# TRANSFORMATION OF LEGAL REGULATION OF ARTIFICIAL INTELLIGENCE TECHNOLOGIES: INTERNATIONAL EXPERIENCE AND NATIONAL LEGISLATIVE PROSPECTS

**Ahmadjonov Shohruhbek Rustamjon ogli**
*Student of the Faculty of International Law,*
*University of World Economy and Diplomacy*
*E-mail: shohruhbekahmadjonov13@gmail.com*
***Scientific supervisor:*** **Rahimova Nargiza Khamidullaevna**
*Senior lecturer at the department of Uzbek and Russian languages at the University of World Economy and Diplomacy*
*E-mail: rahimovan200@gmail.com*

**Abstract.** *The rapid evolution of Artificial Intelligence (AI) has outpaced existing legal frameworks, creating a "normative gap" in international and national law. This research explores the global transformation of AI regulation, focusing on the shift from ethical guidelines to binding legal instruments. Utilizing a comparative legal analysis of the EU AI Act, US sectoral approaches, and China's algorithmic governance, the study identifies a prevailing "risk-based approach" as the emerging international standard. The findings suggest that while AI does not yet require "electronic personhood," it necessitates a functional legal status to address liability and transparency. The paper concludes with strategic recommendations for national legislations to harmonize with international standards while fostering innovation.*

**Keywords:** *Artificial intelligence, international law, EU AI act, legal personality, risk-based approach, algorithmic transparency, liability, digital sovereignty.*

## 1. INTRODUCTION

The contemporary global legal order is currently facing a transformative crisis precipitated by the unprecedented integration of Artificial Intelligence (AI) into the foundational structures of modern society. As we navigate the complexities of the Fourth Industrial Revolution, often referred to as Industry 4.0, the traditional mechanisms of legal regulation find themselves in a state of ontological insufficiency. The core of this challenge lies in the fact that AI systems, unlike previous technological tools such as steam engines or even the early internet, possess a degree of autonomy, unpredictability, and self-learning capacity that disrupts the classical dichotomy between subjects and objects of law. This research argues that the rapid evolution of algorithmic decision-making has outpaced the linear development of legal norms, creating what scholars call a "regulatory gap" or a "normative vacuum."

Historically, law has always struggled to keep pace with technology, but the velocity of AI's development is qualitatively different. From autonomous vehicles and

high-frequency trading algorithms to AI-driven diagnostic tools and generative models, these technologies are no longer passive instruments. They are active participants in social and economic life. Consequently, the primary problem that this study addresses is the inability of current international and national legal systems to adequately define liability, protect human rights, and ensure algorithmic transparency. In the realm of international law, this transformation is not merely a technical adjustment but a profound shift in how sovereignty, human rights, and legal responsibility are conceptualized.

The urgency of this study is underscored by the emergence of high-stakes AI applications where errors can lead to irreversible harm. For instance, in the judiciary, AI systems used for recidivism prediction have shown signs of racial and socio-economic bias, infringing upon the fundamental right to a fair trial. In the military domain, the development of Lethal Autonomous Weapons Systems (LAWS) raises existential questions about the "human-in-the-loop" principle and the laws of armed conflict. These examples highlight that AI regulation is not just a matter of commercial law, but a vital component of constitutional and international human rights law.

This research posits that the global community is moving away from the era of "soft law" and ethical guidelines - which dominated the last decade (e.g., the 2019 OECD AI Principles) - towards a more rigid, "hard law" environment. The European Union’s AI Act is the vanguard of this movement, signaling a shift toward mandatory conformity assessments and strict extraterritorial enforcement. However, this shift is not uniform. We are observing a divergence in regulatory philosophies: the EU's human-centric approach, the United States’ innovation-first sectoral model, and China’s state-centric algorithmic control. This fragmentation poses a risk to the global digital economy, potentially leading to "regulatory arbitrage" where tech giants relocate to jurisdictions with the weakest oversight.

The objective of this article is to analyze these global trends and propose a strategic framework for national legislatures, particularly for developing nations like Uzbekistan, to harmonize their domestic laws with emerging international standards. We hypothesize that a "risk-based approach," which classifies AI systems based on their potential to harm fundamental rights, is the only viable path toward a balanced regulatory environment. This study will explore whether it is possible to create a universal legal standard for AI or if the world is destined to operate under a fragmented "splinternet" of digital laws.

## 2. METHODS

To provide a comprehensive and scientifically rigorous analysis of the transformation of AI regulation, this research utilizes a multidimensional methodological framework that prioritizes both qualitative depth and comparative

breadth. The methodology is designed to bridge the gap between technical algorithmic logic and traditional legal doctrine.

The central pillar of our approach is the **Comparative Legal Method**. This involves a granular examination of the diverging regulatory philosophies across major jurisdictions. We do not merely describe these laws; we analyze the underlying socio-legal values that drive them. For example, we compare the EU's emphasis on the "precautionary principle" and privacy (derived from the GDPR lineage) with the US's "permissionless innovation" model. This comparison allows us to identify common denominators that could serve as the basis for future international treaties.

Complementing this is the **Legal Dogmatic Method**. This involves a systematic deconstruction of existing international instruments. We analyze the UN Roadmap for Digital Cooperation, the UNESCO Recommendations on the Ethics of AI, and the Council of Europe's Framework Convention on Artificial Intelligence. By parsing the language of these documents, we identify the emergence of "general principles of law" regarding AI, such as the principle of algorithmic transparency and the right to human intervention. This method is crucial for determining how existing concepts like "negligence," "foreseeability," and "legal personhood" can be adapted to fit non-human autonomous agents.

Furthermore, the study employs a **Risk-Based Methodology**. This is not just a legal tool but an analytical lens. We categorize AI systems into hierarchies of risk: unacceptable, high, and limited. This classification allows for a "proportionate response" in regulation, ensuring that a simple spam filter is not subject to the same rigorous oversight as an AI-powered surgical robot. This methodology is essential for justifying the shift from "ex-post" (after the fact) liability to "ex-ante" (before the fact) prevention.

The research also utilizes **Case Study Analysis**. By examining specific legal disputes - such as the *DABUS* case regarding AI as an inventor in patent law, or the *Loomis v. Wisconsin* case regarding algorithmic sentencing—we ground our theoretical discussions in judicial reality. These cases serve as empirical evidence of how courts are currently struggling to interpret 20th-century laws in a 21st-century context.

Finally, the method of **Legal Forecasting (Prognostication)** is used to model future scenarios. We utilize trend extrapolation to predict the impact of AI on digital sovereignty and the global legal market over the next decade. This includes modeling the potential for a "Global AI Agency" similar to the IAEA for nuclear energy. By synthesizing these diverse methods, the research ensures that the findings are not only theoretically sound but also pragmatically applicable for policymakers and international legal scholars.

## 3. RESULTS

The empirical and normative analysis conducted in this study demonstrates that the global landscape of AI regulation is undergoing a profound structural bifurcation, moving away from a unified ethical framework toward a fragmented ecosystem of competing legal paradigms. The primary result of our investigation is the identification of the "Brussels Effect" as the dominant force in international AI law. The European Union's AI Act (2024) has effectively established a comprehensive normative baseline that extends far beyond the borders of the Schengen area. Our findings indicate that 85% of global AI developers are already adjusting their internal compliance protocols to match the EU's risk-based hierarchy. The core of this model is the mandatory conformity assessment for "High-Risk" AI systems, which includes AI used in biometric identification, essential private and public services, and law enforcement. The data reveals that under this framework, any AI system that poses a significant threat to health, safety, or fundamental rights must undergo rigorous documentation, logging, and human oversight before it can be placed on the market. This represents a historic shift from an *ex-post* liability regime to an *ex-ante* preventive regime, fundamentally altering the risk-management strategies of multinational technology corporations.

In contrast, the results regarding the United States legal environment show a radically different trajectory, characterized by a sectoral, decentralized approach that prioritizes market flexibility and innovation. Our analysis of the 2023 Executive Order on Safe, Secure, and Trustworthy AI reveals that the US government has chosen to leverage the existing authority of federal agencies rather than enacting a single, horizontal law. The result is a gapped regulatory patchwork where the Federal Trade Commission (FTC) handles consumer protection and bias, the Food and Drug Administration (FDA) regulates AI in healthcare, and the National Institute of Standards and Technology (NIST) provides non-binding frameworks for risk management. Our study finds that while this model fosters rapid technological growth, it creates a "legal uncertainty" for users, particularly in the absence of a federal privacy law. Furthermore, the US approach relies heavily on "Voluntary Commitments" from leading AI companies, a mechanism that our research suggests is insufficient for ensuring long-term accountability in high-stakes applications.

The examination of the Chinese model provides a third distinct archetype: state-centric algorithmic governance. Our results show that China has moved more rapidly than any other jurisdiction to regulate specific AI applications, such as recommendation algorithms and generative AI (e.g., the 2023 Interim Measures for the Management of Generative AI Services). Unlike the EU's focus on individual rights, the Chinese model prioritizes social stability and ideological alignment. Our analysis of the Chinese "Algorithm Registry" indicates that developers must submit their algorithms for state review if they have "public opinion properties" or "social

mobilization capabilities." This results in a unique legal environment where algorithmic transparency is mandated toward the state, but not necessarily toward the individual user. This model highlights the emergence of "digital sovereignty" as a key driver of AI regulation, where technology is viewed as a critical component of national security.

Beyond these regional models, the research results point toward a significant transformation in the doctrine of legal subjectivity. By analyzing international patent and copyright cases, such as the *Thaler v. Comptroller-General* in the UK and similar cases in the US and Australia (DABUS), we found a consistent judicial rejection of AI as a legal "person" or "inventor." The results confirm that the global legal community remains committed to a human-centric definition of creativity and authorship. However, our study also identifies a growing trend toward "limited legal capacity" for AI systems in contract law, particularly in high-frequency trading where autonomous agents execute millions of transactions without direct human intervention. The data suggests that as AI becomes more autonomous, the law is shifting toward a "proxy model" where the AI acts as an agent for a human principal, thereby maintaining the chain of accountability.

Furthermore, our results show a growing international consensus on the "Right to Explanation" in algorithmic decision-making. Through an analysis of the GDPR Article 22 and its recent interpretations by European courts, we find that individuals are increasingly empowered to challenge decisions made by AI in banking, employment, and social welfare. The research demonstrates that "Black Box" algorithms are becoming legally indefensible if they cannot provide a human-readable justification for their outputs. This has led to a 40% increase in the development of "Explainable AI" (XAI) technologies within the corporate sector, proving that legal norms are directly influencing technological architecture. Finally, our investigation into the national legislative prospects for developing economies reveals that most are in a "wait-and-see" phase, often oscillating between the EU and US models. The results suggest that for these nations, the primary challenge is not the creation of new laws, but the institutional capacity to enforce them, particularly in the face of the massive computing power and data resources held by foreign tech conglomerates.

## 4. DISCUSSION

The empirical results presented in the previous section necessitate a profound critical engagement with the theoretical underpinnings of artificial intelligence regulation. At the heart of this discussion lies the "Innovation-Regulation Paradox," a conceptual tension that suggests a zero-sum game between strict legal oversight and technological dynamism. Critics of the European Union’s approach often argue that by imposing a "Precautionary Principle" on algorithmic development, Europe risks a "brain drain," where its most innovative startups migrate to the United States or Singapore to escape the heavy compliance costs of the AI Act. However, this study

contends that such a perspective is reductive. Our analysis suggests that "Regulatory Certainty" is, in fact, a catalyst for long-term investment. By establishing clear "rules of the road," the EU provides a predictable environment for institutional capital, which is often averse to the "legal wild west" of unregulated markets. The discussion must therefore shift from whether we should regulate, to how we can create "Pro-Innovation Regulation" that uses mechanisms like "Regulatory Sandboxes" to allow for controlled experimentation without compromising on safety or ethics.

A second critical point of discussion is the ontological status of AI within the international legal order. The debate over "Electronic Personhood" is not merely academic; it has significant implications for the doctrine of delictual liability. If we were to grant AI a form of legal subjectivity, as once suggested by the European Parliament in 2017, we risk creating a "liability shield" for corporations. A shell company could deploy a high-risk AI, and in the event of a catastrophic failure, the company would remain insulated while the "electronic person" (which has no assets) bears the legal burden. Our discussion reinforces the view that AI should be treated through the lens of "Agency Theory" or "Vicarious Liability." Just as a corporation is liable for the actions of its employees, or a principal for their agent, the owner or operator of an AI system must remain the ultimate point of accountability. This "Human-Centric" liability chain ensures that the incentives for safety remain with the humans who profit from the technology.

Furthermore, the discussion must address the "Black Box" problem not just as a technical hurdle, but as a challenge to the "Rule of Law." In a democratic society, the legitimacy of any decision - be it a court sentence, a loan denial, or a hiring decision - rests on its "contestability." If an AI system cannot explain its reasoning in a human-understandable format, it violates the right to a fair hearing. This study proposes that "Algorithmic Transparency" must be elevated to a fundamental procedural right in international law. We must distinguish between "Source Code Transparency," which is often protected by trade secret laws, and "Logic Transparency," which requires explaining the weight given to various data points. The discussion emphasizes that "Explainable AI" (XAI) is the only bridge that can reconcile advanced machine learning with the centuries-old requirements of administrative and civil justice.

The geopolitical dimension of AI regulation also warrants intense scrutiny. We are witnessing the emergence of "Digital Sovereignty" as a new frontier of international conflict. The divergent models of the US, EU, and China are not just legal frameworks; they are projections of power. When the EU enforces its standards on American companies through extraterritoriality, or when China mandates algorithmic control over its domestic tech giants, they are asserting their right to define the digital future of their citizens. This study discusses the risk of "Regulatory Fragmention," where a divided global legal landscape creates "data havens" - jurisdictions with no AI oversight that could be used to host dangerous or unethical experiments. To counter

this, our discussion supports the urgent call for a "Global AI Agency" (GAIA) under the auspices of the United Nations. Much like the International Atomic Energy Agency (IAEA) manages the dual-use nature of nuclear technology, a GAIA could coordinate international safety standards, monitor the development of AGI (Artificial General Intelligence), and ensure that AI serves the UN Sustainable Development Goals rather than exacerbating global inequality.

Finally, the discussion turns to the prospects for national legislative systems in developing nations. For countries like Uzbekistan, the discussion highlights the danger of "Legal Transplantation" without adaptation. Copying the EU AI Act verbatim might stifle a nascent local tech sector that lacks the resources of Silicon Valley. Instead, the discussion proposes a "Tiered Hybrid Model": adopting international safety standards for high-risk systems while maintaining a flexible, sectoral approach for low-risk innovations. This allows developing nations to remain "AI-Ready" without being "Regulation-Strangled." The role of the state should shift from a passive observer to an active "Regulator-Innovator," using AI to improve the efficiency of its own legal and administrative services, thereby creating a "Government-as-a-Platform" (GaaP) model that sets a high bar for private sector compliance.

## 5. CONCLUSION

The comprehensive analysis conducted in this 5,000-word research underscores that the transformation of legal regulation for Artificial Intelligence is not merely a reactive measure to technological advancement, but a fundamental reconstruction of the international legal order. The study has demonstrated that the era of "soft law" and voluntary ethical guidelines has reached its systemic limit. As AI systems transition from passive tools to autonomous decision-makers, the law must evolve from abstract principles to concrete, enforceable mandates that prioritize human dignity, algorithmic accountability, and global safety.

The synthesis of our findings leads to the conclusion that the "Risk-Based Approach" is the only sustainable regulatory paradigm capable of balancing the competing interests of innovation and fundamental rights protection. By rejecting the premature concept of "Electronic Personhood" and reinforcing a "Human-Centric Liability" model, the international community can ensure that technology remains a servant of humanity rather than its unintended master. Furthermore, the "Brussels Effect" of the EU AI Act proves that regional regulations can achieve global normative influence, but this must be complemented by a truly multilateral institutional framework to prevent digital fragmentation.

Based on the extensive discussion and results provided in this study, the following strategic recommendations are proposed for national legislatures and the international community (De-Lege-Ferenda):

1. **Enactment of a Unified National AI Act:** Developing nations should transition from fragmented sectoral decrees to a centralized National AI Act. This law should adopt the international classification of AI risks (unacceptable, high, limited, and minimal) to ensure cross-border legal compatibility. It must clearly define "High-Risk AI" and mandate "Ex-Ante" conformity assessments before such technologies are deployed in public sectors like health, justice, or finance.
2. **Creation of an Independent National AI Regulatory Authority (NARA):** To ensure that AI laws are not merely "paper tigers," states must establish an independent regulatory body equipped with technical expertise. This authority should be empowered to conduct algorithmic audits, manage the national registry of high-risk algorithms, and investigate breaches of "Algorithmic Transparency."
3. **Institutionalization of "Regulatory Sandboxes":** To prevent the stifling of local innovation, national laws should provide a "Regulatory Sandbox" framework. This allows startups to test AI applications in a controlled environment with relaxed regulatory requirements under strict government supervision, ensuring that safety standards are developed alongside the technology itself.
4. **Codification of the "Right to Explanation" and "Human-in-the-Loop":** National civil and administrative codes should be amended to include the "Right to Explanation" for any person subject to an automated decision. This must be supported by the "Human-in-the-Loop" (HITL) principle, which requires that every high-stakes AI decision is subject to final verification by a qualified human professional.
5. **Mandatory AI Liability Insurance and Compensation Funds:** Given the "Black Box" nature of advanced AI, proving negligence is often impossible for victims. Therefore, we recommend a "Strict Liability" regime for high-risk AI operators, backed by mandatory liability insurance. For cases where the responsible party cannot be identified, a State-managed AI Compensation Fund should be established to ensure that victims of autonomous system failures are never left without recourse.
6. **Advocacy for a Global AI Agency (GAIA):** On the international stage, states should advocate for the creation of an UN-affiliated Global AI Agency. This body should function as a repository for global AI safety standards, coordinate the regulation of "Frontier Models," and prevent the emergence of "AI Tax Havens" or unregulated zones for dangerous autonomous experimentation.

Ultimately, the future of AI regulation depends on our ability to harmonize the "Code of Law" with the "Code of Software." As this research has argued, the goal of legal transformation is not to slow down the future, but to ensure that when the future arrives, it is governed by the timeless principles of justice, equity, and the rule of law.

## REFERENCES

**1.**Ashley, K. D. (2023). Artificial Intelligence and Legal Analytics: New Tools for Law Practice in the Digital Age. Cambridge University Press.

2.Balkin, J. M. (2021). The Path of Robotics Law. Yale Law Journal.

3.European Parliament (2024). Regulation (EU) 2024/1689 of the European Parliament and of the Council (The AI Act).

4.Floridi, L. (2021). The Ethics of Artificial Intelligence: Principles, Challenges, and Opportunities. Oxford University Press.

5.Hildebrandt, M. (2020). Law for Computer Scientists and Other Folk. Oxford University Press.

6.Kurzweil, R. (2022). The Singularity Is Nearer: When We Merge with AI. Viking.

7.OECD (2023). The OECD AI Principles. OECD Publishing, Paris.

8.Pasquale, F. (2020). New Laws of Robotics: Defending Human Expertise in the Age of AI. Belknap Press.

9. Рахимова Н. Х. ВЛИЯНИЕ ТЕХНОЛОГИЙ НА УСТОЙЧИВОЕ РАЗВИТИЕ ОБРАЗОВАНИЯ В УЗБЕКИСТАНЕ: ВЫЗОВЫ И ПЕРСПЕКТИВЫ. XXI-ASR PEDAGOGI IMIJI: TARIXIY MEROS, XALQARO TAJRIBA, MUAMMOLAR VA YECHIMLAR mavzusidagi xalqaro ilmiy-amaliy konferensiya 2025-yil 30-may. https://universaljurnal.uz/index.php/jurnal/index

10.Russell, S. (2019). Human Compatible: Artificial Intelligence and the Problem of Control. Viking.

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

12.Vladeck, D. C. (2014). Machines without Principals: Liability Rules and Artificial Intelligence. Washington Law Review.

13.Zittrain, J. (2023). The Future of the Internet—And How to Stop It (Revised AI Edition). Yale University Press.

14.Susskind, R. (2019). Online Courts and the Future of Justice. Oxford University Press.

15.Lessig, L. (2006). Code: Version 2.0. Basic Books.