisms.

1.3 Research Questions

- How does India's legal and policy framework regulate foreign investment in AI data-centre infrastructure?
- How may investor-protection standards such as fair and equitable treatment, legitimate expectations and indirect expropriation interact with data-governance and environmental measures?
- What is the legal and economic rationale for digital sovereignty and data localisation, and what costs may excessive localisation create?
- How can India preserve environmental regulatory autonomy while maintaining a predictable investment climate?

1.4 Scope, Methodology, and Structure

The paper adopts a doctrinal and comparative legal methodology. Primary sources include Indian statutes, subordinate legislation, government policies, official regulatory materials and investment-treaty texts. Secondary materials are used to interpret international investment-law concepts and comparative approaches. The study focuses on foreign investment in physical AI and data-centre infrastructure rather than foreign investment in AI software generally. It examines India as the principal jurisdiction and uses comparative jurisdictions to illuminate possible regulatory choices rather than to provide exhaustive country studies.

The analysis proceeds from the conceptual relationship between investment protection, digital sovereignty and environmental regulatory autonomy to India's domestic regulatory framework. It then examines treaty standards and their potential application to data and environmental measures, before considering localisation and environmental impacts. Comparative experience is followed by reform proposals intended to reduce uncertainty without restricting legitimate regulation.

2. Conceptual and Legal Framework

2.1 Foreign Direct Investment and Investor Protection

Foreign direct investment is relevant to AI data centres because the projects generally involve durable capital, managerial participation, infrastructure ownership or control and a long-term commercial presence. The legal protection available to a foreign investor depends on both domestic law and the international instruments applicable to the investor's nationality. Domestic investment law determines admission, ownership conditions, foreign-exchange compliance and sectoral requirements. Investment treaties may provide additional substantive and procedural rights.⁷

The contemporary investment-law debate is not adequately captured by a simple opposition between investor rights and State sovereignty. Modern treaty practice increasingly attempts to preserve a regulatory balance. India's 2015 Model Bilateral Investment Treaty (BIT), for example, was expressly presented by the Government as an effort to provide investor protection while maintaining a balance with governmental obligations. Its design includes national treatment, protection against expropriation, due process and an investor-State dispute settlement mechanism subject to conditions, while excluding or limiting certain matters such as taxation, subsidies, compulsory licensing and national security.⁸

For data-centre investment, the practical importance of investor protection lies in regulatory predictability. A foreign investor may make decisions based on representations concerning land, electricity, incentives, connectivity or approvals. However, commercial expectations must be distinguished from legally protected expectations. A general policy statement promising investment facilitation is ordinarily different from a specific and legally attributable assurance that regulation will not change. This distinction is essential because digital and environmental regulation necessarily evolves with technology and scientific knowledge.⁹

2.2 Digital Sovereignty and Data Localisation

Digital sovereignty refers broadly to a State's capacity to govern digital infrastructure, technologies, data and digital economic activity according to domestic public interests. It has

⁷ Department for Promotion of Industry and Internal Trade [DPIIT], 2025; Reserve Bank of India [RBI], 2019

⁸ Government of India, 2015

⁹ Government of India, 2015

multiple dimensions, including control over critical infrastructure, cybersecurity, strategic autonomy, privacy, competition, lawful access to data and resilience of digital systems. Data localisation is only one possible instrument. It can require data to be stored domestically, processed domestically, or subjected to conditions before cross-border transfer.¹⁰

The legal policy justification for localisation may be especially strong for sensitive government information, critical infrastructure data or categories of personal data requiring heightened protection. Yet blanket localisation can also raise costs by preventing firms from using geographically distributed cloud architectures and disaster-recovery systems. It may reduce economies of scale and create incentives for duplicative infrastructure. The policy question is therefore not whether localisation is inherently good or bad but whether the restriction is connected to a demonstrable regulatory objective and calibrated to the risk involved.

India's Digital Personal Data Protection Act, 2023 is significant because it establishes a statutory framework for processing digital personal data while recognising both individual data-protection interests and lawful processing needs (Government of India, 2023). The Act should not, however, be described as imposing a universal requirement that all data be stored in India. Its framework concerns processing and cross-border transfer subject to statutory and governmental mechanisms. The distinction between data-centre geography and data-transfer restrictions is therefore fundamental to legal analysis.

2.3 Environmental Regulatory Autonomy

Environmental regulatory autonomy is the State's capacity to determine and enforce environmental standards without being treated as commercially illegitimate merely because compliance imposes costs on investors. In the data-centre context, this autonomy includes decisions about environmental clearance, construction, water abstraction, wastewater, energy efficiency, renewable-energy procurement, emissions and local infrastructure capacity.¹¹

Indian environmental law is grounded in legislation as well as constitutional and judicial principles. The Environment (Protection) Act, 1986 empowers the Central Government to take measures for protecting and improving environmental quality. The Water (Prevention and Control of Pollution) Act, 1974 regulates pollution and establishes consent mechanisms

¹⁰ Government of India, 2023

¹¹ Government of India, 1986; Government of India, 1974

concerning specified discharges. Electricity and energy-conservation legislation adds another layer, allowing regulators and governments to shape energy consumption and efficiency. These powers are not displaced simply because a project is foreign-owned.¹²

3. The Indian Regulatory Landscape

3.1 FEMA, 1999 and FDI Policy on Data Centres

FEMA provides the statutory architecture for regulating foreign exchange and cross-border capital transactions. Section 6 historically provided the framework for capital-account transactions involving non-residents, with the detailed regime now operating through regulations and rules made under FEMA. For foreign investment, the Foreign Exchange Management (Non-Debt Instruments) Rules, 2019 and related RBI directions operate together with the government's FDI policy. The precise compliance position depends on the structure of the investment, the sector and the transaction involved. India's FDI policy generally adopts a liberal approach. DPIIT materials state that FDI up to 100 percent is permitted under the automatic route in most sectors and activities, subject to conditions (DPIIT, 2025). For data-centre businesses, this facilitates foreign participation where no separate sectoral restriction applies. The regulatory challenge is therefore less about an outright ownership prohibition and more about the cumulative compliance burden imposed by land, construction, power, taxation, data governance and environmental regulation.¹³

This distinction has investment-law significance. A foreign investor entering a liberal market cannot reasonably assume that liberal entry means regulatory immobility. At the same time, government incentives and approval representations should be sufficiently clear to prevent avoidable disputes. State-level data-centre policies can be especially important because incentives may include electricity-related concessions, stamp-duty benefits, land facilitation, infrastructure support and other fiscal or administrative measures. Such benefits should be drafted with transparent eligibility conditions and change-management provisions.¹⁴

¹² Government of India, 1986; Government of India, 1974; Government of India, 2001; Government of India, 2003

¹³ DPIIT, 2025; RBI, 2019

¹⁴ Government of India, 2015; Invest Uttar Pradesh, 2021

3.2 Information Technology Act, 2000 and the DPDP Act, 2023

The Information Technology Act, 2000 remains a central statute for electronic systems, cybersecurity-related obligations and certain forms of intermediary and computer-resource regulation. Although its architecture predates generative AI, it continues to form part of the legal environment within which digital infrastructure operates. The statutory framework has been supplemented by subordinate rules and sectoral measures dealing with security, incident reporting and other digital risks.

The DPDP Act represents a newer statutory layer. Its purpose is to regulate digital personal-data processing while protecting individuals' data interests and enabling lawful processing. For data-centre investors, the compliance consequences may arise through their role as data processors, data fiduciaries or infrastructure providers, depending on the contractual and technical structure of the service. A colocation facility, cloud provider and entity controlling the purposes of processing should not automatically be treated as the same legal actor.

The transition from older information-technology regulation to the DPDP framework also illustrates a central issue in this paper: regulatory change is normal in a technology sector. Investors should expect rules to evolve, but the State can reduce dispute risk by giving clear implementation timelines, publishing guidance, applying requirements consistently and using proportionate enforcement. This is particularly important where compliance requires expensive redesign of storage architecture, security systems or cross-border data flows.

3.3 Environmental Clearance and Energy Regulation

The EIA Notification, 2006 establishes a prior environmental-clearance framework for specified categories of projects. The present legal position is significant because AI data centres do not automatically require environmental clearance solely because they are AI facilities. According to a 2026 Ministry of Environment response, an AI data centre forming part of a building and construction project exceeding the applicable threshold under Item 8(a), or a township and area-development project meeting Item 8(b) thresholds, can require prior environmental clearance. The Ministry also stated that freshwater availability, water balance, greywater generation, recycling and reuse can be considered during appraisal.¹⁵

¹⁵ Ministry of Environment, Forest and Climate Change [MoEFCC], 2026

The Water Act provides a further regulatory mechanism. Section 25 restricts new outlets and discharges without the consent of the State Pollution Control Board, subject to the statutory framework. For large facilities, wastewater and cooling-related discharges may therefore become part of environmental compliance. Groundwater extraction is also subject to central guidelines and regulatory controls. These requirements can materially influence site selection, particularly in water-stressed areas.¹⁶ Energy regulation is equally important. The Energy Conservation Act, 2001 provides the institutional framework for energy efficiency, while the Electricity Act, 2003 regulates generation, transmission, distribution and open access. The Electricity (Promoting Renewable Energy Through Green Energy Open Access) Rules, 2022 facilitate procurement and consumption of green energy through specified mechanisms. Data-centre operators can therefore structure their energy strategy around grid supply, captive generation, renewable-energy procurement and open-access arrangements, subject to applicable state and regulatory conditions.

The legal significance is that environmental and energy requirements are not externalities to the investment regime. They are part of the operating environment in which the investment is made. A coherent policy should therefore communicate these requirements before capital is irreversibly committed. Clear standards can actually strengthen investor confidence because they reduce the risk that individual projects will face ad hoc demands after construction.

3.4 State-Level Incentives and Land Policy

Data-centre investment is strongly influenced by state-level policy because electricity tariffs, land availability, industrial infrastructure, building permissions and local incentives are substantially implemented at the state level. Uttar Pradesh provides a useful illustration. Its official data-centre policy materials reported proposed investments of more than INR 21,000 crore and proposed capacity of 644 MW as of June 2025, alongside multiple commercialised projects (Uttar Pradesh Electronics Corporation Limited, 2026). Such policy competition can accelerate investment but also creates a risk of fragmented standards.¹⁷

State incentives should therefore be linked to measurable public benefits rather than simply announced investment values. Possible conditions include employment, local procurement, renewable-energy use, water-efficiency performance and infrastructure contributions.

¹⁶ Government of India, 1974; Central Ground Water Authority, 2020

¹⁷ Invest Uttar Pradesh, 2025

However, incentive conditions should be transparent and applied prospectively. Sudden withdrawal of a contractual concession is legally different from a general environmental regulation of future operations, and the distinction may matter in domestic and international proceedings.

4. Investor Protection and Bilateral Investment Treaties

4.1 Relevant Treaty Provisions

Investment treaties typically protect covered investments through standards such as fair and equitable treatment, protection against unlawful expropriation and national treatment. The exact wording varies significantly by treaty, so the investor's nationality and the treaty in force at the relevant time must always be established before a claim is assessed. India's treaty practice has also evolved. The 2015 Model BIT reflects an effort to narrow and clarify protections compared with earlier treaty practice (Government of India, 2015). Fair and equitable treatment is potentially the most important standard for regulatory disputes involving data centres. Its content can include protection against arbitrary conduct, serious procedural unfairness and, depending on the treaty and jurisprudence, frustration of legitimate expectations. Yet legitimate expectations should not be treated as a guarantee against every future regulatory change. A sophisticated investor in AI infrastructure should ordinarily anticipate that cybersecurity, data protection, energy and environmental requirements may evolve. Expectations become stronger where the State has made specific, clear and attributable commitments on which the investor reasonably relied. Indirect expropriation presents a different inquiry. A regulation can reduce profitability without amounting to expropriation. Tribunals have generally examined the severity and duration of economic interference, the extent of deprivation, the character of the measure and the circumstances in which the investment was made. In the data-centre context, a prohibition on using a particular cooling technology is analytically different from a rule that makes the entire facility commercially unusable. Similarly, a localisation obligation that increases costs may be less intrusive than a rule that prevents an essential cross-border service from operating.

National treatment requires comparison with appropriate domestic investors or investments. A sustainability standard applied equally to domestic and foreign data centres is less vulnerable than a measure that singles out foreign-owned facilities without a legitimate justification. However, formal equality is not the only issue; the treaty's text and the relevant comparator

analysis remain decisive.¹⁸

4.2 Tension with Regulatory Measures on Data and the Environment

India's investment-arbitration history demonstrates that regulatory measures can produce substantial international disputes. *White Industries v. India* concerned delay and effective access to dispute resolution under the India-Australia BIT and is frequently discussed in relation to fair and equitable treatment and denial of justice. *Vodafone Group Plc v. India* and *Cairn Energy PLC v. India* arose from taxation measures and became prominent examples of the legal and policy consequences of treaty claims. The Devas-related proceedings further demonstrate how foreign investment structures can generate treaty and commercial arbitration proceedings. These disputes are not data-centre cases, but they provide cautionary lessons about treaty exposure and the importance of careful State conduct.¹⁹

The principal lesson for data centres is preventive. India should avoid measures that appear targeted, retroactive, opaque or procedurally unfair. Where new regulation is necessary, a transparent rulemaking process, reasonable transition period and evidence-based justification can strengthen the State's position. This does not mean that regulation must be weak. Rather, regulation should be designed so that its public-interest rationale and proportionality are visible from the administrative record.

5. Digital Sovereignty and Data Localisation

5.1 Justifications for Localisation

Digital sovereignty is particularly relevant to AI because advanced models can process enormous quantities of information and because AI infrastructure may become part of critical economic and governmental systems. Local control may assist law enforcement, cybersecurity, resilience and accountability. It may also reduce dependence on foreign infrastructure and ensure that strategically important data is subject to domestic legal authority.²⁰

Localisation can be justified most strongly where the regulatory risk is specific and demonstrable. Government records, certain critical-infrastructure information and data whose

¹⁸ Government of India, 2015

¹⁹ *White Industries Australia Limited v. Republic of India*, 2011; *Vodafone Group Plc v. Republic of India*, 2025; *Cairn Energy PLC v. Government of India*, 2020; *CC/Devas (Mauritius) Ltd. v. Republic of India*, 2016

²⁰ Government of India, 2023; Ministry of Electronics and Information Technology [MeitY], 2026

compromise could create serious national-security consequences may warrant stronger controls. A risk-based approach is preferable to a universal requirement because not every category of information presents the same risk.²¹

The DPDP Act provides an important basis for regulating cross-border data flows without converting the entire Indian data-centre industry into a closed system. The Act's structure allows the government to regulate transfers through designated mechanisms and recognises lawful processing. This permits a distinction between protecting data and requiring every data-processing activity to occur physically in India.

5.2 Costs and Economic Critiques

Excessive localisation can raise costs for foreign and domestic firms alike. Cloud and AI services often rely on geographically distributed computing, redundancy and disaster recovery. Requiring separate domestic infrastructure for every category of data can reduce utilisation rates and increase capital expenditure. For foreign investors, the added cost may affect the commercial viability of a project and the attractiveness of India relative to alternative locations.²²

Localisation can also create an unusual interaction with environmental policy. If firms are compelled to duplicate storage and compute infrastructure, total electricity and cooling requirements may rise. A policy intended to enhance sovereignty could therefore generate a larger physical infrastructure footprint. Conversely, domestic data-centre clusters may create economies of scale and permit regulators to establish common cybersecurity and sustainability standards. The correct policy is consequently one that links data sensitivity to risk rather than equating sovereignty with physical duplication.²³

6. Environmental Regulatory Autonomy

6.1 Energy and Water Consumption of Data Centres

AI data centres can impose significant demands on electricity systems. High-density computing increases power demand at rack and facility level, while cooling systems add an additional

²¹ Government of India, 2023; Government of India, 2021

²² Organisation for Economic Co-operation and Development [OECD], 2021; World Bank, 2021

²³ OECD, 2021; Government of India, 2023

load. The precise water footprint varies substantially according to climate, cooling technology, humidity, operating temperatures and the source of cooling water. It would therefore be legally and technically unsound to apply a single water-consumption figure to all AI data centres. Indian government responses in 2026 indicate that the industry is adopting direct-to-chip liquid cooling, adiabatic cooling, immersion cooling, closed-loop systems and high-density racks to reduce energy and water consumption (Ministry of Electronics and Information Technology, 2026). This technological variation supports technology-neutral regulation: the law should specify measurable performance outcomes rather than prescribe one cooling technology unless a particular technology is required for a specific risk.²⁴

Environmental regulation should also consider cumulative impacts. A data centre that is environmentally manageable in a region with abundant electricity and recycled water may create serious pressure where the electricity grid is constrained or groundwater is already stressed. Site-specific assessment is therefore more defensible than a uniform national prohibition. It also gives investors clearer information about the conditions that apply before they select a site.²⁵

6.2 Carbon Commitments and Renewable Energy Obligations

India's climate commitments create a policy rationale for increasing energy efficiency and renewable-energy use. Data centres can participate in renewable-energy procurement through mechanisms recognised under electricity regulation, including green-energy open access. Energy-efficiency standards and building codes can also reduce demand. The challenge is to ensure that sustainability requirements are predictable and technologically neutral. A mandatory renewable-energy requirement for data centres could be designed as a performance standard, for example by specifying a percentage of annual electricity consumption to be matched with eligible renewable energy or by recognising verified procurement instruments. Such rules should clarify whether compliance is measured on-site, through contractual procurement, through open access or through other recognised mechanisms. Ambiguity can create both administrative and investment risk.²⁶

The strongest approach is progressive regulation. New facilities can be required to meet higher

²⁴ Ministry of Electronics and Information Technology [MeitY], 2026

²⁵ Ministry of Environment, Forest and Climate Change [MoEFCC], 2026

²⁶ Ministry of Power, 2022; Government of India, 2001; Government of India, 2003

standards from the outset, while existing facilities can receive transition periods. This avoids imposing sudden capital expenditure on sunk investments while still allowing the State to tighten standards as technology improves. The approach also reduces the likelihood that an investor can plausibly claim that a reasonable investment expectation was defeated without warning.

6.3 The Right to Regulate in the Public Interest

International investment law recognises, in different formulations and with treaty-specific variation, that States retain regulatory authority. The police-powers doctrine is particularly relevant to generally applicable measures adopted for public purposes such as health, safety and environmental protection. The existence of a public purpose does not automatically defeat every investment claim, but it can be important in distinguishing ordinary regulation from compensable expropriation.²⁷

Proportionality can provide a useful analytical discipline. A measure should have a rational relationship with its objective; less restrictive alternatives should be considered where appropriate; and the burden imposed should be justified by the public interest pursued. Proportionality should not become a judicial licence to second-guess every technical regulatory choice. In the data-centre context, it is better used as a framework for demonstrating that government considered evidence, alternatives and impacts before adopting a restriction.²⁸

7. Comparative Perspective

7.1 European Union

The European Union offers an example of combining digital governance with energy-efficiency regulation. The Energy Efficiency Directive and related EU measures require increased attention to the energy performance of data centres and promote reporting and efficiency. The EU approach illustrates a regulatory model in which digital infrastructure is treated as part of the energy-transition problem rather than being exempt from it. At the same time, the General Data Protection Regulation (Regulation (EU) 2016/679) regulates personal-data processing through principles of accountability, purpose limitation and lawful processing,

²⁷ Government of India, 2015; United Nations Conference on Trade and Development [UNCTAD], 2012

²⁸ UNCTAD, 2012; Government of India, 2015

while cross-border transfers are governed through specific mechanisms.²⁹

The lesson for India is institutional rather than simply substantive. Digital regulation and environmental regulation can be coordinated through common reporting requirements, measurable standards and risk-based compliance. India need not copy EU rules; it can adapt the principle that large digital infrastructure should internalise measurable resource impacts while preserving legitimate data flows.³⁰

7.2 China

China demonstrates a stronger sovereignty-oriented model. Its Cybersecurity Law, Data Security Law and Personal Information Protection Law establish extensive controls over data, critical information infrastructure and cross-border data transfers. The Data Security Law requires risk monitoring and provides a framework for outbound security management of important data, particularly in relation to critical information infrastructure (People's Republic of China, 2021).

China's model shows how data sovereignty can be integrated into a national-security framework, but it also demonstrates the potential costs of extensive administrative controls. For India, the relevant lesson is that localisation and data-security requirements should be clearly classified and tied to identifiable risks. Broad and uncertain controls may discourage investment more than targeted requirements would.³¹

7.3 Singapore, UAE and Brazil

Singapore provides a particularly relevant comparator because it is both a data-centre hub and a resource-constrained jurisdiction. Its Green Data Centre Roadmap seeks to support additional capacity while improving energy efficiency and the use of green energy. Singapore has also developed a Green Data Centre Standard and a tropical data-centre standard addressing efficient operation in higher-temperature conditions. The Green Data Centre Roadmap initially targeted at least 300 MW of additional capacity in the near term, with further capacity linked

²⁹ European Parliament & Council of the European Union, 2016; European Parliament & Council of the European Union, 2023

³⁰ European Parliament & Council of the European Union, 2016, 2023

³¹ People's Republic of China, 2016, 2021a, 2021b

to green-energy deployment.³²

The Singapore approach suggests that sustainability can be framed as an investment-enabling policy rather than simply as a restriction. Investors receive a clearer pathway to expansion if capacity is connected to measurable efficiency and energy criteria. This is potentially valuable for India because data-centre investors need certainty about whether electricity and water constraints will prevent future expansion.³³

The UAE's 2024 General Framework for Adopting Sustainable Digital Transformation expressly includes green data centres and cloud computing among its sustainability pillars. Although the framework is primarily directed at government digital transformation, it illustrates how digital sustainability can be incorporated into a wider digital-policy agenda (UAE Government, 2026). Brazil provides another useful reference point through its General Data Protection Law (Lei Geral de Proteção de Dados Pessoais), which regulates personal-data processing while operating within a broader digital economy. The Brazilian example reinforces the distinction between data protection and universal physical localisation.³⁴

8. Analysis and Reform Proposals

8.1 Balancing Mechanisms

The principal reform objective should be regulatory coherence. India should develop a dedicated national framework for large-scale data-centre and AI infrastructure that brings together investment facilitation, data governance, energy planning and environmental safeguards. Current regulation is distributed across multiple authorities. Fragmentation can produce inconsistent timelines and uncertainty even where each individual law is defensible.³⁵

First, India should adopt a risk-based classification of data-centre projects. Classification could consider computing capacity, electricity demand, water stress, data sensitivity, critical-sector connectivity and geographic concentration. The classification should trigger predictable requirements rather than discretionary conditions. A high-risk project should face more

³² Infocomm Media Development Authority [IMDA], 2024

³³ IMDA, 2024

³⁴ Presidência da República, 2018; UAE Government, 2024

³⁵ Ministry of Electronics and Information Technology [MeitY], 2026; Ministry of Environment, Forest and Climate Change [MoEFCC], 2026

stringent assessment because of its actual risk profile, not because it is foreign-owned.³⁶

Second, environmental and infrastructure approvals should be integrated through a single project-information architecture. Investors should be able to identify in advance the electricity availability, water restrictions, groundwater rules, land-use requirements and environmental-clearance thresholds applicable to a proposed site. This would reduce the possibility of late-stage regulatory surprises and strengthen India's position if an investor later alleges that its expectations were frustrated.³⁷

Third, sustainability requirements should be performance-based. Instead of prescribing a single cooling system, India could establish maximum water-use intensity, energy-efficiency, heat-rejection and renewable-energy benchmarks, with periodic revision. Facilities exceeding a defined capacity could be required to disclose energy and water performance. The State could then tighten benchmarks prospectively as technologies improve.³⁸

Fourth, investment incentives should be conditional but stable. A state government may legitimately require an investor receiving subsidies or land concessions to meet employment, renewable-energy or local-infrastructure commitments. The conditions should be published before investment and should identify what happens if targets are not met. This approach is preferable to informal promises because it converts expectations into clearly defined legal obligations.³⁹

Fifth, India should develop an investment-dispute prevention mechanism specifically for digital infrastructure. Before a dispute becomes an arbitration, a designated authority could coordinate with the relevant ministry, state government and investor to address misunderstandings concerning regulatory changes. Early consultation cannot remove treaty rights, but it can reduce the probability that ordinary regulatory disagreements become international claims.⁴⁰

8.2 Drafting Recommendations for Future Investment Treaties and Domestic Law

Future Indian investment treaties should expressly preserve the State's right to regulate

³⁶ Government of India, 2023; Ministry of Environment, Forest and Climate Change [MoEFCC], 2026

³⁷ Government of India, 2015; MoEFCC, 2026

³⁸ Government of India, 2001; Ministry of Power, 2022; MoEFCC, 2026

³⁹ Government of India, 2015

⁴⁰ Government of India, 2015

legitimate public interests, including environmental protection, climate policy, cybersecurity, privacy and data governance. Such clauses should be drafted carefully so that they operate as genuine interpretive and substantive safeguards rather than vague political declarations. At the same time, India should avoid excessively broad exceptions that make investor protection practically meaningless. Treaties should clarify that non-discriminatory measures designed and applied to protect public health, environmental quality, cybersecurity and personal-data rights do not constitute indirect expropriation merely because they affect the value or profitability of an investment, subject to the treaty's precise formulation. This would provide tribunals with clearer interpretive guidance while preserving protection against disguised or discriminatory measures.

The FET provision should distinguish protected legitimate expectations from ordinary commercial expectations. An investor should be able to rely on specific written commitments, contractual undertakings and representations made by competent authorities, but general statements of policy should not ordinarily freeze the regulatory system. This distinction would encourage responsible investment planning while preserving governmental capacity to respond to technological developments. Domestic law should likewise require regulatory-impact assessment for major data-centre rules. The assessment should consider economic cost, electricity-system impacts, water availability, emissions, cybersecurity and alternatives. Consultation with investors and affected communities should be institutionalised. Regulatory transparency is not merely an administrative virtue; it is an investment-risk management tool.

India should also establish clear transition rules. Where an existing data centre complies with the law when commissioned but a new sustainability standard is subsequently introduced, the operator should ordinarily receive a reasonable compliance period unless an urgent public-interest risk justifies immediate action. Transition provisions can reduce stranded-asset risk without preventing the State from raising standards. Policy should encourage geographic diversification of data-centre infrastructure. Concentration in a small number of metropolitan clusters can create grid and water stress. Incentives could favour locations with renewable-energy potential, adequate transmission capacity, treated-water availability and lower ecological stress. This would align investment promotion with environmental planning rather than treating environmental constraints as an afterthought.⁴¹

⁴¹ Ministry of Power, 2022; MoEFCC, 2026; IMDA, 2024

9. Limitations of the Study

This study has several limitations. First, AI data-centre regulation is developing rapidly, and policy proposals may change faster than conventional statutory frameworks. The paper therefore distinguishes current legal requirements from emerging policy proposals. Secondly, investment-treaty claims are highly dependent on treaty wording, investor nationality, corporate structure, timing and the factual record. General propositions about FET or expropriation cannot substitute for treaty-specific analysis. Thirdly, data-centre environmental impacts vary significantly according to technology, location and energy source; broad numerical estimates may therefore obscure important differences. Fourthly, state-level policies are diverse and may be amended over time. The examples used here illustrate structural issues rather than providing an exhaustive survey of every Indian state. Finally, the paper is primarily doctrinal and comparative; it does not undertake empirical interviews with investors, regulators or affected communities. Future research could test the proposed framework through project-level case studies and quantitative analysis of energy, water and investment outcomes.

10. Conclusion

AI data centres are becoming strategically important infrastructure for India's digital economy. Their growth offers significant investment and development opportunities, but their scale also makes them different from ordinary digital businesses. They consume electricity, require cooling, occupy land and may process sensitive information. The State therefore cannot reasonably be expected to guarantee a static regulatory environment. At the same time, investors committing substantial capital require transparency, procedural fairness and sufficient predictability to evaluate long-term risk. The central argument of this paper is that investor protection, digital sovereignty and environmental regulatory autonomy can be reconciled through regulatory design. India does not need to choose between attracting foreign investment and protecting public interests. It needs to distinguish legitimate regulation from arbitrary interference and to communicate that distinction through law and policy.

The most defensible regulatory model would be risk-based, technology-neutral and prospective. Data controls should be calibrated to the sensitivity and security risks of particular categories of information rather than equating sovereignty with universal physical localisation. Environmental rules should focus on measurable outcomes in energy efficiency, water use, renewable-energy procurement and emissions while allowing technological flexibility.

Investment incentives should be transparent and conditional, while major regulatory changes should include consultation, impact assessment and reasonable transition periods. Investment treaties should reinforce this balance. Clear public-interest safeguards, carefully drafted exceptions, disciplined FET provisions and protection against discriminatory or arbitrary conduct can reduce uncertainty for both States and investors. India's experience with earlier investment disputes demonstrates the cost of ambiguous treaty commitments and inconsistent governmental conduct. The objective of future treaty drafting should therefore be neither maximal investor protection nor maximal governmental discretion, but predictable regulatory space accompanied by meaningful protection against abuse.

The development of AI infrastructure ultimately makes digital policy inseparable from infrastructure policy. India's competitive advantage will depend not only on the amount of foreign capital it attracts but also on whether that capital can be deployed sustainably and within a stable legal framework. A coordinated approach to data governance, investment protection and environmental regulation can make India an attractive destination for AI data-centre investment while preserving the State's constitutional and policy capacity to protect privacy, security, natural resources and the long-term public interest.

REFERENCES

- Department for Promotion of Industry and Internal Trade. (2025). Foreign direct investment policy. Ministry of Commerce and Industry, Government of India.
- Department for Promotion of Industry and Internal Trade. (2026). Foreign direct investment in India: Annual issue 2025. Ministry of Commerce and Industry, Government of India.
- Government of India. (1999). Foreign Exchange Management Act, 1999.
- Government of India. (2000). Information Technology Act, 2000.
- Government of India. (2001). Energy Conservation Act, 2001.
- Government of India. (2003). Electricity Act, 2003.
- Government of India. (1974). Water (Prevention and Control of Pollution) Act, 1974.
- Government of India. (1986). Environment (Protection) Act, 1986.
- Government of India. (2006). Environmental Impact Assessment Notification, 2006.
- Government of India. (2015). Model text for the Indian Bilateral Investment Treaty.
- Government of India. (2022). Electricity (Promoting Renewable Energy Through Green Energy Open Access) Rules, 2022.
- Government of India. (2023). Digital Personal Data Protection Act, 2023.
- Government of India. (2025). Digital Personal Data Protection Rules, 2025. [Final publication and operative provisions should be checked against the version applicable on the date of submission.]
- Infocomm Media Development Authority. (2023). Sustainability standard for data centres operating in tropical climates.

- Infocomm Media Development Authority. (2024). Green Data Centre Roadmap.
- Infocomm Media Development Authority. (2025). SS 715:2025: Energy efficiency of data centre IT equipment.
- Ministry of Electronics and Information Technology. (2020). Draft Data Centre Policy 2020.
- Ministry of Electronics and Information Technology. (2026). Data centre capacity in the country has increased from about 375 MW in 2020 to around 1500 MW by 2025. Government of India.
- Ministry of Environment, Forest and Climate Change. (2026). Effective use of water in AI data centres: Rajya Sabha response. Government of India.
- People's Republic of China. (2021). Data Security Law of the People's Republic of China.
- United Arab Emirates Government. (2026). The General Framework for Adopting Sustainable Digital Transformation.
- European Union. (2016). Regulation (EU) 2016/679 (General Data Protection Regulation). Official Journal of the European Union.
- European Union. (2023). Directive (EU) 2023/1791 on energy efficiency.
- Uttar Pradesh Electronics Corporation Limited. (2026). Uttar Pradesh Data Centre Policy.
- UNCTAD. (2012). Expropriation: UNCTAD Series on Issues in International Investment Agreements II. United Nations.
- UNCTAD. (2018). Fair and equitable treatment: UNCTAD Series on Issues in International Investment Agreements II. United Nations.
- World Trade Organization. (1994). Agreement on Trade-Related Aspects of Intellectual Property Rights.

- White Industries Australia Limited v. Republic of India, UNCITRAL, Final Award (2011).
- Vodafone Group Plc and Vodafone Consolidated Holdings Limited v. Republic of India, UNCITRAL, India–United Kingdom BIT proceedings.
- Cairn Energy PLC and Cairn UK Holdings Limited v. Republic of India, PCA Case No. 2016-7.
- CC/Devas (Mauritius) Ltd. and Others v. Republic of India, UNCITRAL, India–Mauritius BIT proceedings.