The American Journal of Political Science Law and Criminology
ISSN 2693-0803 Volume 08 - 2026

# Artificial Intelligence and International Law: Legal Implications of AI Development and Global Regulation

Narziev Oybek Elbek Ugli
Faculty of International Law and Comparative Legislation, Tashkent State University of Law, Uzbekistan

Received: 04 Feb 2026 | Received Revised Version: 20 Feb 2026 | Accepted: 06 Mar 2026 | Published: 25 Mar 2026

Volume 08 Issue 03 2026 | Crossref DOI: 10.37547/tajpslc/Volume08Issue03-09

## Abstract

*This paper examines the legal implications of artificial intelligence (AI) development within the framework of public international law. Employing a doctrinal and comparative legal methodology, it surveys the principal international and regional regulatory instruments currently governing AI — including the European Union Artificial Intelligence Act, the OECD Principles on Artificial Intelligence, and UNESCO's Recommendation on the Ethics of Artificial Intelligence — alongside national frameworks in Uzbekistan, the United States, and China. The paper further analyses the unresolved question of AI's legal personhood and liability, using the landmark Fraley v. Facebook (2015) biometric data case as illustrative jurisprudence. Findings indicate that no jurisdiction currently recognises AI as an independent legal subject; liability continues to rest with human developers, operators, and users. The paper concludes that a single binding multilateral instrument is necessary to address jurisdictional fragmentation, protect digital human rights, and anticipate future technological developments.*

Keywords: Artificial intelligence; international law; AI regulation; legal personhood; digital human rights; EU AI Act; data privacy; Uzbekistan.

**© 2026** Narziev Oybek Elbek Ugli. This work is licensed under a Creative Commons Attribution 4.0 International License (CC BY 4.0). The authors retain copyright and allow others to share, adapt, or redistribute the work with proper attribution.

**Cite This Article:** Narziev Oybek Elbek Ugli. (2026). Artificial Intelligence and International Law: Legal Implications of AI Development and Global Regulation. The American Journal of Political Science Law and Criminology, 8(03), 68–72. https://doi.org/10.37547/tajpslc/Volume08Issue03-09

## 1. Introduction

Artificial intelligence (AI) has transitioned from a narrowly specialised computational tool into a pervasive, multi-sector technology capable of reasoning, learning, and autonomous decision-making. Contemporary universal AI systems — whose public deployment accelerated markedly from 2019 onwards — now operate across financial services, healthcare, urban infrastructure, and personal communications. As AI systems gain the capacity to process vast quantities of personal and institutional data, the absence of a coherent global regulatory framework constitutes a growing risk to privacy, security, and fundamental rights.

From the standpoint of public international law, the regulation of AI presents three interconnected challenges: (1) the fragmentation of existing normative instruments across regional and national jurisdictions; (2) the unresolved question of legal liability when AI-generated conduct causes harm; and (3) the inadequacy of established categories of legal personhood to accommodate autonomous technological agents. These challenges are compounded by the borderless character of digital infrastructure, which renders purely national regulatory responses inherently insufficient.

This paper addresses these challenges by surveying the principal international instruments currently in force, analysing comparative national approaches, and examining a significant case of AI-related litigation. It argues that the international community should prioritise the negotiation of a binding multilateral convention on AI governance, drawing on existing regional instruments as a normative foundation.

### 1.1 Research Questions

This paper is guided by three primary research questions:

- What international and regional legal instruments currently govern the development and deployment of AI, and how adequate are they?
- How do major jurisdictions — the European Union, the United States, China, and Uzbekistan — approach the question of legal liability for AI-related harm?
- Is there a legal and policy basis for adopting a binding global instrument on AI regulation?

### 1.2 Scope and Limitations

The analysis is confined to publicly available primary and secondary legal sources published prior to early 2025. The paper does not undertake an empirical survey of AI usage patterns or a technical assessment of specific AI architectures. Questions of intellectual property in AI-generated works, while related, fall outside the scope of this study.

## 2. Methods

This paper employs a doctrinal legal methodology supplemented by comparative analysis. Primary sources — including treaty texts, legislative instruments, regulatory decisions, and judicial rulings — were identified through systematic searches of official governmental and intergovernmental repositories, including the EUR-Lex database, the OECD iLibrary, the United Nations Official Document System, and the legislative portals of the Republic of Uzbekistan.

Secondary sources, including academic commentary, policy reports, and expert statements, were identified through Google Scholar and legal database searches. Sources were selected on the basis of relevance, institutional authority, and recency. Comparative analysis was applied to evaluate the regulatory approaches of the European Union, the United States, China, and Uzbekistan, using the EU AI Act as a benchmark given its status as the most legally comprehensive instrument currently in force.

The Fraley v. Facebook litigation was selected as a case study because it directly implicates AI-driven biometric data processing, involves a binding judicial determination, and has generated substantial academic commentary regarding the intersection of AI and privacy law.

## 3. Results

### 3.1 International and Regional AI Regulatory Instruments

Review of the primary international instruments reveals a landscape characterised by normative ambition but limited binding force. Three instruments merit particular attention.

The European Union's Artificial Intelligence Act (2021) represents the most legally comprehensive instrument in the field. It classifies AI systems into three risk tiers — high-risk, limited-risk, and minimal-risk — and imposes correspondingly graduated obligations. High-risk systems, which include AI used in credit scoring, fraud detection, and algorithmic trading, are subject to mandatory transparency and explainability requirements, compulsory human oversight mechanisms, and financial penalties for non-compliance ranging from €7.5 million to €35 million depending on the gravity of the violation. The Act thus establishes a model of risk-proportionate, ex ante regulation that is absent from any other instrument of comparable scope.

The OECD Principles on Artificial Intelligence (2019) articulate core ethical standards — including safety, respect for human rights, and alignment with human welfare — but are non-binding in character. Similarly, the UNESCO Recommendation on the Ethics of Artificial Intelligence (2021) provides normative guidance on transparency, accountability, and data governance without creating enforceable obligations. The United Nations 2021 Report on AI and Human Rights further identifies privacy and freedom of expression as rights particularly susceptible to AI-related interference, but stops short of proposing treaty-level commitments.

Collectively, these instruments provide a valuable normative foundation; however, their persuasive rather than binding force limits their practical efficacy in deterring harmful AI deployment.

### 3.2 National Regulatory Approaches: A Comparative Overview

Comparative analysis of national frameworks reveals three distinct regulatory orientations.

In the European Union, the AI Act operationalises a precautionary, rights-based approach grounded in fundamental rights law. The rejection by the European Commission in 2020 of the European Parliament's 2017 proposal to recognise certain AI systems as 'electronic persons' confirms that the EU does not currently extend legal personality to AI, while leaving the issue open for future deliberation.

In the United States, regulation remains primarily sector-specific and market-driven, with liability attributed to the developing company or supervising operator. No federal statute currently recognises AI as a legal subject. In China, algorithmic governance rules introduced since 2021 impose strict oversight obligations on AI operators — particularly in relation to high-risk applications — without conferring legal personality on AI systems. Liability is attributed to companies and users.

In Uzbekistan, AI governance has evolved rapidly through three presidential decrees: Decree No. PD-4996 (2021) creating conditions for AI deployment; Decree No. PD-5234 (2021) establishing a special regulatory regime for priority sectors; and Decree No. PD-358 (2024) adopting a national AI development strategy through 2030. The 2024 strategy includes a mandate to develop ethical guidelines and a regulatory legal instrument by December 2025. In cases of AI-related rights violations, liability may currently arise under the Law on Personal Data (2019), Article 46 of the Code of Administrative Responsibility, and Articles 141(1)-(3) of the Criminal Code.

### 3.3 The Question of AI Legal Personhood and Liability

A consistent finding across all jurisdictions examined is the non-recognition of AI as an independent subject of legal liability. AI is universally characterised as an instrument rather than an agent: responsibility rests with the humans who design, deploy, and supervise it. This position is affirmed by Professor Sandra Wachter of the Oxford Internet Institute, who has noted that AI is a tool created and controlled by humans and that responsibility must accordingly rest with humans.

This consensus, while practically convenient, may prove insufficient as AI systems acquire greater autonomy. The threshold question — at what point, if any, autonomous decision-making capacity should attract independent legal consequences — remains unresolved in both scholarship and positive law.

### 3.4 Case Study: Fraley v. Facebook (2015)

The Fraley v. Facebook litigation provides a significant illustration of AI-related liability in practice. Facebook deployed AI-powered facial recognition technology to scan user photographs and identify individuals without their prior consent, in contravention of the Illinois Biometric Information Privacy Act (BIPA) of 2008, which requires explicit and voluntary consent prior to the collection and use of biometric data.

The court found that Facebook had systematically collected and used personal biometric data in violation of BIPA. A settlement of USD 550 million was ordered in 2019, with individual users eligible to receive between USD 1,000 and USD 5,000 per instance of unlawful data collection. This outcome demonstrates that existing privacy and data protection law can generate substantial accountability for AI-driven violations, even in the absence of AI-specific legislation. It also underscores the centrality of meaningful consent as a legal safeguard in AI deployment.

## 4. Discussion

The findings of this paper support three principal conclusions.

First, the current international regulatory framework is normatively fragmented and insufficiently binding. The EU AI Act, while exemplary in its technical sophistication, is a regional instrument of limited geographic reach. OECD and UNESCO instruments provide ethical orientation but lack enforcement mechanisms. This fragmentation is structurally misaligned with the borderless nature of digital infrastructure, which allows AI systems and their data flows to traverse multiple jurisdictions without encountering equivalent legal standards.

Second, the risk-proportionate approach pioneered by the EU AI Act offers a viable template for international standard-setting. Its classification of AI by risk tier, its transparency and human oversight requirements, and its financial penalty regime represent legal innovations that could inform a multilateral convention. As former UN High Commissioner for Human Rights Mary Robinson has observed, artificial intelligence must serve humanity and be constrained by the rule of law and human rights, with clear guarantees to prevent systems from making incorrect decisions that threaten personal privacy and data protection.

Third, the issue of AI legal personhood will require formal international resolution in the near future. The current consensus — that AI is an instrument, not a person — is coherent and defensible for contemporary AI systems, which operate on the basis of human-defined instructions. However, the trajectory of AI development suggests that this consensus will face increasing pressure as systems acquire greater autonomy and generate harm in ways that are difficult to attribute to any specific human decision. International law must develop anticipatory doctrinal frameworks rather than reactive ones.

In this context, the argument advanced by UK Secretary of State Peter Kyle — that a common instrument should be adopted to regulate AI in accordance with democratic principles[3] — carries considerable weight. A binding multilateral convention, building on existing instruments and supplemented by a monitoring and dispute resolution mechanism, would represent the most effective response to the governance challenges identified in this paper.

## 5. Conclusion

This paper has examined the legal implications of AI development within the framework of public international law, with particular attention to the adequacy of existing regulatory instruments, comparative national approaches, and the unresolved question of AI legal personhood.

The primary findings are as follows: existing international instruments are normatively valuable but insufficiently binding; all major jurisdictions continue to treat AI as an instrument rather than a legal subject, with liability attributed to human operators; the EU AI Act constitutes the most legally developed regulatory model currently available; and the Fraley v. Facebook litigation demonstrates that existing data protection law can generate meaningful accountability for AI-related violations under national frameworks.

On the basis of these findings, this paper advances two policy recommendations. First, states should intensify negotiations toward a binding multilateral convention on AI governance, using the EU AI Act and OECD Principles as normative reference points. Second, international legal scholarship and policymaking should proactively develop doctrinal frameworks for AI legal personhood in anticipation of developments in AI autonomy, rather than awaiting a crisis to compel reactive legislation.

AI exists in the digital world, which knows no borders. The legal frameworks that govern it must ultimately reflect the same scope.

## References

1. Code of Administrative Responsibility of the Republic of Uzbekistan, Article 46, paragraphs 1 and 2.
2. Criminal Code of the Republic of Uzbekistan, Article 141, paragraphs 1, 2, and 3.
3. European Commission. (2021). Proposal for a Regulation laying down harmonised rules on Artificial Intelligence (Artificial Intelligence Act). EUR-Lex.
4. Fraley v. Facebook, Inc., No. 11-cv-01726-RS (N.D. Cal. 2015).
5. Kyle, P. (2025, February 11). In the race for AI, Britain needs to protect digital rights and principles.
6. Musk, E. (2018). Interview at South by Southwest.
7. OECD. (2019). Recommendation of the Council on Artificial Intelligence. OECD/LEGAL/0449.
8. Presidential Decree No. PD-4996 (17 February 2021). On Measures to Create Conditions for the Rapid Introduction of Artificial Intelligence Technologies. Republic of Uzbekistan.
9. Presidential Decree No. PD-5234 (26 August 2021). On Measures to Introduce a Special Regime for the Application of Artificial Intelligence Technologies. Republic of Uzbekistan.
10. Presidential Decree No. PD-358 (14 October 2024). On Approving the Strategy for the Development of Artificial Intelligence Technologies until 2030. Republic of Uzbekistan.
11. Robinson, M. (2019). In Artificial Intelligence and Human Rights Forum.
12. UNESCO. (2021). Recommendation on the Ethics of Artificial Intelligence. UNESCO.

**13.** United Nations. (2021). Report on Artificial Intelligence and Human Rights. United Nations.

**14.** Wachter, S. (2024). Limitations and Loopholes in EU AI Act and AI Liability Directives: What This Means for the European Union, the United States and Beyond.