
AI and International Law: Challenges for Future Negotiations

Dr. Purnima Chaudhary
Head of Department
IPEM Law Academy Ghaziabad

Abstract

The swift growth of artificial intelligence (AI) has presented law enforcement and international relations with both never before seen the potential and difficult challenges. AI systems are beginning to impact on essential concepts of international law, like sovereignty of nations, transparency, and the protection of rights for individuals, as they become progressively autonomous and capable to make judgements with little input from humanity. Conventional frameworks are no longer sufficient for dealing with the rapidity, dimension, and intricate nature of AI's international impact because of these intersections, which create an enforceable murky zone. AI has the capacity to ethically aggravate existing inequalities or create entirely novel forms of prejudice, discrimination, and monitoring. Problems with liability arise in the legal context of autonomous machinery that breakdown or cause adverse effects, especially when they are implemented worldwide. Politically, establishing limitations or restrictions is made more challenging by the fact that artificial intelligence technologies frequently has civilian as well as military uses. Inequalities in negotiating power and impact on policy are caused internationally by disparities in artificial intelligence (AI) capabilities between economies, particularly those between high-tech powers and countries with limited resources. This study examines these issues through investigating the present status of international legal proceedings associated with AI, including UN-led initiatives and the framework agreement on AI of the Parliamentary Assembly of Europe. It also looks at how conflicting national interests, ethical distinctions, and confirmation difficulties affect discussions. In the final section, it makes the case for a progressive, flexible governance framework that combines legally binding agreements with flexible norms, guarantees the participation of marginalised governments, and includes strong compliance procedures. Establishing a globally recognised and legally-enforceable AI governance structure that upholds rights, builds assurance, and promotes fair technological advances necessitates a method like this.

Introduction

Virtually every facet of global society is changing rapidly due to artificial intelligence (AI), from governance of society and military planning to medical and revenue generation. AI systems have unparalleled capacity for encouraging innovation; they may enhance worldwide transportation, automating complicated manufacturing procedures, and improve diagnosis and treatment. However, there are also significant risks connected with these same technological advances. There are significant moral and legal issues with the use of AI in applications for warfare, especially when it comes to autonomously firearms. AI poses a threat to economic growth by eliminating jobs, growing inequalities, and strengthening monopoly tactics. Socially, technologies executed in

social media moderation, law enforcement, and monitoring have already shown the ability to diminish conversations about democracy, infringe solitude, and sustain prejudice. Artificial Intelligence (AI) is profoundly reshaping global relations across military, economic, and social spheres. Its transformative potential—ranging from battlefield automation to digital trade optimization—coexists uneasily with severe risks such as autonomous weapons, algorithmic bias, privacy violations, and cross-border regulatory fragmentation. While existing frameworks—like human rights treaties, disarmament conventions, and trade rules—provide partial guidance, they are ill-suited for the rapid pace, opacity, and transnational nature of AI. This paper examines key challenges hampering the negotiation of effective international agreements on AI and offers strategic recommendations to foster coherent and enforceable global governance. This approach represents the extension of a standards, licensing, and liability regime to the global level. We propose that states establish an International AI Organization (IAIO) to certify state jurisdictions (not firms or AI projects) for compliance with international oversight standards. States can give force to these international standards by adopting regulations prohibiting the import of goods whose supply chains embody AI from non-IAIO certified jurisdictions.

Technological Complexity and Legal Specificity

AI evolves at a pace legal systems can't match, and its systems often defy conventional legal definitions. Governments, tech companies, and researchers grapple with opaque "black box" models, whose internal logic resists transparent oversight. Traditional norms—drafted for autonomous weapons or data privacy—face limits in capturing nuanced risks like emergent behavior, algorithmic bias, and complex value-chain liability.

Disparate regulatory architectures further complicate consensus. The European Union's AI Act exemplifies a rights-based risk regime, while countries like the U.S. rely on sectoral oversight, and China on state-driven guidelines. As a result, AI governance lacks clear technical definitions and universal risk taxonomies, making harmonization across jurisdictions challenging.

Cross-Border Jurisdiction and Accountability

AI's transnational nature poses acute jurisdictional dilemmas. Systems trained in one country can deploy malfunctions in another, raising questions such as: whose laws apply? Where should damages be litigated? These questions vex legal practitioners. Without clear jurisdictional rules, victims face uncertainty and states may evade obligations. Disparate levels of commitment across states produce a fragmented landscape where enforcement and standards vary widely.

Accountability is equally complex. As multiple actors—developers, deployers, operators—participate in AI chains, pinpointing responsibility becomes analytically and legally intricate. International law typically predicates liability on identifiable agents, but diffuse corporate-state

hybrids challenge this premise. Recognizing the limits of product liability and state responsibility models is essential for any future treaty.

Military Application: Autonomous Weapons and Security Dilemmas

AI's most pressing challenge lies in its military use. Autonomous weapons—or “killer robots”—can identify and engage targets without human intervention, raising profound human-rights and ethical dilemmas. Since 2014, the Convention on Certain Conventional Weapons (CCW) has attempted to regulate such systems, but progress has stalled. In May 2025, the UN General Assembly convened its first dedicated session on autonomous weapons. Secretary-General Guterres set a 2026 deadline for states to develop binding regulations, yet key nations (U.S., Russia, China, India) still favor national frameworks over global treaties. Civil society voices warn that failure to act could trigger an arms race threatening human rights.

Conclusion

The accelerating development and deployment of artificial intelligence (AI) across borders is outpacing existing international legal structures, challenging foundational principles such as sovereignty, accountability, and the protection of human rights. The increasing autonomy of AI systems, their dual-use nature, and the global asymmetry in technological capabilities contribute to legal ambiguity, ethical risks, and geopolitical tensions. Current international legal efforts—such as those initiated by the UN and the Parliamentary Assembly of Europe—represent important steps, but remain limited by fragmented interests and enforcement difficulties.

To effectively address these challenges, a forward-looking and adaptive global governance framework is essential. This framework must blend binding international legal instruments with flexible, evolving norms; ensure equitable representation of under-resourced and marginalised nations in policymaking; and implement credible enforcement mechanisms. Only through such a comprehensive, inclusive, and enforceable approach can the international community ensure that AI technologies are developed and deployed in ways that respect human dignity, uphold international law, and promote equitable global progress.

REFERENCES

1. Scherer, M. U. (2016). *Regulating Artificial Intelligence Systems: Risks, Challenges, Competencies, and Strategies*. Harvard Journal of Law & Technology.
2. UNIDIR. (2021). *The Relevance of International Law for the Regulation of Lethal Autonomous Weapons Systems*.
3. ICRC. (2019). *Autonomous Weapon Systems: Implications of Increasing Autonomy in the Critical Functions of Weapons*.
4. OHCHR. (2021). *The Right to Privacy in the Digital Age*.

5. Boulanin, V., & Verbruggen, M. (2017). *Mapping the Development of Autonomy in Weapon Systems*. SIPRI.
6. Floridi, L., & Cowls, J. (2019). *A Unified Framework of Five Principles for AI in Society*. Harvard Data Science Review.
7. Wagner, B., & Eßer, J. (2021). *AI Sovereignty in Europe*. Stiftung Neue Verantwortung.
8. United Nations Secretary-General's Roadmap for Digital Cooperation (2020)
9. Council of Europe. (2020). *Recommendation on the Human Rights Impacts of Algorithmic Systems*
10. European Commission. (2021). *Proposal for a Regulation Laying Down Harmonised Rules on Artificial Intelligence (AI Act)*