LEX ET PRAXIS JOURNAL
A Peer-Reviewed Journal of Legal Studies and Practice

Volume 1, Issue 1, (168-187)

Artificial Intelligence as a Geopolitical Legal Actor: Rethinking International Law for the LLM Era

Arditya Prayogi[1], Muhammad Sobri Maulana[2], Dwitia Pratiwi[3]

[1]UIN K.H. Abdurrahman Wahid Pekalongan, Indonesia
[2] Esnawan Space Air Force Hospital Jakarta, Indonesia
Correspondent: arditya.prayogi@uingusdur.ac.id

Received : June 16, 2026
Accepted : June 25, 2026
Published : June 25, 2026

Citation: Prayogi, A., Maulana, M. S., & Pratiwi, D. (2026). Artificial Intelligence as a Geopolitical Legal Actor: Rethinking International Law for the LLM Era. *Lex et Praxis Journal: A Peer-Reviewed Journal of Legal Studies and Practice*, *1*(1), 168-187.

ABSTRACT: The rapid diffusion of large language models (LLMs) has transformed artificial intelligence from a technical tool into a strategic infrastructure capable of shaping state capacity, private power, information environments, and the practical operation of legal norms. This article examines whether, and in what analytical sense, artificial intelligence can be described as a geopolitical legal actor in the LLM era. It does not argue that AI systems possess legal personality. Rather, it proposes that frontier AI systems function as actor-like socio-technical infrastructures because they mediate legal obligations, redistribute bargaining power, influence public reason, and alter the conditions under which states exercise sovereignty, jurisdiction, responsibility, and human-rights duties. Using normative legal research, document analysis, and public empirical indicators from the Stanford AI Index, the European Union, the Council of Europe, the United Nations, UNESCO, OECD, NIST, the G7 Hiroshima Process, and other governance instruments, the article identifies a central gap: existing international law recognizes states and corporations as legal subjects and duty-bearers, but it lacks a coherent framework for AI systems that operate across borders, rely on concentrated compute and data supply chains, and are deployed through globally dominant platforms. The article advances a novelty claim by connecting geopolitical AI concentration, international legal fragmentation, and LLM-mediated governance into one framework. It argues for a layered international legal architecture combining human-rights impact assessment, compute and model transparency, cross-border accountability, remedies for affected persons, and inclusive capacity-building for developing countries.

Keywords: Artificial Intelligence, International Law, Digital Sovereignty, AI Governance, Legal Responsibility

INTRODUCTION

Artificial intelligence is no longer merely a subject of domestic technology regulation. In the LLM era, AI has become a geopolitical infrastructure. The most capable systems are trained on global data resources, deployed through cloud platforms, optimized with advanced chips, embedded into public and private decision-making, and governed by a mixture of corporate policies, voluntary standards, regional laws, and soft-law instruments. This transformation creates a legal puzzle: international law traditionally regulates states, international organizations, corporations through domestic and transnational law, and individuals in specific regimes. It does not yet have a mature vocabulary for frontier AI systems that mediate speech, knowledge, administrative decisions, security risks, and economic competition across borders.

The phrase "AI as a geopolitical legal actor" must therefore be used carefully. This article does not claim that AI systems are legal persons or bearers of rights and duties equivalent to humans, corporations, or states. Instead, it uses "actor" as an analytical concept. LLMs act in the sense that their design, deployment, outputs, and governance rules alter the behavior of institutions, users, markets, and states. They become legally relevant because they create risks, allocate access, influence decisions, and generate harms or benefits that law must attribute to human and institutional duty-bearers.

The empirical context is striking. The 2026 AI Index reports that U.S. private AI investment reached USD 285.9 billion in 2025, compared with USD 12.4 billion in China; the United States also hosted 5,427 AI data centres and produced more top-tier AI models, while China narrowed the performance gap and led in publications, citations, patent output, and industrial robot installations (Stanford Institute for Human-Centered Artificial Intelligence, 2026). The 2025 AI Index similarly reported that in 2024 U.S.-based institutions produced 40 notable AI models, compared with 15 from China and three from Europe (Stanford Institute for Human-Centered Artificial Intelligence, 2025). These figures show that LLM governance is not only about ethics and safety; it is also about the distribution of geopolitical capacity.

At the same time, international AI governance is accelerating. The EU AI Act entered into force in August 2024 and introduced staged obligations for prohibited practices, general-purpose AI models, and high-risk systems (European Commission, 2026). The Council of Europe opened the first legally binding international treaty on AI, human rights, democracy, and the rule of law for signature in September 2024 (Council of Europe, 2024). The United Nations General Assembly adopted Resolution 78/265 on safe, secure, and trustworthy AI for sustainable development (United Nations General Assembly, 2024). The UN High-level Advisory Body on AI proposed a scientific panel, policy dialogue, standards exchange,

capacity development network, global fund, data framework, and UN AI office (United Nations High-level Advisory Body on Artificial Intelligence, 2024). UNESCO and the OECD have also issued global ethical and intergovernmental AI principles (UNESCO, 2022; OECD, 2024a).

Despite this normative activity, a gap remains between AI's transnational operational reality and the legal tools available to regulate it. LLMs are developed through value chains that cross multiple jurisdictions: training data may originate globally; compute may be concentrated in a small number of data centres; model weights and application programming interfaces may be controlled by private firms; deployment may affect users in states that lack bargaining power; and governance may rely on terms of service rather than democratic lawmaking. The resulting legal order is fragmented and often asymmetric.

This article addresses three questions. First, in what sense can LLMs be described as geopolitical legal actors without granting them legal personality? Second, what gaps arise when international law is applied to LLM-mediated power? Third, what legal architecture could reduce regulatory fragmentation while preserving innovation, human rights, and the interests of developing countries?

LITERATURE REVIEW

The literature on artificial intelligence and law has increasingly moved from a narrow concern with domestic technological regulation toward a broader debate on global governance, international legal order, and geopolitical power. AI governance is no longer discussed merely as a question of innovation policy, consumer protection, or technical safety, but also as a matter of institutional design, cross-border accountability, and the distribution of regulatory authority. Tallberg et al. (2023) argue that the global governance of AI requires both empirical and normative inquiry because AI is becoming an emerging regulatory field with implications for institutions, legitimacy, and international cooperation. Similarly, Cihon et al. (2020) show that international AI governance remains fragmented and that the choice between centralised and decentralised governance architectures will significantly affect the effectiveness, inclusiveness, and adaptability of future AI regulation.

Within international law scholarship, AI is increasingly understood as a disruptive force that challenges existing legal categories and attribution mechanisms. Chesterman (2021) explains that AI creates difficulties for international law because its risks may involve questions of responsibility, attribution, prevention, and institutional coordination. Maas (2019) similarly argues that AI may affect not only the substance of international legal rules, but also the development, displacement, or even transformation of the global legal order. These studies are

important because they shift the discussion from whether AI should merely be regulated to how AI reshapes the conditions under which international law operates.

Another relevant body of literature concerns digital sovereignty and infrastructural power. Sovereignty in the AI era is not limited to territorial jurisdiction, but also includes control over data, compute infrastructure, cloud systems, standards, and technological dependencies. Scassa (2023) argues that sovereignty has acquired new meanings in digital governance, particularly because AI technologies challenge traditional ideas of autonomy and control. Srivastava and Bullock (2024) further explain that AI systems increasingly affect global governance by shaping how public and private actors exercise instrumental, structural, and discursive power. This perspective supports the argument that LLMs are not neutral tools, but infrastructures embedded within broader geopolitical relations.

The debate on AI legal personhood also provides an important conceptual foundation for this article. Solum (1992) introduced one of the earliest and most influential legal discussions on whether artificial intelligences could ever be treated as legal persons. More recent scholarship, however, remains cautious. Forrest (2024) argues that legal personhood is a flexible and politically constructed concept, but extending it to AI raises complex ethical and legal questions involving harm, agency, responsibility, and rights. For the purposes of this article, the most defensible position is not to recognize AI as a legal person, but to understand AI as producing actor-like legal effects through the institutions, markets, and state practices in which it is embedded.

Human rights and due process scholarship further strengthens the need for a rights-based approach to LLM governance. AI systems may affect privacy, equality, freedom of expression, access to information, administrative fairness, and legal remedies. Wachter et al. (2017) show that claims about a general “right to explanation” under the GDPR are legally more complex than often assumed, while Wachter et al. (2018) propose counterfactual explanations as a practical method to improve accountability in automated decision-making. These debates are relevant to LLMs because their outputs may influence legal information, public administration, benefits distribution, migration processes, policing, and other rights-sensitive domains. Affected individuals therefore require notice, explanation, human review, and access to remedies when AI-supported decisions affect their legal interests.

The literature on AI regulation also highlights the limits of purely principle-based governance. Veale and Zuiderveen Borgesius (2021) show that the EU AI Act represents a major risk-based regulatory approach, but they also identify concerns regarding enforcement, harmonisation, and the position of affected individuals. This suggests that AI governance

cannot rely only on abstract ethical principles or voluntary standards. It must include enforceable obligations, institutional oversight, documentation duties, audit mechanisms, and accessible complaint procedures. For LLMs, such requirements are especially important because responsibility is distributed across developers, data providers, cloud infrastructure providers, deployers, public authorities, and human decision-makers.

Based on these strands of literature, this article positions LLMs as geopolitical legal infrastructures rather than legal persons. Existing studies have examined AI governance, international law, digital sovereignty, legal personhood, and automated decision-making accountability. However, they have not sufficiently integrated these debates into a single framework that explains how LLMs mediate legal authority, redistribute geopolitical power, and expose the fragmentation of international law. This article therefore contributes by connecting AI governance fragmentation, digital sovereignty, value-chain accountability, human-rights safeguards, and the position of developing countries within one layered international legal framework.

METHODLOGY

This study uses normative legal research supported by document analysis and public empirical indicators. The legal materials include treaties, regulations, soft-law instruments, policy frameworks, and international organization reports. The principal instruments examined are the EU AI Act, the Council of Europe Framework Convention on Artificial Intelligence, UN General Assembly Resolution 78/265, the UNESCO Recommendation on the Ethics of Artificial Intelligence, the OECD AI Principles, the NIST AI Risk Management Framework, the G7 Hiroshima Process Code of Conduct, the Bletchley Declaration, and China's Interim Measures for Generative AI Services.

The empirical component does not attempt to produce original statistical measurements. Instead, it uses publicly available, cited indicators to contextualize legal analysis: AI private investment, model production, AI incidents, data-centre concentration, AI adoption, and governance timelines. These indicators are treated as background evidence that demonstrates why international law must address AI not only as a consumer-protection issue but also as a question of power, jurisdiction, and global distribution.

The analysis proceeds through doctrinal interpretation, comparative governance mapping, and normative synthesis. Doctrinal interpretation is used to examine how existing concepts such as sovereignty, jurisdiction, due diligence, human rights, and accountability apply to AI systems. Comparative mapping identifies differences among risk-based regulation,

human-rights treaty obligations, voluntary standards, and state-control models. Normative synthesis produces a proposed framework for international law in the LLM era.

RESULTS AND DISCUSSION

1. The LLM Era as Geopolitical Infrastructure

LLMs differ from earlier software systems because their power depends on infrastructure that is both technical and geopolitical: advanced semiconductors, cloud computing, energy, data pipelines, human feedback, model evaluation, deployment platforms, and regulatory permissions. Control over any layer can create leverage. Export controls on chips, data-localization laws, cloud procurement rules, copyright litigation, model access policies, and safety-evaluation standards all become tools of international influence.

The concentration of investment and infrastructure is legally significant because it affects who can comply with, shape, or resist regulatory obligations. Where one or two jurisdictions dominate model development and compute, other states may become rule-takers rather than rule-makers. They may import AI services subject to foreign terms of service, foreign safety practices, and foreign data governance rules, even when those systems affect domestic education, administration, policing, courts, media, and elections.

The investment gap is not merely economic. It translates into agenda-setting capacity. Firms and states with the largest model-development ecosystems can define technical benchmarks, safety norms, audit practices, and market expectations. In international law, this creates a power asymmetry comparable to earlier debates on digital sovereignty, data colonialism, platform regulation, and the global digital divide.

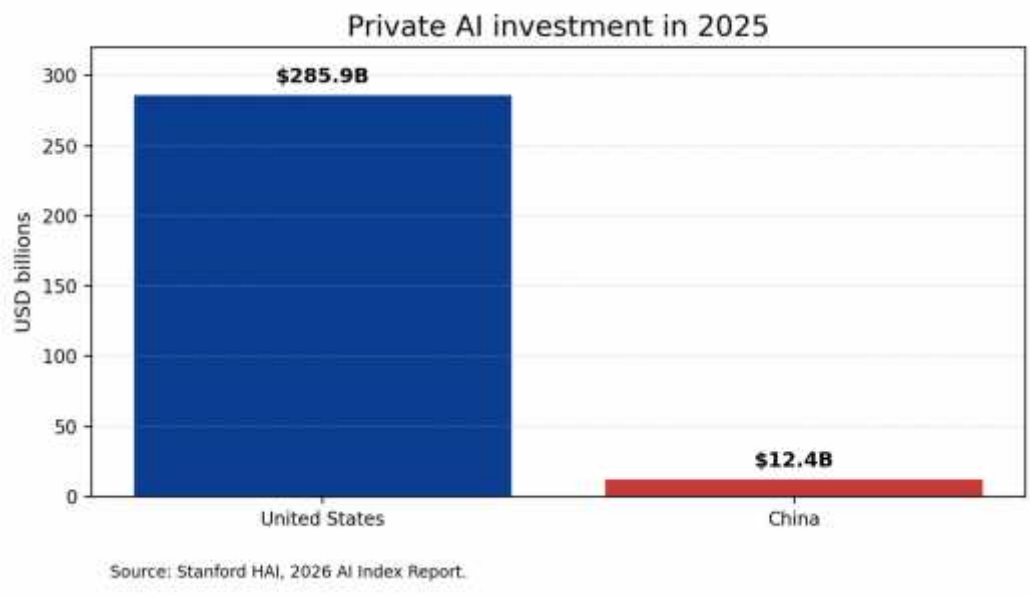

Figure 1. U.S. and China private AI investment in 2025. Data from Stanford HAI 2026 AI Index Report (Stanford Institute for Human-Centered Artificial Intelligence, 2026)

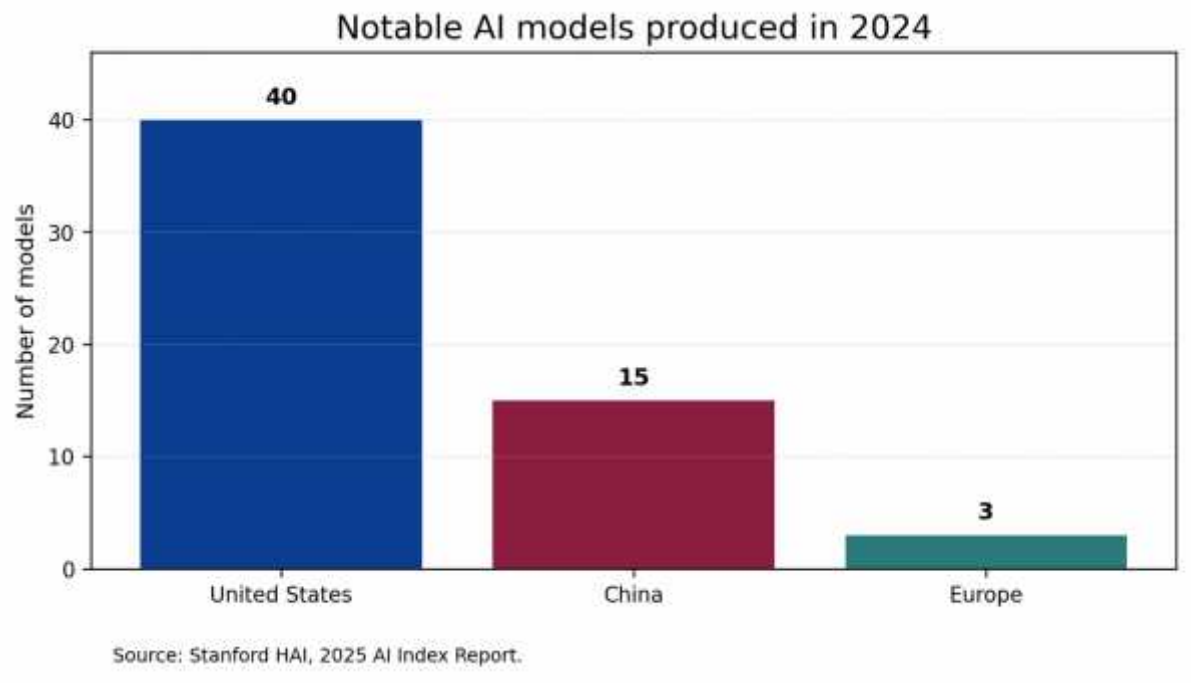

Figure 2. Notable AI model production by geography in 2024. Data from Stanford HAI 2025 AI Index Report (Stanford Institute for Human-Centered Artificial Intelligence, 2025)

Table 2. Selected empirical indicators and legal relevance

Indicator	Reported value	Legal relevance
Private AI investment, 2025	United States: USD 285.9 billion; China: USD 12.4 billion	Shows asymmetry in private capacity to develop, deploy, and influence frontier AI governance.
Notable AI models, 2024	United States: 40; China: 15; Europe: 3	Demonstrates concentration of frontier model production and regulatory leverage.
AI data centres, 2025	United States: 5,427 data centres	Links AI sovereignty to infrastructure, energy, and cloud jurisdiction.
Documented AI incidents	2024: 233; 2025: 362	Supports need for cross-border reporting, remedy, and risk-management duties.
Global organizational AI adoption	88% in 2025 according to AI Index summary	Increases urgency of legal accountability across public and private sectors.

2. From Technical Tool to Actor-Like Legal Infrastructure

The novelty of the LLM era is not that machines become legal subjects. The novelty is that AI systems increasingly operate as infrastructures through which legal relations are

mediated. A government may use an LLM to summarize asylum documents, triage public benefits, translate legal information, generate policy drafts, or monitor security threats. A law firm may use an LLM to produce legal memoranda. A platform may use generative AI to moderate content. In each case, the system is not a legal person, but it becomes part of the chain through which legal authority is exercised.

This creates an attribution problem. When an LLM produces a discriminatory recommendation, hallucinates legal facts, reveals personal data, infringes copyright, or amplifies disinformation, responsibility cannot sensibly be placed on the model as such. Responsibility must be traced across the value chain: model developer, deployer, data provider, cloud infrastructure provider, procuring public authority, and human decision-maker. International law needs a vocabulary for this distributed accountability.

The actor-like quality of LLMs is also discursive. LLMs can produce legal explanations at scale, shape public understanding of rights, influence diplomatic narratives, and generate persuasive content in multiple languages. They may therefore affect not only legal compliance but also the social legitimacy of law. This matters for democratic governance because public reason increasingly passes through privately governed AI interfaces.

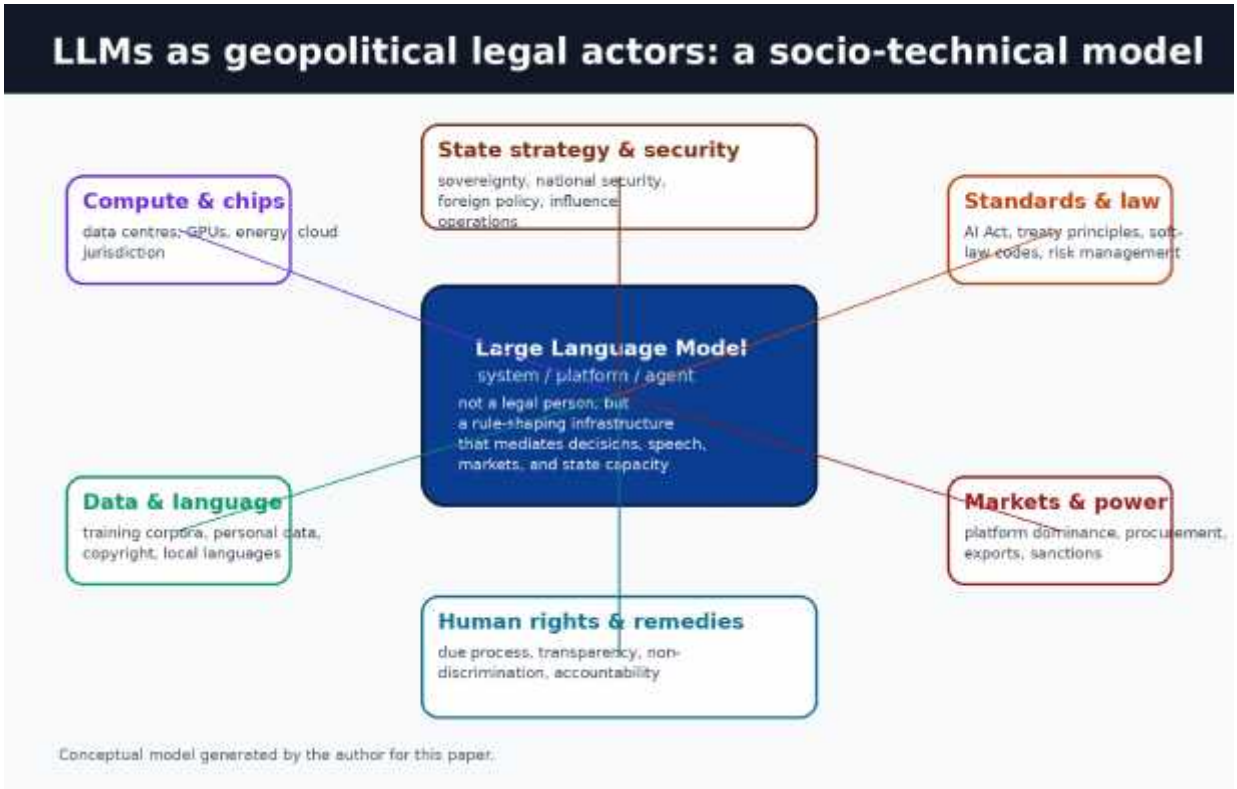

Figure 3. Conceptual model: LLMs as geopolitical legal actors in an analytical, not personhood-based, sense

3. Fragmented International AI Governance

The international governance landscape has developed rapidly but unevenly. The EU AI Act is a binding regional regulation with extraterritorial market effects. The Council of Europe Convention is a treaty organized around human rights, democracy, and the rule of law. The OECD and UNESCO instruments supply global principles, while NIST offers operational risk-management guidance. The G7 Hiroshima Process and Bletchley Declaration rely on voluntary commitments and safety cooperation. China's generative AI measures illustrate a state-security and content-governance model. These instruments overlap but do not yet form a coherent international legal regime.

This fragmentation has three consequences. First, compliance burdens are uneven: firms operating globally must interpret multiple standards, while smaller states may lack capacity to audit imported AI systems. Second, norms may be set by market power rather than democratic participation. Third, affected persons may face uncertainty about remedies when harms arise from cross-border AI systems.

Table 3. Comparative mapping of AI governance instruments

Instrument	Legal character	Core focus	Relevance to LLMs
EU AI Act	Binding EU regulation with staged application	Risk-based regulation, prohibited practices, high-risk systems, GPAI obligations	Creates detailed obligations for general-purpose AI providers and may influence global compliance practices.
Council of Europe Framework Convention on AI	International treaty	Human rights, democracy, rule of law, risk and impact management	Provides rights-based treaty vocabulary for public and private AI activities.
UNGA Resolution 78/265	Non-binding UN resolution	Safe, secure, trustworthy AI for sustainable development	Frames AI governance around SDGs, human rights, and digital inclusion.
UN HLAB Final Report	Expert report to UN system	Scientific panel, policy dialogue, standards exchange,	Offers institutional design options for global AI governance.

Instrument	Legal character	Core focus	Relevance to LLMs
		capacity network, fund, data framework, UN AI office	
UNESCO Recommendation on AI Ethics	Global standard-setting instrument	Human rights, dignity, transparency, fairness, human oversight	Provides ethical and policy basis for rights-respecting AI.
OECD AI Principles	Intergovernmental soft-law standard	Trustworthy AI, human rights, transparency, robustness, accountability	Supports interoperability and policy convergence.
NIST AI RMF 1.0	Voluntary risk-management framework	Govern, map, measure, manage AI risks	Operationalizes risk management for developers and deployers.
G7 Hiroshima Process Code	Voluntary code of conduct	Advanced AI systems, foundation models, risk-based lifecycle actions	Creates safety expectations for frontier model organizations.
Bletchley Declaration	Political declaration	Frontier AI safety and human-centric AI	Signals international consensus on catastrophic and systemic risks.
China Interim Measures	Domestic regulation	Public-facing generative AI, security, public interest, lawful rights	Shows an alternative governance model emphasizing development and security.

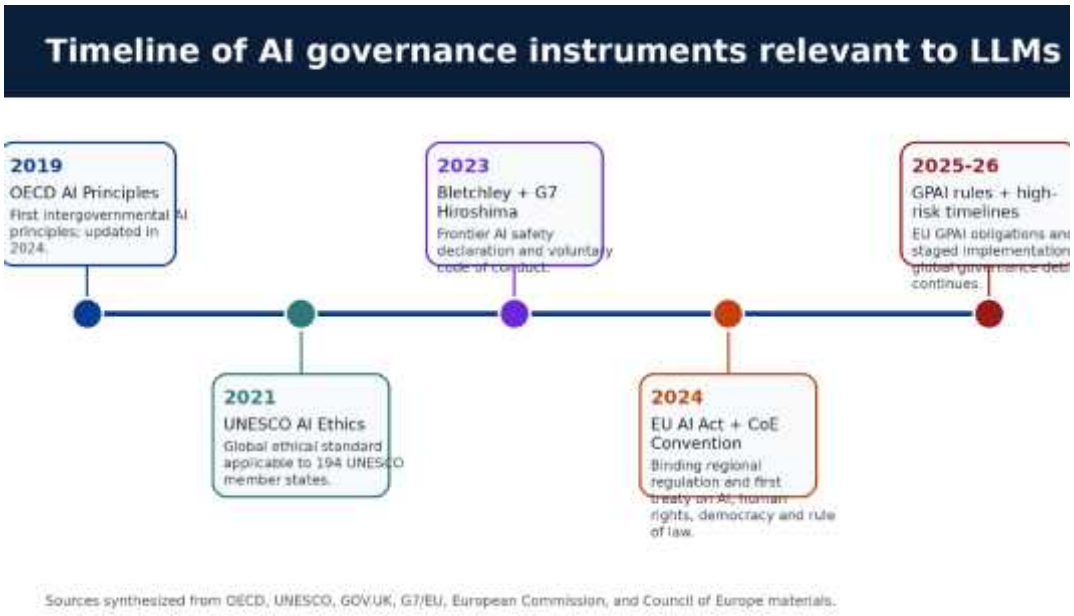

Figure 4. Selected AI governance milestones relevant to the LLM era

Sovereignty, Jurisdiction, and Extraterritoriality

AI governance exposes the limits of territorial sovereignty. A state may regulate AI systems used within its territory, but the model may be trained abroad, hosted on foreign cloud infrastructure, improved through global user feedback, and updated continuously without a discrete local act. Traditional jurisdictional triggers such as territory, nationality, effects, and protective principles remain useful, but they become difficult to apply when harm is produced by distributed model behavior.

Digital sovereignty debates show that sovereignty in AI is no longer simply about territorial control. It also concerns infrastructural control, data governance, language representation, public-sector dependence, procurement capacity, and the ability to audit systems used in critical domains. Scassa (2023) argues that sovereignty has become a broader way of thinking about technology governance and AI, particularly in relation to data and control. Srivastava and Bullock (2024) similarly argue that AI systems are becoming integral to global governance by affecting how global governors exercise power and pursue digital sovereignty.

The EU AI Act demonstrates one approach: regulate access to a large market, thereby creating external compliance incentives. Yet this approach can create “Brussels effects” without global democratic participation. A state outside the EU may benefit from higher safety standards but may not have participated meaningfully in the standards that shape its domestic AI ecosystem. International law should therefore supplement extraterritorial market regulation with inclusive multilateral mechanisms.

4. Human Rights, Democracy, and Due Process

The strongest legal foundation for global AI governance is not technological exceptionalism but human rights. AI systems can interfere with privacy, equality, expression, access to information, labour rights, education, health, political participation, and due process. The Council of Europe Convention explicitly links AI systems to human rights, democracy, and the rule of law; UNESCO similarly places human rights and dignity at the centre of AI ethics (Council of Europe, 2024; UNESCO, 2022).

LLMs create particular due-process risks. Their outputs may be fluent but unreliable; they may mask uncertainty; they may reproduce bias; and they may be difficult to challenge if integrated into administrative or legal workflows. A person affected by an AI-supported decision needs notice, explanation, access to relevant information, human review, and a remedy. The Council of Europe Convention's emphasis on documentation, sufficient information to challenge decisions, complaints, safeguards, and notice that one is interacting with an AI system is therefore especially important (Council of Europe, 2024).

Democratic legitimacy also requires public control over the use of AI in state functions. When governments outsource AI systems to private vendors, they should not outsource accountability. Public procurement should require audit rights, model documentation, evaluation evidence, data-protection safeguards, incident reporting, and termination rights where systems violate rights or democratic principles.

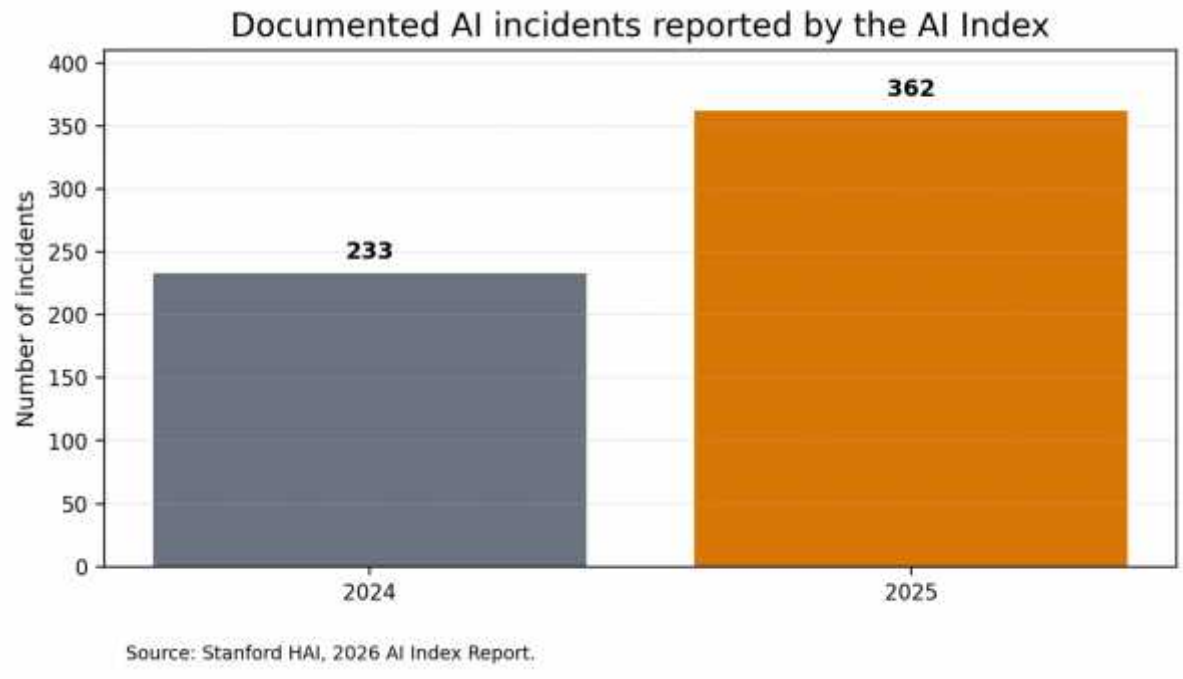

Figure 5. Increase in documented AI incidents. Data from Stanford HAI 2026 AI Index Report (Stanford Institute for Human-Centered Artificial Intelligence, 2026)

5. Responsibility and Accountability Across the AI Value Chain

LLM harms are rarely caused by one actor. A model developer may decide the architecture and training process; a data supplier may provide datasets; a cloud provider may supply compute; an application provider may adapt the model; a government agency may deploy it; and a human official may rely on its output. Existing legal systems often assign liability at the point of deployment, but systemic harms may originate upstream. International law should therefore encourage value-chain accountability rather than a narrow focus on the final user.

The NIST AI RMF is useful because it moves from abstract principles to risk-management functions: governing, mapping, measuring, and managing AI risks (National Institute of Standards and Technology, 2023). The G7 Hiroshima Process similarly encourages organizations developing advanced AI systems to apply lifecycle actions through a risk-based approach (European Commission, 2023). These frameworks are not substitutes for binding law, but they can help translate international human-rights obligations into operational duties.

A layered accountability model should contain at least five obligations: documentation of model purpose and limitations; human-rights and safety impact assessment; independent or regulator-accessible audit for high-risk deployments; incident reporting; and effective remedy. For general-purpose systems, the model provider should not be automatically liable for every downstream misuse, but it should bear duties proportionate to control, foreseeability, and capacity to mitigate systemic risk.

Table 4. Value-chain accountability model for LLM governance

AI value-chain actor	Typical control	Suggested legal duty
Frontier model developer	Training design, model weights, safety evaluation, release strategy	Systemic risk assessment, technical documentation, transparency summaries, red-team testing, incident reporting.
Cloud/compute provider	Infrastructure access, logging, security, regional hosting	Security controls, lawful access policies, resilience, sanctions/export-control compliance, audit cooperation.
Application provider/deployer	User interface, domain adaptation, prompts, integration into workflows	Context-specific impact assessment, user notice, human oversight, monitoring, complaint channels.

AI value-chain actor	Typical control	Suggested legal duty
Public authority	Legal mandate, procurement, reliance on AI output	Democratic authorization, public register, rights-based safeguards, appeal and remedy, non-delegation of accountability.
Auditors/standards bodies	Evaluation protocols and certification practices	Independence, methodological transparency, conflict-of-interest control, public-interest reporting.

6. Security, Military, and National Security Exceptions

AI governance is complicated by the national-security exception. States often resist binding international obligations where AI intersects with defence, intelligence, cybersecurity, and strategic competition. Yet many risks that threaten human rights and democratic institutions arise precisely at the boundary between civilian and security uses: influence operations, automated surveillance, cyber capabilities, synthetic media, and dual-use model capabilities.

The Council of Europe Convention recognizes that national-security activities are not fully treated in the same way as other activities, but it also states that such activities must respect international law and democratic institutions and processes (Council of Europe, 2024). This is a crucial principle. National security cannot become a blanket zone of AI impunity. International law should require minimum safeguards even where states invoke security: legality, necessity, proportionality, oversight, recordkeeping, and remedy where possible.

The Bletchley Declaration's focus on safe, human-centric, trustworthy, and responsible AI shows that even politically diverse states can agree that frontier AI creates global risks requiring cooperation (Government of the United Kingdom, 2025). However, declarations are not enough. Security-sensitive AI requires confidence-building measures, shared evaluations, incident-notification channels, and norms against AI-enabled destabilization of democratic processes.

7. The Global South, Capacity Asymmetry, and Legal Inclusion

The LLM era risks reproducing a global hierarchy in which a few states and firms produce models while many countries become data sources, user markets, or regulatory adopters. The 2025 AI Index reports strong optimism toward AI in several countries, including Indonesia, where 80% of surveyed respondents viewed AI products and services as more beneficial than harmful (Stanford Institute for Human-Centered Artificial Intelligence, 2025).

Optimism, however, should not be confused with capacity. States may welcome AI but lack compute, local-language data, safety-evaluation institutions, or bargaining power over foreign vendors.

International law should therefore address AI capacity not as charity but as legal inclusion. The UNGA resolution and UN advisory process connect AI governance to sustainable development and capacity-building (United Nations General Assembly, 2024; United Nations High-level Advisory Body on Artificial Intelligence, 2024). This is vital because meaningful participation in AI governance requires technical expertise, regulatory institutions, public datasets, local-language evaluation, access to compute, and civil-society oversight.

For developing countries, the most urgent legal tasks are not always frontier-model licensing. They include public-sector procurement rules, data-protection enforcement, AI literacy, local-language safeguards, consumer protection, judicial capacity, election integrity, and cross-border cooperation. A global AI fund, standards exchange, and capacity development network would help reduce dependence on private vendors and foreign regulatory templates.

8. Toward a Layered International Legal Framework for the LLM Era

A single global AI treaty may be politically difficult in the near term, but international law can still evolve through layered governance. The goal should not be to freeze innovation. The goal should be to ensure that AI systems affecting public rights and international order are subject to traceable duties, independent scrutiny, and effective remedies.

The proposed framework has five layers. First, a human-rights baseline should apply to all AI systems that materially affect rights, whether developed by public or private actors. Second, general-purpose and frontier models should be subject to transparency and systemic-risk duties proportionate to capability and deployment scale. Third, high-impact public-sector uses should require democratic authorization, public registers, impact assessment, and appeal mechanisms. Fourth, cross-border AI incidents should be reportable through interoperable channels. Fifth, developing countries should have access to capacity-building, standards participation, and public-interest compute.

The framework is compatible with existing instruments. It draws on the EU AI Act's risk-based approach, the Council of Europe Convention's human-rights orientation, UNESCO and OECD principles, NIST operational risk management, and UN capacity-building proposals. Its added value is to connect those instruments to geopolitical power and infrastructure sovereignty rather than treating AI governance as a purely technical compliance problem.

Table 5. Proposed layered international legal framework for LLM governance

Layer	Legal rule or mechanism	Expected effect
Human-rights baseline	Mandatory assessment of privacy, equality, expression, due process, labour, and remedy impacts	Prevents AI governance from becoming purely technical or market-based.
Frontier/GPAI transparency	Capability reporting, training-content summaries where lawful, safety evaluations, systemic-risk mitigation	Improves accountability for models deployed across sectors and jurisdictions.
Public-sector safeguards	Public register, procurement transparency, human oversight, appeal rights, audit access	Preserves democratic accountability when states use AI.
Cross-border incident reporting	Shared taxonomy, regulator-to-regulator notification, emergency cooperation	Reduces uncertainty when AI harms cross borders.
Inclusive capacity-building	Global fund, standards exchange, public-interest compute, local-language evaluation	Allows developing countries to participate as rule-makers, not only rule-takers.

CONCLUSION

AI should not be recognized as a legal person merely because LLMs can produce human-like text or participate in institutional workflows. A more appropriate approach is to understand LLMs as geopolitical legal infrastructures: systems that mediate rights, markets, security, knowledge, and state capacity while remaining attributable to human and institutional duty-bearers. This framing avoids the conceptual mistake of granting legal personality to AI, while still recognizing that AI systems generate actor-like effects in international relations and law.

The central research gap lies in the mismatch between AI's transnational infrastructure and the fragmented governance tools of international law. Instruments such as the EU AI Act, the Council of Europe Convention, UN resolutions and reports, the UNESCO Recommendation, OECD Principles, NIST AI RMF, the G7 Hiroshima Process, and the Bletchley Declaration show rapid normative development, but they have not yet produced a coherent global accountability regime. Key unresolved issues include distributed

responsibility, cross-border remedies, compute and data concentration, national-security exceptions, and the meaningful participation of developing countries in shaping AI governance.

This article's novelty is its connection of LLM governance with geopolitical legal power. LLMs are not only technological products to be regulated, but infrastructures that shape the conditions of regulation itself. International law must therefore move beyond principle-heavy AI ethics toward enforceable, interoperable, and inclusive duties grounded in human rights, frontier-model transparency, public-sector safeguards, cross-border incident reporting, and capacity-building. The main recommendations call for human-rights impact assessments, shared taxonomies of AI incidents and remedies, auditable documentation and safety evaluations by frontier model providers, human review and appeal in rights-affecting decisions, inclusive multilateral consultation, global support for local-language datasets and public-interest compute, and minimum safeguards for national-security uses of AI based on legality, necessity, proportionality, oversight, and international law.

REFERENCES

Budiman, A., Nasrullah, R., & Prayogi, A. (2026). Metonymy in Slank song lyrics with political and social themes: A cognitive linguistic study. *International Journal of Linguasphere, 2*(1), 61–70.

Cambridge University Press. (2024). The UN General Assembly adopts U.S.-led resolution on safe, secure, and trustworthy artificial intelligence. *American Journal of International Law: Contemporary Practice of the United States*. https://www.cambridge.org/core/journals/american-journal-of-international-law/

Chesterman, S. (2021). Weapons of mass disruption: Artificial intelligence and international law. *Cambridge International Law Journal, 10*(2), 181–203.

Cihon, P., Maas, M. M., & Kemp, L. (2020). Fragmentation and the future: Investigating architectures for international AI governance. *Global Policy, 11*(5), 545–556. https://doi.org/10.1111/1758-5899.12890

Council of Europe. (2024). *The Framework Convention on Artificial Intelligence and human rights, democracy and the rule of law*. https://www.coe.int/en/web/artificial-intelligence/the-framework-convention-on-artificial-intelligence

Cyberspace Administration of China et al. (2023). *Interim Measures for the Management of Generative Artificial Intelligence Services*. English translation available from https://www.chinalawtranslate.com/en/generative-ai-interim/

European Commission. (2023). *Hiroshima Process International Code of Conduct for Advanced AI Systems*. https://digital-strategy.ec.europa.eu/en/library/hiroshima-process-international-code-conduct-advanced-ai-systems

European Commission. (2026). *AI Act: Shaping Europe's digital future*. https://digital-strategy.ec.europa.eu/en/policies/regulatory-framework-ai

European Parliament and Council of the European Union. (2024). Regulation (EU) 2024/1689 laying down harmonised rules on artificial intelligence (Artificial Intelligence Act). *Official Journal of the European Union*.

Forrest, K. B. (2024). The ethics and challenges of legal personhood for AI. *Yale Law Journal Forum, 133*, 1175–1211.

Government of the United Kingdom. (2025). *The Bletchley Declaration by countries attending the AI Safety Summit, 1–2 November 2023*. GOV.UK. https://www.gov.uk/government/publications/ai-safety-summit-2023-the-bletchley-declaration

International Telecommunication Union & Oxford Martin AI Governance Initiative. (2025). *The annual AI governance report 2025: Steering the future of AI*. International Telecommunication Union. https://aiforgood.itu.int/reports_publications/the-annual-ai-governance-report-2025-steering-the-future-of-ai/

Maas, M. M. (2019). International law does not compute: Artificial intelligence and the development, displacement or destruction of the global legal order. *Melbourne Journal of International Law*, *20*(1), 29–57.

Muzaki, M., Soleha, H. A., Minatika, N., Fadilah, M. N., & Prayogi, A. (2026). Harmonization of reason and revelation in the Islamic scientific tradition: A study of the concept of integration of knowledge at UIN KH. Abdurrahman Wahid, Ibn Tofail, and Ibn Rushd. *Aslama: Journal of Islamic Studies, 3*(1), 1–8.

National Institute of Standards and Technology. (2023). *Artificial Intelligence Risk Management Framework (AI RMF 1.0) (NIST AI 100-1)*. U.S. Department of Commerce. https://www.nist.gov/itl/ai-risk-management-framework

National Institute of Standards and Technology. (2024). *Artificial Intelligence Risk Management Framework: Generative Artificial Intelligence Profile (NIST AI 600-1)*. U.S. Department of Commerce. https://nvlpubs.nist.gov/nistpubs/ai/NIST.AI.600-1.pdf

OECD. (2024a). *AI Principles*. https://www.oecd.org/en/topics/sub-issues/ai-principles.html

OECD. (2024b). *OECD updates AI Principles to stay abreast of rapid technological developments*. https://www.oecd.org/en/about/news/press-releases/2024/05/oecd-updates-ai-principles-to-stay-abreast-of-rapid-technological-developments.html

Scassa, T. (2023). Sovereignty and the governance of artificial intelligence. *UCLA Law Review Discourse, 71*, 214–229. https://www.uclalawreview.org/sovereignty-and-the-governance-of-artificial-intelligence/

Solum, L. B. (1992). Legal personhood for artificial intelligences. *North Carolina Law Review, 70*, 1231–1287.

Srivastava, S., & Bullock, J. (2024). *AI, global governance, and digital sovereignty*. arXiv. https://arxiv.org/abs/2410.17481

Stanford Institute for Human-Centered Artificial Intelligence. (2025). *The 2025 AI Index report*. Stanford University. https://hai.stanford.edu/ai-index/2025-ai-index-report

Stanford Institute for Human-Centered Artificial Intelligence. (2026). *The 2026 AI Index report*. Stanford University. https://hai.stanford.edu/ai-index/2026-ai-index-report

Tallberg, J., Erman, E., Furendal, M., Geith, J., Klamberg, M., & Lundgren, M. (2023). The global governance of artificial intelligence: Next steps for empirical and normative research. *International Studies Review, 25*(3), viad040. https://doi.org/10.1093/isr/viad040

UNESCO. (2022). *Recommendation on the ethics of artificial intelligence*. UNESCO. https://www.unesco.org/en/articles/recommendation-ethics-artificial-intelligence

United Nations General Assembly. (2024). *Resolution 78/265: Seizing the opportunities of safe, secure and trustworthy artificial intelligence systems for sustainable development*. https://docs.un.org/en/A/RES/78/265

United Nations High-level Advisory Body on Artificial Intelligence. (2024). *Governing AI for humanity: Final report*. United Nations. https://www.un.org/sites/un2.un.org/files/governing_ai_for_humanity_final_report_en.pdf

Veale, M., & Zuiderveen Borgesius, F. (2021). Demystifying the draft EU Artificial Intelligence Act. *Computer Law Review International, 22*(4), 97–112. https://doi.org/10.9785/cri-2021-220402

Vinuesa, R., Azizpour, H., Leite, I., Balaam, M., Dignum, V., Domisch, S., Felländer, A., Langhans, S. D., Tegmark, M., & Nerini, F. F. (2020). The role of artificial intelligence in achieving the Sustainable Development Goals. *Nature Communications, 11*, 233. https://doi.org/10.1038/s41467-019-14108-y

Wachter, S., Mittelstadt, B., & Floridi, L. (2017). Why a right to explanation of automated decision-making does not exist in the General Data Protection Regulation. *International Data Privacy Law*, *7*(2), 76–99. https://doi.org/10.1093/idpl/ipx005

Wachter, S., Mittelstadt, B., & Russell, C. (2018). Counterfactual explanations without opening the black box: Automated decisions and the GDPR. *Harvard Journal of Law & Technology*, *31*(2), 841–887.