
ARTIFICIAL INTELLIGENCE, FOREIGN INVESTMENT AND TECHNOLOGY SOVEREIGNTY: EMERGING CHALLENGES FOR DEVELOPING COUNTRIES

Ayushi Maggu, Amity Law School, Noida, Amity University

ABSTRACT

Foreign investment can finance artificial intelligence infrastructure and widen access to advanced services, while leaving developing countries dependent on external suppliers for computing, models and technical decisions. This paper examines how investment governance can address that tension without treating technological self-sufficiency as a realistic universal objective. Using a doctrinal and comparative method, it analyses selected trade and intellectual property rules, European regulatory instruments, judicial principles on privacy, India's AI capacity programme and the African Union's continental strategy. The central argument is that technology sovereignty should be assessed through effective regulatory authority, domestic capacity and the practical ability to change suppliers. Investment approval, local data storage and national ownership do not independently establish those conditions. The paper proposes proportionate screening, negotiated capability development, enforceable procurement safeguards and regional cooperation. These measures should connect investment incentives with demonstrable public benefits while protecting individual rights and preserving lawful international collaboration.

Keywords: Artificial Intelligence; Foreign Investment; Technology Sovereignty; Developing Countries; Technology Transfer; Data Governance.

I. Introduction

An investment in an artificial intelligence company can change who controls the infrastructure through which knowledge is produced and public services are delivered. A foreign investor may supply capital, computing resources and access to international markets. The same transaction may give it influence over sensitive datasets, local research priorities or the conditions under which essential software remains available. The legal question is therefore broader than whether capital should enter the country. It concerns the distribution of continuing authority after that capital has been admitted.

Technology sovereignty is a contested concept. Pohle and Thiel examined how claims to digital sovereignty combined different demands concerning state authority, economic autonomy and individual self-determination. Their analysis cautioned against assuming that the phrase describes a settled legal entitlement. For this paper, technology sovereignty means the effective capacity of a developing country to govern consequential technological uses, cultivate relevant domestic expertise and maintain meaningful alternatives to a particular supplier. This working definition permits international cooperation and subjects public control to constitutional limits.¹

Three questions guide the enquiry. How can AI-related foreign investment support development while creating dependency? Which legal rules constrain or support measures intended to preserve domestic technological choice? How should developing countries structure investment conditions and institutions to secure public benefits? The working proposition is that investment supports sovereignty when it expands usable domestic capabilities and preserves enforceable decision-making authority. Local incorporation or server location alone supplies insufficient evidence of that result.

The method is doctrinal and comparative, drawing on verified treaty provisions, judicial materials, academic articles and selected policy instruments available by 14 September 2026. India and the African Union provide contrasting illustrations of national and regional capacity-building approaches; European instruments are comparative references rather than laws binding developing countries generally. The study does not measure investment effects statistically or claim a comprehensive survey of national AI legislation. Its contribution is an

¹ Julia Pohle and Thorsten Thiel, “Digital Sovereignty” 9(4) Internet Policy Review (2020).

integrated legal analysis connecting investment entry with the later operation, oversight and replacement of AI systems.

II. Foreign Investment and the Structure of AI Dependence

AI investment takes several legally distinct forms. A foreign company may establish a data centre, acquire an enterprise, subscribe for a minority shareholding or finance a research partnership. A government may instead purchase access to an overseas model without receiving any direct investment. These arrangements can create similar dependencies but do not necessarily engage the same investment rules. Treating every purchase of a digital service as foreign direct investment would obscure the separate roles of procurement, trade in services and corporate control.

The location of spending also differs from the location of technological authority. Construction and maintenance may occur locally while model development, licensing and important operational decisions remain elsewhere. Conversely, a foreign-owned research facility may employ domestic specialists and support locally relevant innovation. The useful enquiry follows specific rights: who may inspect the system, adapt it, decide permissible uses and continue operating it if commercial relations deteriorate? Those rights should be identified from contracts and technical arrangements rather than inferred from the investor's nationality.

Dependence can become difficult to reverse through ordinary business choices. A start-up accepting discounted computing may design its services around proprietary interfaces. Later migration can require rewriting software, reformatting data and rebuilding staff expertise. The initial discount can be commercially beneficial while increasing future switching costs. This paper therefore treats exit capability as a matter for investment and procurement design. An apparently affordable project may impose substantial future costs if the recipient cannot move its work to another provider on practicable terms.

Critical scholarship also asks who defines the purposes of technological development. Mohamed, Png and Isaac argued that decolonial approaches could expose power imbalances in AI and bring affected communities into technical practice. That perspective supports scrutiny of research agendas and participation, although it does not establish that every foreign-financed project reproduces colonial domination. The relevant question is whether local institutions and communities can influence objectives, contest harmful uses and share in the knowledge

generated.²

The development case for openness remains substantial. International collaboration can make expertise and equipment available sooner than wholly domestic production. Smaller economies may rationally specialise in applications, evaluation or language resources rather than attempt to manufacture every component. The proposed standard is therefore selective capability: retain sufficient expertise and legal access to exercise public choices in important sectors. A policy demanding comprehensive self-sufficiency could consume scarce resources while reducing access to useful technology. That counterargument must remain part of any defensible sovereignty strategy.

III. Trade Investment and Intellectual Property Constraints

Technology conditions must begin with the correct legal instrument. The WTO Agreement on Trade-Related Investment Measures applies to investment measures related to trade in goods. Its prohibition concerns inconsistency with specified GATT obligations, and its illustrative list addresses measures such as certain domestic purchasing requirements. It should not be described as a universal prohibition of every technology-transfer arrangement. Equally, calling a requirement an AI-development incentive does not remove a goods-related local-content condition from scrutiny.³

Services commitments require a separate enquiry. The General Agreement on Trade in Services recognises supply through commercial presence, while market-access and national-treatment obligations depend on the relevant commitments and limitations. Article XIV contains exceptions, including provisions relevant to privacy, subject to its conditions. A government evaluating cloud or AI-service restrictions must therefore identify the service, mode of supply and applicable schedule before reaching a conclusion. A public-interest objective is relevant to the analysis but cannot substitute for it.⁴

Investment agreements may add protection for investors and restrict particular performance requirements. The original 2016 Trans-Pacific Partnership text illustrates how drafting can address minimum treatment, specified technology-transfer requirements and indirect

² Shakir Mohamed, Marie-Therese Png and William Isaac, “Decolonial AI: Decolonial Theory as Sociotechnical Foresight in Artificial Intelligence” 33 *Philosophy & Technology* 659–684 (2020).

³ Agreement on Trade-Related Investment Measures, 1994, arts. 1–4 and annex.

⁴ General Agreement on Trade in Services, 1994, arts. I, XIV, XVI and XVII.

expropriation. That original agreement did not itself enter into force and is used here only as a drafting example. Its provisions cannot be applied automatically to a developing country's investors or measures; the operative treaty, reservations and jurisdictional conditions must be established independently.⁵

This distinction matters for regulatory reform. A proposed audit requirement should be assessed against the obligations actually undertaken, the information sought and the safeguards surrounding access. The possibility of an investor claim neither proves that the requirement is unlawful nor makes treaty review unnecessary. Governments should document the public purpose, evidence and alternatives considered. A well-reasoned measure is easier to defend than an unexplained demand imposed after officials have promised unrestricted operation. Treaty negotiation and domestic regulatory planning should therefore occur together.

TRIPS article 66(2) requires developed-country members to provide incentives promoting technology transfer to least-developed-country members. Its beneficiaries are not all developing countries, and it does not grant every local enterprise a right to a foreign model's source code. Article 67 separately addresses technical and financial cooperation. These provisions offer grounds for seeking structured international support, but their precise addressees and obligations must be preserved when proposing an AI-capacity programme.⁶

Intellectual property is also not a single barrier removable through one licence. Patent rules, protection of undisclosed information and contractual restrictions may concern different elements of an AI system. TRIPS articles 39 and 40 address protected information and anticompetitive licensing practices, while article 31 concerns certain uses of patents without authorisation. A patent-related permission would not by itself supply model weights, training data or practical expertise. Reform should identify the particular right and the technical resource needed before selecting a remedy.^{7,8}

IV Data Governance and Public Accountability

Data localisation is frequently presented as a direct route to technological control. Its effects

⁵ Trans-Pacific Partnership Agreement, signed Feb. 4, 2016, ch. 9, arts. 9.6, 9.10 and annex 9-B (original TPP text, used as a drafting example; not itself an agreement in force).

⁶ Agreement on Trade-Related Aspects of Intellectual Property Rights, 1994, arts. 66(2) and 67.

⁷ Agreement on Trade-Related Aspects of Intellectual Property Rights, 1994, arts. 39–40.

⁸ Agreement on Trade-Related Aspects of Intellectual Property Rights, 1994, arts. 27–31.

depend on what is localised and who retains access. A locally situated server may remain remotely administered under a foreign supplier's contractual conditions. A dataset kept domestically may still be unavailable to public auditors or local researchers. Conversely, a carefully governed international transfer can preserve enforceable protections. Location matters, but an adequate assessment must also examine access permissions, security arrangements, reuse rights and the ability to obtain effective remedies.

These distinctions are especially significant when public bodies supply data for model development. Permission to provide a particular service should not silently become permission to train unrelated commercial systems. Contracts should specify authorised purposes, retention, subcontracting, deletion and the treatment of derived outputs. Those terms require a lawful basis under the relevant domestic regime. Describing information as a national resource cannot extinguish the rights of the people whose activities produced it or cure unlawful collection.

In *Justice K.S. Puttaswamy v. Union of India*, the Supreme Court of India recognised privacy as a fundamental right. The opinion of Chandrachud J. addressed informational privacy and the requirements of legality, legitimate state aim and proportionality for interference. The decision was not about AI investment. Its relevant implication here is that an appeal to national technological development cannot independently justify unlimited state access to personal information. Sovereignty-oriented programmes remain subject to constitutional scrutiny.⁹

The Court of Justice's *Schrems II* decision supplied a different lesson about transfers. It invalidated the EU-US Privacy Shield decision while maintaining the validity of the standard contractual clauses decision subject to the requirements explained by the Court. The assessment extended to the protection available in the destination country. This was an EU data-protection ruling, not a general investment restriction. Its comparative value is that contractual assurances must be considered alongside the legal environment in which performance and redress are expected.¹⁰

UNESCO's 2021 Recommendation connected AI ethics with human rights, accountability, data governance and assessment of impacts. As a recommendation, it does not independently operate as an investment treaty or domestic licensing statute. It nevertheless provides a policy

⁹ *Justice K.S. Puttaswamy (Retd.) v. Union of India*, (2017) 10 SCC 1; opinion of D.Y. Chandrachud J., paras. 180 and 325.

¹⁰ *Data Protection Commissioner v. Facebook Ireland Ltd. and Maximillian Schrems*, Case C-311/18, ECLI:EU:C:2020:559 (July 16, 2020); Court of Justice, Press Release No. 91/20.

basis for requiring governments to examine foreseeable effects before using consequential systems. Developing countries can translate those principles into proportionate domestic procedures, with clear responsibility for evaluation and remedies rather than reliance on a supplier's general statement of ethical commitment.¹¹

A practical accountability arrangement should distinguish the information different audiences need. Affected individuals need intelligible reasons and a route to challenge consequential decisions. Regulators may require confidential technical evidence that would be unsuitable for unrestricted publication. Researchers may need controlled access for independent testing. These functions should be specified separately. Demanding public release of everything may create unnecessary privacy and commercial risks; accepting secrecy for everything may make oversight ineffective. Appropriate access is a question of purpose, authority and safeguards.

V Comparative Regulatory and Development Approaches

The European Union's 2019 foreign-investment screening framework identified critical technologies, including artificial intelligence, and access to sensitive information among factors relevant to security or public order. Its provisions also addressed transparency, confidentiality and recourse against screening decisions. This supplies a useful comparative example of linking review to identifiable risks. It should not be portrayed as a rule requiring developing countries to exclude foreign AI investment or as a comprehensive account of every subsequent European screening development.¹²

The EU AI Act addresses a different regulatory task. Its original 2024 text specifies territorial connections, obligations for high-risk systems and duties concerning general-purpose AI models. Investment clearance and compliance with rules governing an AI product consequently involve different enquiries. The comparative lesson is institutional: permission to acquire or finance a business does not establish that its systems meet applicable operational requirements. This paper uses the cited provisions analytically and does not offer a complete account of the Act's phased implementation or subsequent changes.¹³

India's Cabinet approved the IndiaAI Mission in March 2024 with a budget outlay of Rs.

¹¹ UNESCO, Recommendation on the Ethics of Artificial Intelligence (Nov. 23, 2021).

¹² Regulation (EU) 2019/452, OJ L 79I/1, Mar. 21, 2019, arts. 3–4.

¹³ Regulation (EU) 2024/1689 (Artificial Intelligence Act), arts. 2, 9–15 and 53.

10,371.92 crore. The announcement connected computing access, indigenous models, datasets, skills, application development, start-up finance and trusted AI. These were programme commitments, not proof of completed capacity or measured investment effects. The mission illustrates an approach in which public support seeks to improve domestic participation in an international technological economy.¹⁴

The African Union's Continental Artificial Intelligence Strategy, endorsed in July 2024, promoted an Africa-centred approach and coordination among member states. Its regional orientation is significant for countries that may struggle to negotiate or finance capabilities separately. A continental strategy, however, does not itself establish a common investment licence or harmonise every national obligation. Its implementation requires institutions, financing and national action. Comparing it with India's programme therefore reveals different scales of coordination rather than evidence that either approach has already achieved technological autonomy.¹⁵

Together, these instruments expose three distinct tasks: assessing investment-related risks, regulating the use of systems and supporting technological capacity. Combining all three under an undefined national-security power would make routine decisions unpredictable and overburden a single authority. Completely separating them would risk contradictory conditions. A developing country should allocate responsibility clearly while requiring consultation where an investment affects public-sector deployment, critical infrastructure or access to sensitive information. The coordination process should preserve each authority's legal mandate.

Institutional design should also reflect national differences. A country with established technical universities may prioritise research partnerships and advanced model evaluation. A smaller administration may first need reliable connectivity, shared procurement expertise and access to regional testing facilities. An identical requirement to establish a national frontier-model laboratory could be wasteful in the second setting. Comparative borrowing is most useful when it identifies the function a rule performs and then asks whether local institutions can perform that function credibly.

¹⁴ Press Information Bureau, Government of India, "Cabinet Approves Ambitious IndiaAI Mission to Strengthen the AI Innovation Ecosystem" (Mar. 7, 2024).

¹⁵ African Union, Continental Artificial Intelligence Strategy (2024), endorsed July 18–19, 2024.

VI Emerging Challenges for Developing Countries

The first challenge is identifying control beyond share ownership. A minority investor may obtain contractual influence over infrastructure purchasing, data use or licensing. A non-equity supplier may hold a practical veto through exclusive technical access. Review systems built only around majority acquisitions can therefore miss material dependencies. This does not justify unlimited scrutiny of ordinary contracts. A proportionate trigger should connect the relevant rights with a specified public risk, such as interruption of an essential service or privileged access to sensitive information.

Second, investment incentives can reward expenditure without securing learning. A project may satisfy a capital-spending target through imported equipment while leaving domestic staff unable to maintain or adapt the system. Training attendance is equally weak evidence if participants gain no usable responsibility. Where public support is justified by capability development, its conditions should identify the work domestic participants will be able to perform, the resources available to them and the period over which those capabilities should endure.

Third, public authorities face an information disadvantage when negotiating complex systems. A ministry may understand its service needs but lack expertise to assess model limitations, data-export formats or migration costs. External consultants can help, yet their independence and access to evidence must be secured. Otherwise, the state can become dependent on the same commercial network for supply, evaluation and dispute resolution. Shared technical teams and conflict-of-interest rules may address this problem more effectively than multiplying formal approval stages.

Fourth, concentration can restrict domestic enterprise development. A platform that supplies essential computing while competing in downstream applications may have incentives to favour its own services. That possibility requires evidence before any finding of unlawful conduct. Competition authorities should examine exclusivity, discriminatory access and the effects of acquisitions under their own statutory standards. A sovereignty policy should also scrutinise domestic incumbents; replacing foreign concentration with protected local dominance may leave smaller firms and public purchasers with equally limited choices.

Fifth, imported systems may inadequately reflect local languages, institutions and patterns of

disadvantage. A model that performs acceptably in one setting may require substantial evaluation before use elsewhere. This creates a development opportunity for local research, but only if procurement budgets and contracts recognise that work. Governments should not mistake a globally marketed product for locally demonstrated suitability. The relevant evidence concerns the intended population, actual task and consequences of error, especially where decisions affect access to essential public services.

Sixth, infrastructure projects create resource and continuity questions. Authorities should assess electricity and water requirements, public infrastructure costs and the allocation of disruption risks before granting incentives. A project that depends on an uninterrupted supply of imported equipment also needs a credible maintenance plan. These are project-specific enquiries rather than reasons for categorical exclusion. Their omission can leave public agencies responsible for expensive facilities that they cannot operate sustainably or replace when commercial circumstances change.

Finally, sovereignty can be invoked to weaken scrutiny at home. Preferential treatment for politically connected firms, opaque access to citizens' data and restrictions on independent research may all be described as measures of national control. Such claims require the same evidential and legal discipline as claims made by foreign investors. Technology policy gains public legitimacy when the people affected can obtain reasons and remedies. National ownership is consequently an inadequate substitute for accountable governance.

VII Reform and Investment Design

Consider a hypothetical foreign consortium proposing an AI system for a national agricultural advisory service. It offers investment in local facilities and discounted access to a proprietary model in return for a long service contract and permission to use agricultural records. The investment may expand access to useful advice. Yet if the public authority cannot export the records, verify local-language performance or change suppliers, its future choices may narrow. The example is illustrative and does not describe an observed transaction.

The first reform is a documented assessment before approval or procurement. Officials should identify the project's public purpose, the legal character of each arrangement and the rights transferred to the investor. Where risks justify conditions, those conditions should specify measurable duties and a review mechanism. Routine commercial applications should not face

the same requirements as systems controlling essential public functions. Published criteria and reasoned decisions can protect legitimate investment while limiting arbitrary intervention.

Second, public incentives should purchase identifiable additional benefits. A research grant or infrastructure concession could support supervised training, jointly defined research or independently demonstrated local adaptation where legally permissible. Agreements should distinguish access to a finished service from acquisition of the capacity to modify or evaluate it. Disbursement can be staged against verified milestones, with proportionate recovery for non-performance. Treaty and procurement review should precede the offer, since calling a condition voluntary does not necessarily resolve its legal treatment.

Third, procurement should preserve operational continuity and exit. The agricultural-service contract should define export formats, migration assistance, notice of material changes and the rights needed to retain public records. Authorities should test a transfer before becoming deeply dependent on the supplier. Technical escrow may help in a suitable project, but deposited code is of limited value without licences, documentation and people able to operate it. The chosen safeguard must correspond to a realistic continuity plan.

Fourth, oversight should be enforceable throughout operation. Relevant regulators need access to appropriate records, evaluation evidence and incident information, supported by confidentiality protections. Contracts should identify the entity responsible for compliance and the consequences of unauthorised subcontracting or reuse. Complaint procedures should remain accessible to affected people. A one-time certification cannot settle whether later updates change a system's risks or whether the actual deployment differs from the version initially examined.

Fifth, regional cooperation should make limited resources more effective. Countries could jointly finance evaluation facilities, share procurement expertise and negotiate research access while preserving lawful data protections. Agreements establishing such cooperation should allocate decision-making authority, costs and remedies, including arrangements for smaller participating states. Shared infrastructure will not necessarily produce shared benefits unless access rules prevent the largest contributor or host institution from dominating its use. Regional cooperation therefore needs its own accountability provisions.

Finally, governments should publish evidence of outcomes. Useful indicators include

independent technical responsibilities acquired by local staff, verified access for domestic researchers, the cost of switching providers and compliance with promised public safeguards. These indicators should be assessed alongside investment volume and service performance. The proposed framework is open to evaluation: if a restriction raises costs without improving capability or reducing an identified risk, it should be revised. Sovereignty policy should be judged by the choices it makes practically available.

VIII Conclusion

Artificial intelligence investment can support development while leaving crucial decisions outside the effective reach of domestic institutions. The difficulty arises because financing, ownership, technical competence and legal control do not necessarily move together. The analysis supports a functional understanding of technology sovereignty: a country requires the ability to govern important uses, develop relevant expertise and maintain alternatives. Those capabilities can grow through foreign participation when the terms of participation are carefully designed.

Trade rules and intellectual property protections require precise legal analysis rather than general claims that technology transfer is either prohibited or compulsory. Judicial privacy principles also demonstrate why greater state control must remain accountable to individuals. Comparative initiatives offer useful regulatory and capacity-building functions, but their legal status, implementation and institutional settings differ. Developing countries should connect proportionate screening with enforceable procurement, measurable learning commitments and regional cooperation. The objective is durable technological choice supported by public accountability, rather than autonomy inferred from investment totals or national labels.

References:**A. International Agreements**

- Agreement on Trade-Related Investment Measures, 1994, arts. 1–4 and annex, available at: Source (last visited on Sept. 14, 2026).
- General Agreement on Trade in Services, 1994, arts. I, XIV, XVI and XVII, available at: Source (last visited on Sept. 14, 2026).
- Agreement on Trade-Related Aspects of Intellectual Property Rights, 1994, arts. 66(2) and 67, available at: Source (last visited on Sept. 14, 2026).
- Agreement on Trade-Related Aspects of Intellectual Property Rights, 1994, arts. 39–40, available at: Source (last visited on Sept. 14, 2026).
- Agreement on Trade-Related Aspects of Intellectual Property Rights, 1994, arts. 27–31, available at: Source (last visited on Sept. 14, 2026).
- Trans-Pacific Partnership Agreement, signed Feb. 4, 2016, ch. 9, arts. 9.6, 9.10 and annex 9-B (original TPP text, used as a drafting example; not itself an agreement in force), available at: Source (last visited on Sept. 14, 2026).

B. Regulatory Instruments

- Regulation (EU) 2019/452, OJ L 79I/1, Mar. 21, 2019, arts. 3–4, available at: Source (last visited on Sept. 14, 2026).
- Regulation (EU) 2024/1689 (Artificial Intelligence Act), arts. 2, 9–15 and 53, available at: Source (last visited on Sept. 14, 2026).

C. Cases

- Justice K.S. Puttaswamy (Retd.) v. Union of India, (2017) 10 SCC 1; opinion of D.Y. Chandrachud J., paras. 180 and 325, available at: Source (last visited on Sept. 14, 2026).
- Data Protection Commissioner v. Facebook Ireland Ltd. and Maximillian Schrems,

Case C-311/18, ECLI:EU:C:2020:559 (July 16, 2020); Court of Justice, Press Release No. 91/20, available at: Source (last visited on Sept. 14, 2026).

D Policy Instruments

- UNESCO, Recommendation on the Ethics of Artificial Intelligence (Nov. 23, 2021), available at: Source (last visited on Sept. 14, 2026).
- Press Information Bureau, Government of India, “Cabinet Approves Ambitious IndiaAI Mission to Strengthen the AI Innovation Ecosystem” (Mar. 7, 2024), available at: Source (last visited on Sept. 14, 2026).
- African Union, Continental Artificial Intelligence Strategy (2024), endorsed July 18–19, 2024, available at: Source (last visited on Sept. 14, 2026).

E Academic Articles

- Julia Pohle and Thorsten Thiel, “Digital Sovereignty” 9(4) Internet Policy Review (2020), available at: Source (last visited on Sept. 14, 2026).
- Shakir Mohamed, Marie-Therese Png and William Isaac, “Decolonial AI: Decolonial Theory as Sociotechnical Foresight in Artificial Intelligence” 33 Philosophy & Technology 659–684 (2020), available at: Source (last visited on Sept. 14, 2026).