ENSURING LEGAL CERTAINTY AND LIABILITY IN ARTIFICIAL INTELLIGENCE DEVELOPMENT: CONTEMPORARY FRAMEWORKS

Vadiya Alakbarzade*

Abstract

The legal security and liability issues that have emerged with the rapid development of artificial intelligence (hereinafter - AI) technologies have become one of the key legal and scholarly challenges of the modern age in the context of international law and human rights. This article examines the impact of artificial intelligence on human rights, especially the right to respect for private life, the principle of non-discrimination, freedom of expression and data confidentiality. The study analyzes the normative frameworks and guiding principles put forward by influential international organizations such as the Council of Europe, UNESCO and the Organization for Economic Co-operation and Development (OECD) regarding the ethical and legal governance of artificial intelligence. In the light of the general principles of international law, the article emphasizes the imperative to adhere to principles of transparency, lawfulness, and data minimization during the data collection and processing phase. The article thoroughly examines issues such as legal gaps, the concept of technological neutrality, and the legal personhood or status of artificial intelligence. In this context, leading legal scholars and ethical theorists such as Luciano Floridi and Frank Pasquale emphasize that technology is inherently non-neutral and highlight the importance of establishing mechanisms for the legal accountability of artificial intelligence systems based on scientifically grounded principles. The study proceeds by presenting the comparative regulatory models adopted by jurisdictions such as the European Union, the United States, China, and South Korea regarding the legal governance of artificial intelligence. As a result, the article underscores the need to develop flexible, accountable, and human rights-compliant mechanisms at both the international and domestic levels, grounded in the principle of technological neutrality, in order to ensure the safe, lawful, and ethical development of artificial intelligence.

Keywords: *artificial intelligence, legal liability, human rights, ethics of artificial intelligence, international legal regulation, right to privacy, non-discrimination, freedom of expression, technological neutrality, legal personhood, due diligence principle.*

I. Introduction

In the current era of rapid technological evolution, artificial intelligence (AI) has emerged as a transformative force with far-reaching implications for legal systems, fundamental rights, and democratic governance. As AI technologies increasingly influence decision-making processes in areas such as healthcare, employment, finance, law enforcement, and public administration, they simultaneously generate significant legal and ethical concerns. Central among these is the issue of legal certainty—namely, the need to define clear and enforceable legal norms that govern the development, deployment, and accountability of AI systems.

Within the framework of international human rights law, the integration of AI into public and private sectors introduces a new dimension of risk regarding individual rights and state obligations. Emerging technologies have the capacity to infringe upon core rights protected by the Universal Declaration of Human Rights (UDHR), including the right to privacy, the right to non-discrimination, and freedom of expression. Moreover, algorithmic decision-making and data processing systems may operate in

* PhD candidate in Law, Baku State University, Deputy Director for Legal Affairs, Strategy and Digital Management at "Sağlam Ailə" Medical Center

non-transparent ways that undermine due process, legal redress, and procedural fairness. In this context, the concept of legal responsibility—particularly the attribution of liability in cases of harm—must be reconsidered to address the complexities of autonomous and semi-autonomous systems.

International bodies such as the Council of Europe, UNESCO, and the OECD have recognized the urgency of these issues, advocating for governance mechanisms that uphold the rule of law while supporting innovation. For example, the Council of Europe's 2024 Framework Convention on AI, Human Rights, Democracy and the Rule of Law seeks to establish a harmonized legal foundation rooted in technological neutrality, transparency, and accountability. Likewise, UNESCO's 2021 Recommendation on the Ethics of Artificial Intelligence emphasizes the integration of ethical principles—such as human oversight, justice, and fairness—into AI governance models.

This article undertakes a comprehensive analysis of the intersection between AI and international legal norms, with a focus on legal liability, data protection, algorithmic fairness, and state responsibility. It evaluates regulatory models across jurisdictions—including the European Union, United States, China, and South Korea—while highlighting the necessity of a globally coordinated, human rights–based approach. In doing so, the study underscores that legal systems must evolve in tandem with technological advancements, ensuring that the rights, freedoms, and dignity of individuals remain protected in the digital age.

II. Artificial Intelligence and Human Rights Context

The rapid advancement of artificial intelligence (AI) has rendered its legal regulation one of the foremost priorities on the global governance agenda. As stated in the explanatory memorandum of the "Framework Convention on Artificial Intelligence, Human Rights, Democracy and the Rule of Law [12], opened for signature by the Council of Europe in 2024, this international treaty aims to ensure that artificial intelligence systems conform fully to the principles of human rights, democracy, and the rule of law throughout their entire lifecycle. The Convention is intended to address regulatory gaps in the rapidly evolving technological landscape and, rather than regulating specific technologies, seeks to maintain technological neutrality [11]. At the same time, the development of AI systems introduces significant legal and ethical risks across various domains of public life, including violations of the right to privacy, discriminatory practices, unlawful interference with personal data, and constraints on freedom of expression [35, Art. 12, 19]. For instance, as emphasized in the Executive Order signed by the President of the United States in 2023 [21], irresponsible use of AI can exacerbate adverse societal effects such as fraud, discrimination, bias, and disinformation. Accordingly, the principles of human rights protection and legal certainty are prioritized in the global governance of artificial intelligence [35, §II.2]. The importance of fundamental values such as the protection of human dignity and rights, transparency, and justice is also underlined in UNESCO's "Recommendation on the Ethics of Artificial Intelligence", adopted in 2021. These guiding principles are intended to promote legally sound and ethically aligned development and deployment of artificial intelligence systems.

The development of AI has introduced new challenges in the implementation of several fundamental human rights. As emphasized in the reports of the United Nations and other international organizations [27], right enshrined in the Universal Declaration

of Human Rights (UDHR)- including the right to life, liberty and personal security (Article 3), the right to an effective remedy (Article 8), the right to privacy (Article 12), and freedom of thought and expression (Article 19) are regarded as core principles that must be integrated into the design and development of artificial intelligence systems. For instance, empirical studies documenting racial and ethnic bias in algorithmic systems such as facial recognition technologies [2] demonstrate the necessity of principles of equality and non-discrimination to ensure fairness in AI outcomes. In this regard, the European Union promotes the development of transparent and explainable algorithms [14; 15] as part of its broader effort to mitigate risks of discrimination and opacity stemming from AI technologies. In light of these developments, it is evident that the impact of artificial intelligence on human rights, including violation of privacy, discriminatory practices, limitations on freedom of expression, and infringements upon the inviolability of private life – has emerged as a matter requiring robust regulatory oversight within the framework of international human rights law [27].

III. Artificial Intelligence and International Legal Norms: Data Protection, Algorithmic Justice and Automated Decision-Making

In the application of AI within the framework of International human rights principles, the rights to privacy, fairness and accountability must be rigorously upheld. Article 12 of the Universal Declaration of Human Rights (UDHR) affirms that everyone has the right to protection against arbitrary interference with their private life, family, home and correspondence. Similarly, Article 17 of the International Covenant on Civil and Political Rights (ICCPR) [32, Art. 17] enshrines the right to be protected from unlawful or arbitrary interference with one's privacy and communications. The Council of Europe Convention 108 (1981) [7] and its modernized "Convention 108+" Protocol (2018) [9] require that the development and deployment of AI systems comply with the principle of privacy and data protection as set forth in Article 8 of the European Convention on Human Rights (ECHR) [6, Art. 8]. At the international level, organizations such as the United Nations [27] and UNESCO [35] emphasize the importance of lawfulness, purpose limitation, transparency and strict adherence to the "privacy by design" approach in the collection, storage and processing of personal data by AI systems. For instance, it is recommended that Data Protection Impact Assessments (DPIAs) be conducted for high-risk AI projects, [20, Art. 35] alongside the implementation of data minimization and strategies and enhanced cybersecurity safeguards. [20, Art. 5]. Furthermore, UNESCO's Recommendation on the Ethics of Artificial Intelligence [35, §III.8] places particular emphasis on the protection of data and the right to privacy throughout the AI lifecycle, calls for the establishment of robust national and international legal frameworks to ensure effective data governance.

The Impact of AI on Data Protection and the Right to Privacy. AI systems process vast volumes of personal data for purposes including profiling, quantitative analysis and automated decision-making. Such practices can ultimately pose significant threats to the right to privacy. According to the Council of Europe's recommendations [9], where AI projects involve the processing of personally identifiable information, they must comply with the principles enshrined of Convention 108+ - lawfulness, fairness, purpose, limitation, proportionality and personal data protection. In addition, the principles of "privacy by design" and "privacy by default" [20, Art. 25] must be applied. These approaches require that only data which is necessary and relevant be

collected, and that it be processed in a manner consistent with legal and transparent standards. Technical and organizational safeguards must be implemented to ensure the transparent and accountable operation of AI systems. The rights of data subjects – including the right to be informed about the collection and use of their data, the right to object, and the right to request human review [20, Arts. 13–15, 22] – must be respected and upheld. At the international level, the European Union's General Data Protection Regulation (GDPR) [20] provides that AI algorithms, whether developed independently or integrated into existing systems, fall within the scope of binding data protection requirements. Users must be informed of how profiling is conducted and must have access to adequate transparency measures in order to minimize the risks of discrimination and error [20, Art. 22]. UNESCO's Recommendation on the Ethics of Artificial Intelligence [35, §III.8] likewise underscores the fundamental importance of data protection and the right to privacy across the entire AI lifecycle. It further calls for the establishment of robust national and international legal frameworks to effectively address these concerns. As a result of the international normative obligations [27] and policy recommendations, national legal systems are required to implement specific safeguards aimed at preventing privacy infringements in AI applications. These may include pre-implementation risk assessment [20, Art. 35], data anonymization techniques, and enhanced cybersecurity protocols [9]. In accordance with access to information and data protection laws, state institutions must also ensure transparency by disclosing how data is processed and must afford individuals the ability to challenge decisions made by automated systems [20, Art. 22]. Ongoing international monitoring, and cross-border cooperation are crucial to ensuring that AI evolves in a manner that is fully compliant with privacy rights [35, §IV.13].

Algorithmic Justice and Non-Discrimination. The application of AI in decision-making systems increases the risk of individuals being subjected to discrimination based on gender, race, religion, disability, and other personal characteristics. This contradicts the fundamental principles of international law, namely the right to equality before the law and protection from discrimination. For instance, Article 7 of the Universal Declaration of Human Rights (UDHR) emphasizes that all individuals are equal before the law, and core UN human rights instruments such as the International Convention on the Elimination of All Forms of Racial Discrimination [31, Art. 2] mandate a comprehensive prohibition of discrimination. Article 14 of the European Convention on Human Rights (ECHR) and Article 21 of the Charter of Fundamental Rights of the European Union [19, Art. 21] enshrine the same principle by prohibiting discrimination. This legal framework requires the integration of fairness and inclusivity into the design and development of AI systems. However, AI models frequently replicate patterns embedded in historical data and may inadvertently reinforce systemic biases. As a result, algorithmic systems can exacerbate discrimination, for instance, in recruitment, credit scoring or law enforcement. The "Fairness and Non-Discrimination" principle in UNESCO's Recommendation on the Ethics of Artificial Intelligence [35, §III.9] underscores that AI systems must promote social justice and avoid discriminatory outcomes. Accordingly, states and private entities should identify potential discriminatory impacts of algorithmic systems at early stages and implement appropriate technical and organizational safeguards.

In international practice, such as the Council of Europe's draft Convention on AI [10], specific measures are envisaged to address algorithmic bias and discrimination

risks. Furthermore, the EU's draft Artificial Intelligence Act highlights fairness as a core criterion in classifying high-risk AI systems, particularly those involving public sector functions and decision-making authority, and imposes obligations to mitigate discrimination.

In particular, for AI systems used in the public sector, human rights impact assessments should be conducted [27], and any resulting discriminatory effects must be thoroughly evaluated. Finally, the reinforcement of remedial legal protections—such as ensuring the right to judicial review of biased automated decisions [20, Art. 22]—plays a vital role in safeguarding the right to equality and justice.

IV. Legal Regulation of Automated Decision-Making and Human Oversight

Although automated decision-making systems can make rapid and large-scale decisions in many areas of life, the complete exclusion of the human factor from these processes raises new ethical and legal concerns. Under international human rights law, individuals have the right not to be subject to significant decisions made solely by automated systems. For instance, Article 22 of the General Data Protection Regulation (GDPR) [20, Art. 22] grants data subjects the right not to be subject to a decision based solely on automated processing that produces legal or similarly significant effects. This provision also requires that the underlying decision-making mechanisms be transparent, include human involvement, and allow for the possibility of post-decision review.

UNESCO's Recommendation on Ethics of Artificial Intelligence [35, §III.10] highlights in its article "Human Oversight and Determination" that primary responsibility must always rest with humans, not with AI systems. In its proposed Artificial Intelligence Act [17, Art. 14], the European Union mandates that high-risk AI systems operate under effective human oversight. For instance, the 2024 text of the European Commission's Artificial Intelligence Act [14, Art. 14(3)] calls for tools to enable active human monitoring of such systems (e.g., a "stop button") and the development of comprehensive human-machine interfaces. The objective is not only to identify technical failures and biases, but also to ensure that humans can consciously intervene in system decisions. Various regulatory measures may be envisaged to strengthen human oversight in automated systems. For instance, where public authorities utilize AI, legislation should require human actors to be actively involved in the decision-making and accountable for the final decision [11, Principle 4]. Whether in the public or private sector, users must have the right to challenge system decisions and request human review [20, Art. 22(3)]. Additionally, administrators and decision-makers should uphold the principle of "necessary human control," gaining a thorough understanding of AI's capabilities and limitations through targeted education and training programs [35, §III.10].

V. Legal Gaps, Ethical Risks and Technological Neutrality

AI applications give rise to a number of regulatory gaps within existing legal frameworks. While modern technological innovation is advancing rapidly, traditional legal systems struggle to adapt to these developments. For example, as emphasized in the Explanatory Memorandum of the Council of Europe's Framework Convention [11, para. 15], mechanisms intended to address the legal gaps emerging from rapid technological change should be technology-neutral-that is, overarching legal principles rather than tailored to specific technologies. However, some experts, including Luciano

Floridi [22, p. 42], challenge this approach. Floridi argues that the prevailing doctrine of technological neutrality is flawed - "no technology is ever neutral" and its design inherently reflects value-laden moral choices. This perspective underscores the legal significance of ethical risks: there is a need for legal frameworks that define principles such as reliability, fairness, and transparency in both the design and application of AI systems Without such regulation, challenges concerning the attribution of liability may arise- i.e., when harm results from a system failure, it becomes difficult to identify who should be held accountable [29, p. 358].

The issue of legal personhood also remains central in AI-related legal discourse. In traditional legal theory, "legal subject" refers to entities such as individuals or corporations, created for an indefinite range of purposes. However, with the evolution of AI systems, discussions have emerged around the potential recognition of AI as a distinct legal person. For example, former US District Judge Katherine Forrest states in her speech that legal subjectivity is a dynamic and inherently political concept, evolving over time as new legal categories are established to protect human interests. She emphasizes that human-like consciousness is not a necessary precondition for legal subjectivity. Corporations, for example, are not human beings, yet they possess rights and obligations granted for the purpose of functional utility [30, p. 1235]. On this basis, some legal scholars suggest that if AI systems achieve advanced cognitive complexity and autonomous reasoning capacity, standardized criteria may be required to grant them legal personhood [1]. Conversely, other perspectives argue that the current legal personhood structure is sufficient for maintaining liability mechanisms, while some advocate for the development of new mechanisms specifically designed to safeguard human accountability in the face of potentially harmful AI outcomes [35, §IV.7]. In scenarios where AI technologies might claim "consciousness" in the future, the legal system may need to expand its theoretical foundations to determine appropriate liability standards. At present, ongoing legal scholarship explores the adaptation of traditional liability theories-such as producer liability and operator liability AI applications. Altogether, this evolving landscape demonstrates that both the principle of technological neutrality and emerging concepts of legal personhood are integral to shaping contemporary approaches to legal responsibility in the context of AI.

VI. International responsibility of the state regarding artificial intelligence

International law establishes obligations that attribute responsibility to states for activities arising from the use of artificial intelligence. According to the Articles on the Responsibility of States for Internationally Wrongful Acts (ARSIWA, adopted by the United Nations in 2001) [36, Art. 2], a state is held responsible for any conduct that qualifies as an internationally wrongful act. Under t of Article 2 of ARSIWA, such conduct consists of a breach of an international obligation attributable to the state. Crimes or violations of international law committed by state organs or individuals acting under state authority in the context of managing AI systems are deemed acts of the state. For example, the emergence of racial discrimination in facial recognition systems implemented by public institutions is considered a violation of the state's international human rights obligations [23, Art. 5]. Article 3 of ARSIWA emphasizes that the fact that an act complies with domestic law does not mean that it is also lawful under international law [36, Art. 3].

Crimes or violations of international law committed by state organs or individuals acting under state authority in the context of managing AI systems are deemed acts of the state. For example, if racial discrimination emerges from facial recognition systems implemented by public institutions, such an occurrence is considered a breach of the state's international human rights obligations. Article 3 of ARSIWA further clarifies that conformity with domestic law does not render an act lawful under international law. Acts involving AI carried out by state bodies are thus indirectly attributed to the state. Articles 4–8 of ARSIWA [36, Arts. 4-8] establish that the conduct of any organ forming part of the state's institutional structure may incur full international responsibility. For example, if a human rights violation occurs through an AI system developed or deployed by experts under state direction or control, that violation is evaluated as part of the state's international legal responsibility [34, para. 4]. Article 11 of ARSIWA also holds a state responsible for conduct that it acknowledges and adopts as its own. In accordance with Article 12, an internationally wrongful act arises when the conduct of a state is not fully in conformity with its binding international obligations [36, Art. 12]. In this regard, states must ensure compliance with core standards such as human rights, non-discrimination, data confidentiality, and transparency when implementing AI systems [35, §IV.5]. Should a state or its authorized institutions fail to uphold these obligations as a result of AI deployment, international legal responsibility will be incurred. Moreover, under Article 14(3) of ARSIWA, the state is obligated to prevent certain adverse outcomes. In other words, a state's failure to act, despite foreseeing that the use of AI may result in unlawful outcomes, may itself constitute a breach of international law. For instance, if a state anticipates that the use of mass automated surveillance will infringe upon human rights, yet fails to take legislative or administrative steps to prevent it, the resulting harm triggers state liability [16, §125]. Articles 28–31 of ARSIWA specify the legal consequences a state faces for committing internationally wrongful acts. According to Article 30, the state must cease the wrongful conduct and offer guarantees of non-repetition. Article 31 requires the state to provide full reparation for the material and moral damage caused. These principles are directly applicable to violations arising from AI use. For example, if the misuse of a state-operated high-tech surveillance system leads to the unlawful dissemination of personal data and harms individuals, the responsible authority must cease the violation, implement institutional safeguards to prevent recurrence, and compensate affected persons.

In sum, ARSIWA clarifies the scope of state responsibility under international law in relation to artificial intelligence. The message to states is clear: while the deployment of AI may fall under national sovereignty, it is simultaneously subject to international legal scrutiny. States must ensure that AI applications within their jurisdiction conform to international law and proactively implement preventive measures to avoid violations. Failure to do so may result in international accountability, including proceedings before international tribunals.

VII. Principles of "Due Diligence" and "Failure to Prevent"

In international law, the principle of due diligence obliges states to exercise maximum effort to prevent harmful events that may occur within their jurisdiction. This means that states are under a duty to take progressive and reasonable measures against any activity that could harm neighboring states, their own citizens, or the international community at large [24]. For example, the Council of Europe's

Recommendation on the Prevention of Violence against Women affirms that states must act with due diligence when responding to acts of violence and must adopt adequate preventive, investigative, and punitive measures. This legal obligation is echoed in instruments such as the CEDAW Committee's General Recommendations, declarations on violence against women [8], and other international human rights documents. The European Court of Human Rights has similarly stressed in its case law that states must take operational preventive measures to protect individuals.

In the context of artificial intelligence, the due diligence principle requires states to implement legislation, standards, and monitoring mechanisms to mitigate risks associated with AI technologies. For example, states should carry out risk assessments, algorithmic bias evaluations, and security audits in AI projects, and adopt preventive regulatory measures to avoid discriminatory or otherwise harmful outcomes. Failure by a state to fulfill its due diligence obligation—that is, not taking the necessary precautions despite being capable of doing so—may constitute a case of failure to prevent under international law [36, p. 66]. In this context, if a rights violation occurs as a result of AI implemented within public or private institutions under the state's jurisdiction, affected individuals may pursue legal remedies, and the state may be held internationally responsible.

Consequently, states should adopt a due diligence-based approach to prevent legal risks arising from AI technologies. As part of this approach, they should:

- Conduct preliminary impact assessments for systems with a high risk of misuse [26, §1.4];
- Establish robust oversight mechanisms through regulatory and enforcement bodies [35, §IV.5];
- Enhance access to legal remedies for individuals [33, Principle 11];
- Provide full and effective compensation in cases of violations [25, §57].

Otherwise, state inaction may be regarded as a breach of international law under Article 3 of the Articles on the Responsibility of States for Internationally Wrongful *Acts (*ARSIWA) [36, Art. 3].

VIII. Recommendations from International Organizations and Legal Scholars

International organizations have adopted various instruments to shape the ethical and legal governance framework for artificial intelligence (AI). UNESCO's 2021 Recommendation on the Ethics of Artificial Intelligence prioritizes human rights and human dignity in AI systems, emphasizing the principles of transparency, fairness, accountability, and human oversight. The OECD's 2019 AI Principles adopt a similar position—supporting technological innovation while ensuring that "trustworthy AI" upholds human rights and democratic values [26, Principle 1.2]. These OECD guidelines provide practical regulatory recommendations to help governments and the private sector develop governance environments conducive to the implementation of these principles. It is evident that the overall aim is to establish a human rights-based framework for AI development and use.

In addition to the efforts of international organizations, a number of prominent legal scholars have made significant contributions to this field by conducting theoretical research on the legal normativity of AI. For instance, Frank Pasquale, Professor of Law at Yale University, is widely recognized for his work on "algorithmic judgment" [28, p. 8], in which he underscores the critical importance of ensuring accountability in the

deployment of AI systems. Luciano Floridi, in contrast, advocates the position that "technology is never neutral," [22, p. 42], emphasizing the role of public interest and ethical values in the design and governance of AI systems.

The research conducted by these legal theorists and philosophers illustrates that standardized policy frameworks alone are insufficient to ensure responsible AI governance [5, p. 156]. Instead, a synthesis of legal and ethical approaches is necessary to address the complex challenges posed by AI [38, p. 195].

At the United Nations level, the establishment of a High-Level Advisory Body on Artificial Intelligence in 2023 aims to develop global standards for AI governance and to promote a value-driven, rights-respecting global AI framework [37].

In conclusion, both international documents and expert opinions emphasize the necessity of placing AI under value-based governance, with a strong emphasis on safeguarding human rights at every stage of AI development and deployment [35, §IV.1].

IX. Comparative Regulatory Analysis: EU, US, China, South Korea

There are significant regulatory divergences among regions and countries in the governance of artificial intelligence (AI). The European Union adopted a risk-based legislative framework with its Artificial Intelligence Act in 2024 [18]. This regulation imposes strict technical, transparency, and accountability requirements on AI systems classified as high-risk, with a particular emphasis on the protection of fundamental rights. Furthermore, the European Commission's work plan includes provisions for permanent legal remedies for individuals harmed by AI applications [14; 15].

However, a uniform approach to AI-related liability has not yet been fully developed. As a result, regulatory fragmentation among Member States may persist, compelling affected individuals to seek legal redress on a national basis.

In the United States, AI governance is largely sector-specific and agency-driven. Executive Order 14110, signed in 2023, provides guidance on developing safe, reliable, and accountable AI, instructing federal agencies to update and align existing legal frameworks. U.S. institutions such as the Department of Justice [13], the Federal Trade Commission, and the Civil Rights Commission have sought to apply existing authorities to address discrimination and bias within AI systems. While certain states (e.g., California) have adopted standalone AI regulations, there remains no unified federal legislation. Accordingly, U.S. AI policy continues to operate within the bounds of existing legal norms, while international instruments—such as the AI Bill of Rights—remain non-binding and advisory in nature.

In China, AI regulation is characterized by centralized state control. In 2023, regulatory agencies introduced the Interim Measures for the Governance of Generative AI Services [4, Order No. 15], which constitute the first comprehensive rules for open content generation systems (e.g., ChatGPT-type models). Additionally, separate laws adopted in 2022–2023 address "deep synthesis" (deepfake) technologies [3] and recommendation algorithms, emphasizing data protection and content authenticity. China's broader regulatory framework includes stringent privacy rules under the Cybersecurity Law (2017), Data Security Law (2021), and Personal Information Protection Law (2021). For example, beginning in September 2025, all AI-generated text, audio, and video must be clearly labeled or watermarked, ensuring transparency and accountability. Overall, China is developing a complex regulatory architecture that

simultaneously promotes technological advancement and enforces state-centric oversight mechanisms.

South Korea passed its first comprehensive AI law—the Basic Law on the Development of Artificial Intelligence—in late 2024. This legislation introduces a risk-based model, similar to that of the EU, and includes content labeling obligations for generative AI outputs. In the future, content produced by such systems must be labeled to prevent misinformation and detect deepfakes. The law mandates human oversight in high-risk domains such as healthcare, employment, and essential services, and requires the formulation of risk management protocols. It also promotes infrastructure investments to foster responsible AI innovation. Enforcement bodies have insisted on strict adherence to existing privacy protections, particularly under the Personal Information Protection Act (PIPA). South Korea's regulatory model aims to balance innovation with individual rights protection.

This comparative analysis demonstrates that the EU seeks legal certainty by enacting the first dedicated AI law based on a risk framework; the U.S. relies on adapting existing laws within a fragmented regulatory landscape; China emphasizes state surveillance, content governance, and ideological conformity; and South Korea pursues a balanced, innovation-friendly regime with strong rights protections. These divergent approaches significantly influence the shaping of emerging global AI standards, as each region navigates its own equilibrium between technological development, democratic accountability, and human rights safeguards.

X. Conclusion

The issue of legal certainty and state responsibility concerning artificial intelligence (AI) is increasingly gaining importance within the framework of both international human rights norms and domestic legislation. AI technologies must respect individuals' rights to privacy, non-discrimination, and freedom of expression. International organizations (UNESCO, OECD, Council of Europe, etc.) and leading legal scholars emphasize that the principle of respect for human rights should form the basis for the design and implementation of AI systems. While the application of the technological neutrality principle contributes to the durability and adaptability of regulations, critics such as Luciano Floridi argue that the design of technology is itself an ethical act, inherently embedding values into AI systems. Legal systems are inherently flexible when it comes to legal personhood, having historically created new mechanisms and doctrines when necessary (e.g., corporate liability, intellectual property, legal fiction entities).

Under the UN Articles on the Responsibility of States for Internationally Wrongful Acts (ARSIWA), states may be held internationally responsible for violations committed through or by means of artificial intelligence. In this context, breaches committed by state organs, state-affiliated entities, or individuals acting under state instruction in the development or deployment of AI systems are attributable to the state under international law. In other words, international responsibility arises for any violation linked to the creation or use of state-sanctioned or state-controlled AI technologies.

States must adopt preventive measures grounded in the due diligence principle to mitigate the risks associated with AI. This includes a positive obligation to identify, assess, and minimize potential harms arising from the deployment of AI systems. A state's failure to prevent foreseeable human rights violations, such as the discriminatory

application of AI algorithms, may result in international legal liability for the resulting damages.

Regulatory approaches vary across jurisdictions:

- The European Union favors a risk-based, fundamental rights-oriented regulatory model;
- The United States focuses on adapting existing regulatory frameworks through agency-specific guidance;
- China enforces comprehensive state-led control and content governance;
- South Korea seeks to balance innovation and accountability through comprehensive legislation and robust oversight.

As a result, key principles such as privacy, non-discrimination, freedom of expression, technological neutrality, and state responsibility should be prioritized in legal frameworks governing AI. The development of a multi-level human rights–based legal architecture—nationally, regionally, and globally-is essential to ensure the ethical, transparent, and accountable use of artificial intelligence.

References:

1. Bryson, J. J., et al. (2017). Of, for, and by the people: The legal lacuna of synthetic persons. Artificial Intelligence and Law, 25(3), 273-291.
2. Buolamwini, J., & Gebru, T. (2018). Gender shades: Intersectional accuracy disparities in commercial gender classification. Proceedings of Machine Learning Research, 81, 1-15.
3. CAC. (2022). Provisions on the Administration of Deep Synthesis in Internet Information Services. Order No. 12.
URL: https://www.chinalawtranslate.com/en/deep-synthesis/(last access: 12.01.2025).
4. CAC. (2023). Interim Measures for the Management of Generative AI Services. Order No. 15.
URL: https://www.chinalawtranslate.com/en/generative-ai-interim/(last access: 10.01.2025).
5. Cath, C., Wachter, S., Mittelstadt, B., Taddeo, M., & Floridi, L. (2018). Artificial intelligence and the 'good society': The US, EU, and UK approach. Science and Engineering Ethics, 24(2), 505-528.
6. Council of Europe. (1950). European Convention on Human Rights (ECHR). ETS No. 5.
URL: https://rm.coe.int/1680a2353d (last access: 11.01.2025).
7. Council of Europe. (1981). Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (Convention 108). ETS No. 108.
URL: https://rm.coe.int/1680078b37 (last access: 08.01.2025).
8. Council of Europe. (2002). Recommendation Rec(2002)5 on the protection of women against violence.
URL: https://www.coe.int/en/web/genderequality/recommendation-rec-2002-5-and-other-tools-of-the-council-of-europe-concerning-violence-against-women (last access: 10.01.2025).
9. Council of Europe. (2018). Protocol Amending the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (Convention 108+). CETS No. 223.
URL: https://rm.coe.int/16808ac918 (last access: 12.01.2025).

10. Council of Europe. (2023). Draft Framework Convention on Artificial Intelligence, Human Rights, Democracy and the Rule of Law.

URL:https://internazionale.camera.it/sites/internazionale/files/atti_approv/APCE_Opinion-303_EN.pdf (last access: 09.01.2025).

11. Council of Europe. (2024). Explanatory Report to the Framework Convention on AI, Human Rights, Democracy and the Rule of Law.

URL: https://rm.coe.int/1680afae67 (last access: 12.01.2025).

12. Council of Europe. (2024). Framework Convention on Artificial Intelligence, Human Rights, Democracy and the Rule of Law. Strasbourg: Council of Europe.

URL: https://www.coe.int/en/web/artificial-intelligence/the-framework-convention-on-artificial-intelligence (last access: 07.01.2025).

13. Department of Justice (DOJ). (2023). Algorithmic Justice Initiative: Guidance on AI and Civil Rights.

URL: https://www.justice.gov/archives/crt/ai (last access: 11.01.2025).

14. European Commission. (2024). Artificial Intelligence Act (Final Text). COM(2024) final.

URL: https://data.consilium.europa.eu/doc/document/ST-11625-2024-INIT/en/pdf (last access: 05.01.2025).

15. European Commission. (2024). Proposal for a Regulation laying down harmonized rules on artificial intelligence (Artificial Intelligence Act). Brussels: EU.

URL: https://eur-lex.europa.eu/eli/reg/2024/1689/oj/eng (last access: 09.01.2025).

16. European Court of Human Rights. (2018). Big Brother Watch v. United Kingdom. App. No. 58170/13, 62322/14, 24960/15.

URL: https://hudoc.echr.coe.int/fre#{%22itemid%22:[%22001-210077%22]} (last access: 12.01.2025).

17. European Parliament. (2020). Resolution on a comprehensive European industrial policy on AI. 2020/2016(INI).

URL: https://www.europarl.europa.eu/doceo/document/TA-8-2019-0081_EN.html (last access: 12.01.2025).

18. European Parliament. (2024). Regulation on Artificial Intelligence (AI Act). Regulation (EU) 2024/1689.

URL: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=OJ:L_202401689 (last access: 08.01.2025).

19. European Union (EU). (2000). Charter of Fundamental Rights of the European Union. OJ C 364/1.

URL: https://www.europarl.europa.eu/charter/pdf/text_en.pdf (last access: 09.01.2025).

20. European Union (EU). (2016). General Data Protection Regulation (GDPR). Regulation (EU) 2016/679.

URL: https://gdpr-info.eu/(last access: 06.01.2025).

21. Exec. Order No. 14,110, 3 C.F.R. (2023). Safe, Secure, and Trustworthy Development and Use of Artificial Intelligence.

URL: https://www.federalregister.gov/documents/2023/11/01/2023-24283/safe-secure-and-trustworthy-development-and-use-of-artificial-intelligence (last access: 12.01.2025).

22. Floridi, L. (2018). Soft ethics and the governance of the digital. Philosophy & Technology, 31(1), 1-8.

23. International Convention on the Elimination of All Forms of Racial Discrimination. (1965). 660 U.N.T.S. 195.
URL: https://www.ohchr.org/en/instruments-mechanisms/instruments/international-convention-elimination-all-forms-racial (last access: 09.01.2025).
24. International Court of Justice. (1949). Corfu Channel Case (UK v. Albania). 1949 I.C.J. 4.
URL: https://www.icj-cij.org/case/1 (last access: 10.01.2025).
25. International Court of Justice. (2012). Ahmadou Sadio Diallo (Guinea v. DRC), Compensation. 2012 I.C.J. 324.
URL: https://www.icj-cij.org/node/102047 (last access: 07.01.2025).
26. OECD. (2019). OECD Recommendation of on Artificial Intelligence. OECD/LEGAL/0449.
URL: https://oecd.ai/en/assets/files/OECD-LEGAL-0449-en.pdf (last access: 12.01.2025).
27. Office of the High Commissioner for Human Rights (OHCHR). (2021). The Right to Privacy in the Digital Age. UN Doc. A/HRC/48/31.
URL: https://docs.un.org/en/A/HRC/48/31 (last access: 11.01.2025).
28. Pasquale, F. (2015). The black box society: The secret algorithms that control money and information. Harvard University Press.
29. Scherer, M. U. (2016). Regulating artificial intelligence systems. Harvard Journal of Law & Technology, 29(2), 353-400.
30. Solum, L. B. (1992). Legal personhood for artificial intelligences. North Carolina Law Review, 70(4), 1231-1287.
31. UN General Assembly (UNGA). (1965). International Convention on the Elimination of All Forms of Racial Discrimination. UNTS Vol. 660.
URL: https://treaties.un.org/pages/viewdetails.aspx?src=treaty&mtdsg_no=iv-2&chapter=4&clang=_en (last access: 12.01.2025).
32. UN General Assembly (UNGA). (1966). International Covenant on Civil and Political Rights (ICCPR). UNTS Vol. 999.
URL:https://treaties.un.org/PAGES/ViewDetails.aspx?chapter=4&clang=_en&mtdsg_no=IV-4&src=TREATY (last access: 12.01.2025).
33. UN General Assembly. (2005). Basic Principles and Guidelines on the Right to a Remedy and Reparation. A/RES/60/147.
URL: https://legal.un.org/avl/pdf/ha/ga_60-147/ga_60-147_ph_e.pdf (last access: 12.01.2025).
34. UN Human Rights Committee. (2011). General Comment No. 34 on Freedoms of Opinion and Expression. U.N. Doc. CCPR/C/GC/34.
URL: https://www2.ohchr.org/english/bodies/hrc/docs/gc34.pdf (last access: 12.01.2025).
35. UNESCO. (2021). Recommendation on the Ethics of Artificial Intelligence. Paris: UNESCO.
URL: https://www.unesco.org/en/articles/recommendation-ethics-artificial-intelligence (last access: 12.01.2025).
36. United Nations. (2001). Articles on Responsibility of States for Internationally Wrongful Acts. U.N. Doc. A/RES/56/83.

URL:https://legal.un.org/ilc/texts/instruments/english/commentaries/9_6_2001.pdf (last access: 10.01.2025).

37. United Nations. (2023). Secretary-General announces creation of new AI advisory board URL: https://press.un.org/en/2023/sga2236.doc.htm (last access: 08.01.2025).

38. Zuboff, S. (2019). The age of surveillance capitalism: The fight for a human future at the new frontier of power. PublicAffairs.

URL: https://www.hbs.edu/faculty/Pages/item.aspx?num=56791 (last access: 09.01.2025).

Date of receipt of the article in the Editorial Office
(23.01.2025)