INTERNATIONAL REGULATION OF ARTIFICIAL INTELLIGENCE: AN OBSERVATION OF ITS EMERGING GLOBAL GOVERNANCE

Nohyoung Park

TABLE OF CONTENTS

INTERNATIONAL REGULATION OF ARTIFICIAL INTELLIGENCE: AN OBSERVATION OF ITS EMERGING GLOBAL GOVERNANCE

Nohyoung Park[*]

I. INTRODUCTION

Artificial intelligence (AI), including generative AI, has become a global priority for policymakers as rapid technological advancements raise questions of accountability, fairness, safety, and security. Its dual-use potential underscores why AI requires a coherent international legal framework: technologies intended for civilian applications can be repurposed for military or national security activities. This nature of AI has sparked heightened calls for international regulation, as unregulated AI may pose international risks, such as privacy violations, ethical dilemmas, and even threats to international peace and security.

Recent events, ranging from discussions at the United Nations (UN) to high-level summits in Europe and Asia, show a growing consensus on the urgency of AI governance. However, different states have adopted varying approaches, reflecting distinct legal traditions, security concerns, and industrial priorities. This paper intends to observe the main features of emerging AI regulations from the standpoint of international law. It examines how states and international organizations define AI, mitigate its risks in civilian contexts, coordinate through formal and informal frameworks, and grapple with potential military applications. Finally, the discussion turns to the China-US AI competition, which shapes global policy debates on export controls, data access, and security.

II. THE DEFINITION OF AI SYSTEMS TO BE AGREED INTERNATIONALLY

One of the major challenges in the international regulation of AI is defining it in a manner that aligns with rapid technological changes. The Organization for Economic Cooperation and Development (OECD), a

* Professor Emeritus at Korea University Law School.

group of developed countries, has defined an AI system.[1] The *EU Artificial Intelligence Act* (hereinafter referred to as the EU AI Act) and the *Council of Europe Framework Convention on Artificial Intelligence and Human Rights, Democracy and the Rule of Law* (hereinafter referred to as the CoE AI Convention) basically match the definition of AI coined by the OECD. Given how quickly AI evolves, its definition must be flexible enough not to stifle legitimate innovation or to exclude emerging variants of AI technologies. From an international law vantage point, harmonized definitions are vital for creating binding treaty obligations, ensuring harmonized enforcement, and clarifying state responsibility when AI is misused.

III. STATES' EFFORTS TO ENSURE AI SAFETY AND MITIGATE AI RISKS FOR CIVIL PURPOSES

A. General Regulation of AI Safety

Many states have published AI strategies that concentrate on civilian applications, such as healthcare, transportation, finance, and consumer services. The key tension lies in fostering innovation while preventing harm.

1. European Union. — The EU's approach stands out for its emphasis on a risk-based framework. Under the EU AI Act, effective in August 2024, systems posing 'unacceptable risk' (e.g., manipulative or exploitative uses) are effectively banned, while 'high-risk' systems must comply with strict rules on data governance, robustness, and oversight. This law is also extraterritorial and imposes obligations on AI providers or deployers located outside the EU when offering systems in the EU market. From an international law standpoint, such extraterritorial reach can raise questions about jurisdiction and potential conflicts with non-EU legal regimes.

2. United States. — The US tends to regulate AI through sector-specific agencies such as the Federal Trade Commission (FTC) or the Food and Drug Administration. Although the US has not yet enacted a unified federal AI law, executive orders and agency guidance highlight consumer protection, competition policy, and national security. This decentralized model may risk

1 An AI system is 'a machine-based system that, for explicit or implicit objectives, infers, from the input it receives, how to generate outputs such as predictions, content, recommendations, or decisions that can influence physical or virtual environments. Different AI systems vary in their levels of autonomy and adaptiveness after deployment.' OECD, *Recommendation of the Council on Artificial Intelligence*, I, OECD/LEGAL/0449 (2024).

fragmentation, potentially complicating the international alignment over AI regulation. Furthermore, there needs to be a consistent AI policy between different administrations, as US President *Donald Trump* released a new executive order (EO) to remove barriers to American leadership in AI on January 23, 2025 just after repealing former US President *Joe Biden*'s EO of October 2023 emphasizing responsible AI principles.

3. South Korea. — South Korea is the second jurisdiction after the EU to establish a comprehensive regulatory framework for AI systems. Its *AI Basic Act*, adopted in December 2024, appears to foster AI innovation primarily while imposing stricter requirements on high-impact AI systems similar to the EU AI Act.

B. AI Liability

There is a very good need to establish clearer rules on liability for AI-related harms, as traditional liability regulations do not fit the harm caused by the AI system. A notable initiative is the *EU Product Liability Directive* (hereinafter referred to as the EU PLD), effective in December 2024 to replace the original product liability directive of July 1985. The EU PLD aims to ensure that the product liability rules apply to any type of product, including the newest technologies such as software, including AI. However, in its 2025 work programme released on February 11, 2025, the European Commission announced that it planned to withdraw the *AI Liability Directive*, which was proposed to regulate the damage caused by AI systems in 2022 in parallel with the EU AI Act, because 'no foreseeable agreement' is expected on the proposal. In the US, the FTC has an enforcement authority to ensure that consumers and workers are protected from AI harms. The diversity of legal regimes may necessitate the utilization of harmonized international standards for liability, potentially through treaty law, model laws, or guidelines, to address cross-border liability cases.

C. International Cooperation for AI Regulation

International law governing technologies, such as cyber and AI, evolves through voluntary norms as well as through treaties. There are good indications of international cooperation for AI regulation, although detailed legal obligations must be agreed upon further.

1. OECD. — Although non-binding, the OECD's Principles on AI[2] are receiving broad support internationally. They highlight essential values such as transparency and accountability that align with many existing international law norms. Repeated adherence to the principles by a critical mass of states can contribute to the concerted development of international AI rules.

2. UN. — Two UN General Assembly resolutions were adopted through the initiative of the US emphasizing the safe, secure, and trustworthy use of AI and China emphasizing AI capacity building for developing countries in March and July 2024 respectively. Although these resolutions, adopted without a vote, have no binding effect, they would further guide the national and international regulatory development of AI systems. Additionally, the *Global Digital Compact* (GDC), adopted at the Summit of the Future in September 2024, aims to establish a more comprehensive framework for the global governance of digital technology and AI. If successfully implemented, it could pave a way for a multi-stakeholder approach to regulating AI globally.

3. Council of Europe. — The CoE AI Convention, open for signature on September 5, 2024, is the first binding international treaty on AI governance. However, certain exemptions for national security and defense and the option of indirect application to private sectors may dilute its effectiveness.

4. AI Summits. — A number of countries have gathered to discuss AI safety since the UK AI Safety Summit in November 2023 and the AI Seoul Summit in May 2024. The recent Paris AI Action Summit took place on February 10-11, 2025. The UK, the initiator of such summits, and the US, however, did not join the statement pledging an open, inclusive and ethical approach to AI development, while over 60 countries and regions including China, France, India, and the EU signed it in Paris. The UK apparently had concerns about national security and global governance, while the US had new concerns that too much regulation of AI could kill a transformative industry just as it is taking off. Thus, even major Western countries do not currently appear to be 'like-minded' in AI regulation for various reasons and perspectives.

2 The Principles, originally agreed by the Council on May 22, 2019, are the first intergovernmental standard on AI.

IV. STATES' EFFORTS TO REGULATE AI SYSTEMS FOR MILITARY AND NATIONAL SECURITY PURPOSES

The dual-use nature of AI emphasizes the importance of addressing its military and security implications in international law. AI can drastically alter the conduct of warfare and intelligence operations with respect to autonomous weapon systems and cyber operations. States reaffirm the applicability of international humanitarian law (IHL) to AI-driven warfare in that AI weapon systems comply with the principles of distinction, proportionality, and precautions. The challenge for states is now how to apply IHL to AI, as with cybersecurity. Another challenge is how tech companies are monitored and regulated in the development of AI, which could be used for military and national security purposes.

1. NATO. — NATO's *Artificial Intelligence Strategy*, adopted in October 2021 and revised in July 2024, articulates the *Principles of Responsible Use* (PRUs) for AI in defense, encompassing transparency, accountability, and bias mitigation.

2. REAIM Summits. — In February 2023, the Netherlands and South Korea co-hosted the summit on Responsible Artificial Intelligence in the Military Domain (REAIM 2023), the first global platform for all stakeholders to discuss military applications of AI, where a joint call to action on the responsible development, deployment, and use of AI in the military domain was adopted. The joint call to action was agreed upon by China and the US. In September 2024, South Korea with Kenya, the Netherlands, Singapore, and the UK hosted REAIM 2024, where the *Blueprint for Action* focusing on the technical, ethical, and operational aspects of military AI was adopted. The Blueprint was supported by 61 countries, but 30 countries including China, India, Israel did not endorse it. Although these initiatives are not legally binding and they are not supported by all those countries concerned, they can influence state practices and shape new norms that might later develop into customary international law.

3. US. — The *Political Declaration on Responsible Military Use of AI*, led by the US and endorsed by many countries, outlines best practices for states developing or deploying AI-enabled weapons. It encourages rigorous testing, legal reviews, and retention of human control over critical decisions. However, its non-binding nature and optional word ('should' instead of

'shall') may limit real enforceability. It should be a potential steppingstone towards formal rules.

V. CHINA-US COMPETITION IN AI DEVELOPMENT, DEPLOYMENT, AND USE

China-US competition significantly affects international AI regulation. Both countries are committed to advanced computing, supercomputers, and machine learning, which have immediate applications in both the civilian and defense areas.

1. Export Controls and Access to Chips. — The development and deployment of AI technologies requires advanced computer chips. The US has imposed stringent export controls to restrict China's access to advanced semiconductors. These measures reflect a strategic objective: slowing the AI progress of China by limiting the hardware essential for training and deploying complex AI models. In response, China is pursuing accelerated domestic chip production. It illustrates how geopolitics intertwines with technology regulations. From an international law perspective, the obligations under the World Trade Organization agreements regarding export restrictions against national security exceptions should be reviewed and refined in the AI era.

2. Restricting Access to Data. — AI systems require high-quality data. The US has recently heightened the scrutiny of its adversary states, regarding access to sensitive personal data or government-related datasets. It is perceived that advanced AI, combined with large datasets, could bolster foreign surveillance, misinformation campaigns, or cyber-attacks. However, these restrictions may entail the risk of data localization measures that undermine the free flow of information.

3. An Emerging Thread of Commonality. — High-level meetings between Chinese and US officials have occasionally signaled a shared acknowledgement of AI risks. Regarding the need to address the risks posed by advanced AI systems and to improve AI safety, officials from both countries convened in Geneva, Switzerland, in May 2024 to discuss AI risks and safety. However, no concrete agreements or outcomes were achieved.

Nonetheless, there have been positive signs of bilateral cooperation between China and the US. On November 16, 2024, during a meeting on the sidelines of the APEC summit in Lima, Peru, an agreement was reached to

refrain from giving AI control of nuclear weapons systems. The agreement commits both countries to ensure that 'there should be human control over the decision to use nuclear weapons.' If China and the US continue to reach meaningful agreements, that could pave the way for a broader global consensus on AI regulation, given their status in technology and security.

VI. OBSERVATION

AI's rapid growth has prompted complex patchwork of regulations across countries. International law in this domain is still in its formative stages, combining soft-law instruments such as declarations and voluntary norms with nascent treaty efforts such as the CoE AI Convention, in addition to domestic legislation specific to AI, such as those of the EU and South Korea. From an international governance standpoint, states try to balance the need for innovation with the imperative of minimizing risks and ensuring respect for human rights.

The major hurdles remain as follows: first, defining AI in a way that accommodates future innovations without overly broadening or narrowing the regulatory scope; second, allocating liability for AI-driven harms across borders for self-learning systems to produce unexpected outcomes; and third, enforcing standards in national security and military contexts, where transparency is limited and strategic incentives to deploy advanced AI could overshadow proper legal restraints.

With technology advances at an ever-accelerating pace, states may have two choices: crafting legal structures that responsibly and ethically guide AI's development and deployment or risking a fragmented regulatory landscape that leaves critical gaps in accountability and governance. Continued dialogue and negotiation resulting in any agreement in the form of treaties or voluntary norms is required, if international law is to keep pace with AI's evolution in international peace and security context.

(Edited by Li Jiesi)