Dialogue Social Science Review (DSSR)
www.thedssr.com

ISSN Online: 3007-3154
ISSN Print: 3007-3146

DIALOGUE SOCIAL SCIENCE REVIEW

Vol. 3 No. 12 (December) (2025)

Global Efforts to Regulate Artificial intelligence

Abdus Samad Khan
Assistant Professor, Department of Law Abdul Wali Khan University Mardan
Email: abdus@awkum.edu.pk

ABSTRACT
The world is working faster and harder to regulate Artificial Intelligence because it is creating a significant influence on the employment sector, healthcare, and the life of people. The given paper examines the main regulatory frameworks that have been created by the European Union, the United States, the United Kingdom, and China, shaping the way each of the jurisdictions handles such critical issues as bias and data security in its own distinctive style. Using the recent legislation, official reports, and academic analysis, the study determines the new tendencies and the friction points in the regulatory space, which is why the key conclusion is that cross-national collaboration is necessary to develop AI safely and sustainably.

Introduction

The socioeconomic interactions and labor markets are undergoing fundamental change with the artificial intelligence. The use of AI is spread across various industries, such as staffing, self-driving, medical research, and content management, which result in considerable productivity and creativity. Nevertheless, certain dangers are also associated with this rapid development. The systems are also likely to cause errors and reinforcement of the biases that exist in society. Also, the spread of fake content, including deepfakes, is dangerous to the social discourse and information security and needs to be regulated right now.

Methodology

To collect the information to be used in this analysis, the publicly available sources were used such as official government websites, reputable news outlets, and international research organizations. The first study consisted of extensive searches of the latest AI regulatory reports of the European Union, the US Congress, and the Chinese authorities concerned with regulations. This was then subjected to a close examination of primary legal materials including the entire EU AI Act and the recent US Presidential Executive Orders. To carry out the comparative analysis, the most common concepts were identified, such as risk categorization models and the need to have informational transparency. The study is founded on a desk-based evaluation of published sources exclusively and without human interviews and provides an updated view until the end of 2025. All the references are based on the OSCOLA reference style containing the footnotes to indicate the specific source.

Risk-Based AI Act of the European Union

The European Union has taken the forefront in the world by passing the AI Act which was provisionally accepted in December 2023. This legislation coming into full force on 1 August 2024, will have extensive standards akin in effect to the impact of the GDPR on data security, and will likely be in full effect by 2026, at the end of a gradual transition phase. More importantly, the Act uses a risk-based category framework of AI applications. Risk systems are categorically forbidden that could be the threat to the basic

ISSN Online: 3007-3154
ISSN Print: 3007-3146

rights, such as the general social scoring of the citizens by the government, or other manipulative methods at the expense of the minority. Application of real-time remote biometric identification of people in public spaces is also heavily prohibited, except under certain, strictly controlled exceptions.

Then there is the high-risk category that is allowed but with strict compliance requirements. Such systems that include systems with serious considerations on core life outcomes are covered by this category including employment screening systems, educational admittance systems, credit assessment systems, medical devices systems, and law enforcement systems. The developers of such systems are required to have strong risk management systems, one of them being the provision of quality training data, good record keeping, transparent openness to the users and provision of human check systems to ensure that all undiscriminatory results are reduced. Not all types of systems such as automated loan or hiring systems will meet such requirements, and they have to successfully complete a conformity assessment to be registered in an EU database and be deployed.

The characteristic aspect of the approach provided by the EU is the focus on key rights and secure deployment. Policymakers present a scenario in which AI would promote welfare of society and provide strict protection to the values of privacy, non-discrimination, and transparency. By instituting one, unified regulation among the member states, regulatory fragmentation becomes impossible, and EU can become a world pioneer in supporting trustful AI construction, which has already brought the international legislative deliberations.

The changing Patchwork Approach of the United States.

The US regulatory environment is the opposite of the harmonized European framework: in itself, the regulatory framework is a patchwork of executive interpretation, regulatory oversight, and variant state legislation. Though a detailed federal law is taking ages to be introduced, the current regulatory frameworks and state efforts have already started taking care of urgent issues. The keystone of the federal plan is the Executive Order 14110 of October 2023 by President Biden, a wide sweeping order, which gives various agencies various responsibilities.

These roles are divided into the following main themes: (1) Safety and Security, is aimed at setting standards to gain access to AI systems to risks to national security, cybersecurity, and critical infrastructure. (2) Innovation and Competition that also covers global talent attraction, financing of research, understanding of intellectual property rights as well as provision of income to small businesses. (3) Labor Protection, which deals with exploring the role of AI in job displacement and encouraging the process of workforce training. (4) Civil Rights and Equity, requiring that action be taken to avoid bias in services and the legal system that recognizes the AI tendency to widen inequities in the system. Other avenues consist of Consumer Protection and using the available laws to act against false statements and Data Privacy whereby structures are established to reduce the data risk. Moreover, the E.O. establishes principles of clear and risk-oriented Government use of AI, and promotes the idea of international leadership by providing the international collaboration process.

More importantly, the Executive Order is not statutory but simply guidelines. As a result, in the agencies such as the National Institute of Standards and Technology (NIST) and the Federal Trade Commission (FTC) are already putting its provisions into action. The Order endorses the NIST, which is the focus of technical standards development due to its 2023 Risk Management Framework. At the same time, FTC claims that the current

ISSN Online: 3007-3154
ISSN Print: 3007-3146

consumer protection regulations forbid misleading AI messages. Meanwhile, the Congress is very active but seriously divided around broad legislation, arguing about the necessity to introduce obligatory licensing, evaluate the impacts, and establish a new regulatory agency. Dangers of fake AI-created political content and child protection are the most common issues brought up during hearings, and several pending bills require transparency labels on deepfakes, especially during elections.

Pro-Innovation Stance and Global Safety Agenda of the United Kingdom

The United Kingdom has made itself an AI innovator, with a pro-innovation, and deliberately relaxed approach to regulation, inclined towards guidance rather than strict laws. This strategy was described in a March 2023 White Paper, which proposed taking advantage of existing sectoral regulators (e.g., in finance, healthcare, and transport), on the basis of five main principles, safety, transparency, fairness, accountability and contestability. The first move to avoid the issue of an AI regulator or a prescriptive law was based on the fact that the regulation could be too strict and harming to the emerging AI industry. As late as 2023, however, the government adopted a government advisory group recommending the use of primary legislation due to a belief that voluntary advice was inadequate. The government despite this internal pressure has continued to be conservative and focus on the need to have conclusive evidence before binding regulations are imposed.

At the same time, the UK has attempted to take a proactive position in global debates on the topic of AI safety, especially hosting the first AI Safety Summit Bletchley Park in November 2023. In this meet more than 150 government, academic and industrial representatives were present to discuss existential risks frontier (advanced) AI. The subsequent declaration, which involved the key forces like the US and China, created consensus on the necessity to conduct joint research on the systemic risks and hazard-based policy-making approach Results of the summit were: a UK AI Safety Institute to test models and failures was established; they work closely with the US on similar tests; they invest heavily into computing power and safety science; and they plan to partner with developing countries to provide fair access to useful AI.

The Fair but Tight Regulatory Environment in China

The regulatory environment of AI can be defined as a state regulation that rapidly implements AI and is marked by a strong state control, which is also a part of the larger approach that China uses to preserve technology control and social stability. Several years of direct and indirect rules have been proposed leading to the present Generative AI Regulations that became effective in August 2023. Such regulations narrowly apply to providers of publicly accessible content where models are to be registered and ideological scrutiny is to take place. Importantly, the productions will have to meet the current legislation and the ideals of socialism, explicitly banning the creation of unlawful or untrue materials. Lack of compliance may lead to an instant corrective action or harsh administrative punishment.

Additionally, there are rules labeled to be put in place in September 2025 to make AI-generated content identifiable (e.g. watermarking or metadata) to prevent misinformation and augment traceability. Data security and transparency technical standards are also being formalised continuously in 2025, usually with a compulsory compliance standard. These rules entrench in national security and social ordering objectives to curtail transmission of subversive information and fraud and further encourage shared moral principles to be seen rather than individualistic expression.

Dialogue Social Science Review (DSSR)
www.thedssr.com

ISSN Online: 3007-3154
ISSN Print: 3007-3146

DIALOGUE SOCIAL SCIENCE REVIEW

Vol. 3 No. 12 (December) (2025)

Other Global Operations and Comparative Expectation

In addition to the larger blocs, many other country-specific AI governance models are being created by various other countries and international organizations. Multilateral endeavors, e.g. the G7 Principles and OECD AI Principles, provide overall objectives of a high level but are not legally binding. The proposed AI and Data Act (AIDA) of 2022 by Canada, which is still open to discussion in 2025, follows the risk-based approach to the EU very well, as it aims at influencing the high impact systems and establishing a specialized control authority. Japan, in its turn, initially preferred a more relaxed and human-centric guidance plan relying on self-regulation and making use of already existing laws, but as of 2024, they are moving to the more tangible standards, such as the laws on the identification of deepfakes.

This is due to the fragmented global regulatory environment and complexities that are displayed by the data protection laws, the multinational corporations face a considerable compliance challenge. However, world statements show that there is an intersection in priorities of such principles as human agency and ethical deployment. The prevalent combination of prescriptivism (EU), sector regulation (US), and state regulation (China) is a real-time experiment on the world. There are efforts in collaboration to spread best practice and set minimal prohibitions on practices such as social scoring or even deceptive deepfakes, despite countries competing to happen to set a leadership approach in governance practice.

Critical Problems with the Regulation of AI

The domain of regulation of AI in itself is quite a challenge to define. The technology scale is a complex machine learning model to basic algorithmic tools. The EU has followed a wide definition whereas other individuals lean towards case-by-case. Weakly specified rules may either fail to identify mischievous applications, or punish innocent systems accidentally. Majority of jurisdictions waive the low-risk applications, yet the boundary line, such as between a chatbot used on recersion or as a medical diagnostic tool, is always ambiguous. To add to this is the inherent incompatibility.

between the fast pace of technology rate and the slow legislature. A new law might be enforced when completely new technologies have already come into existence. It must then require the construction of review language and elasticity in regulatory structures and that the regulatory officials working be skilled in a manner that is able to face the talent of the industry at large.

The dilemma is always whether to encourage innovation or required protection. Excessive regulation will impact poorly on small companies and make countries impotent in the international market, whereas a weak regulation threatens the rights and privacy of personal information. This is evident in the fact that the US favors innovation whereas the EU is more precautionary. One of the key areas of contention is liability: who is to be held accountable in case an AI system is harmful? They are also hard to comply and enforce due to the lack of transparency of AI systems where it is complicated to inspect and verify. Also, the multinational character of the AI services makes jurisdictional reach more difficult, as the possible extraterritorial impact of the EU Act illustrates. This requires more global coordination and sharing of information among the supervisory organs.

The Jurisdictional Enforcement Riddle

One of the biggest challenges to a consistent global strategy of AI regulation is jurisdictional friction. Because the modern AI systems are typically run on cloud

ISSN Online: 3007-3154
ISSN Print: 3007-3146

computing, the application trained in one country can instantly affect the discourse of people in different countries, their employment opportunities, or surveillance of other areas. This leads to regulatory distortion: the operating company faces a different set of rules, and the affected citizens follow another set of rules, and thus erosion of the effectiveness of local regulations. As a leader, the European Union has been proactive in trying to overcome this with the assertion of the extraterritoriality of the AI Act that would stipulate compliance of any entity that may be offering its service to EU citizens. Despite other jurisdictions following in their footsteps, the impulse poses a complicated and gunky compliance obligation on business, where conflicting demands, disparate risk rankings, and even punishment are the defining feature. As a result, multinational companies have to make challenging strategic decisions to either invest massively to comply with all requirements, displace certain products in highly regulated economies or to move central operations to less regulated locations. The actual systemic risk is with the malicious actors and non competitive actors who knowingly take the advantage of such jurisdictional blind spots by basing their data, systems, of governance decisions on jurisdictions with lax regulation. Regulators cannot gain authority and find required evidence despite other people having to bear the consequences. Even if at any given time purely domestic systems of government might work, they will inevitably soon be torn apart, for with all the best of standards that a given nation can have, any geographic border is impossible to reach. A lasting solution, consequently, is based on a multi pillar approach to international commitment; (1) The creation of common prohibitive norms covering the most risky AI practices, that the most egregious deeds become universal. (2) Coming to a consensus on some fundamental principles of reciprocity, in which compliance with one strict framework is accepted to satisfy the minimum protection stringencies of a second one. (3) Adopting realistic systems of global liaison against illegal acts, like joint.

investigation teams, standard reporting channels, mutual recognition of penalties, speeding up the delivery of information across the borders. In the absence of these global coordination mechanisms, AI governance will continue to be limited just in one country, but its impacts will be experienced globally and this will be senseless to both the regulators and the people.

Conclusion

Artificial intelligence is a massive disruptive innovation that is forcing every world leader to move swiftly in regulating systems to control the impacts of AIs on society. The EU AI act is a risk-based, bold and comprehensive strategy whereas the US is applying a decentralized system of state laws and federal directions, which is faster to adapt. The United Kingdom has a pro-innovative, deliberative approach and has been seeking to lead the way in global safety, whereas China has a fast-tracked paradigm based on state-controlling and social-stabilizing policies. The lack of universal standard underscores conflicting philosophical ways of attaining a balance between innovation and the protection. However, there have been certain recurrent issues, among them the requirement of transparency in its operations, reduction of possible harms and preservation of public confidence, which have resulted in common steps, like compulsory labelling of synthetic materials and bans on the highly intrusive applications. In the future, long-term international collaboration and flexibility of regulation will be required. As the AI progresses exponentially, the policymakers need to be on their guard, willing to reform regulations, cross-border experiences, and borderline encouraging self-governed ethical standards in the business sector.

ISSN Online: 3007-3154
ISSN Print: 3007-3146

Vol. 3 No. 12 (December) (2025)

Reference

European Commission, 'AI Act Enters into Force' (News Article, 1 August 2024) <https://digital-strategy.ec.europa.eu/en/news/ai-act-enters-force> accessed 6 December 2025.

European Commission, 'AI Act: Risk Framework and Provisions' (News Article Details) <https://digital-strategy.ec.europa.eu/en/policies/european-approach-artificial-intelligence> accessed 6 December 2025.

ArtificialIntelligenceAct.eu, 'EU AI Act Overview' (Explainer on Risk Categories, 2025) <https://artificialintelligenceact.eu/> accessed 6 December 2025.

Congress.gov, 'Highlights of the 2023 US AI Executive Order' (CRS Report, Updated April 2024) <https://crsreports.congress.gov/product/pdf/R/R47843> accessed 6 December 2025.

Brookings Institution, 'How Different States are Approaching AI' (Analysis, 2025) <https://www.brookings.edu/articles/ai-regulation-in-the-us-states/> accessed 6 December 2025.

NCSL, 'Artificial Intelligence 2025 Legislation' (Summary of State Laws, July 2025) <https://www.ncsl.org/technology-and-communication/artificial-intelligence-2025-legislation> accessed 6 December 2025.

Brookings Institution, 'State AI Bills and Themes in 2025' (Analysis Continued) <https://www.brookings.edu/articles/state-ai-legislation-in-2025/> accessed 6 December 2025.

Cooley (Law Firm), 'Outcomes of the UK AI Safety Summit 2023' (Insight, Nov 2023) <https://www.cooley.com/news/insight/2023/2023-11-03-outcomes-of-the-uk-ai-safety-summit> accessed 6 December 2025.

UK Government, 'Chair's Summary of AI Safety Summit' (Declaration, Nov 2023) <https://www.gov.uk/government/publications/ai-safety-summit-2023-the-bletchley-declaration> accessed 6 December 2025.

White & Case (Law Firm), 'China AI Regulation Tracker' (Insight, Sep 2025) <https://www.whitecase.com/insights/our-thinking/china-ai-regulation-tracker> accessed December 2025.

China Law Translate, 'Interim Measures for Generative AI' (Unofficial Translation, 2023) <https://www.chinalawtranslate.com/en/generative-ai-measures/> accessed 6 December 2025.

Brookings Institution, 'Global AI Plans and National Strategies' (2025) <https://www.brookings.edu/articles/global-ai-strategies/> accessed 6 December 2025.