35. JURISPRUDENCE

PROTECTING HUMAN RIGHTS IN THE ERA OF ARTIFICIAL INTELLIGENCE: INTERNATIONAL LEGAL PERSPECTIVES ON NON-DISCRIMINATION AND THE RIGHT TO PRIVACY

Oleksandr Zhyhaliuk,
Fourth Year Student Majoring for Bachelor Degree
7981897@stud.kai.edu.ua
Department of International and European Law
Faculty of Law and International Relations
State University "Kyiv Aviation Institute"
Kyiv, Ukraine

Koropatva Anastasiia,
Fourth Year Student Majoring for Bachelor Degree
7922893@stud.kai.edu.ua
Department of International and European Law
Faculty of Law and International Relations
State University "Kyiv Aviation Institute"
Kyiv, Ukraine

Vasylyshyna Nataliia,
Dr.Sc. in Pedagogics, Professor,
Professor of the Foreign Languages and Translation Department
Scientific Secretary of the Academic Council
of the Faculty of Law and International Relations
nataliia.vasylyshyna@npp.kai.edu.ua
Foreign Languages and Translation Department
Faculty of Law and International Relations
State University "Kyiv Aviation Institute"
Kyiv, Ukraine

Abstract. Today we are witnessing the unprecedented integration of artificial intelligence (AI) systems into all areas of public life—from government services and criminal justice to the private sector (credit scoring, automated hiring, targeted advertising, medical diagnostics). Simultaneously, these technologies introduce new systemic risks to fundamental human rights enshrined in the Universal Declaration of Human Rights (1948), the International Covenant on Civil and Political Rights (1966), and regional instruments. Particularly, serious are violations of the right to respect for private and family life (Art. 12 UDHR, Art. 17 ICCPR, Art. 8 ECHR) and the principle of non-discrimination (Arts. 2 & 26 ICCPR, Art. 14 ECHR, ICERD 1965, etc.). Algorithmic bias, mass profiling, automated decisions without sufficient human oversight, real-time biometric surveillance, and inferential data already cause discriminatory outcomes and significantly erode privacy. Traditional international

human rights mechanisms, developed in the pre-digital era, are inadequate against the speed, scale, and opacity of algorithmic processes.

Key words: human right, human rights law, proportionality principle, limitation of human rights, legitimate aim, necessity and suitability, balancing test, judicial review, rule of law, democratic society.

Purpose and Research Objectives: a comprehensive analysis of the current state of international legal regulation of the protection of the right to privacy and the principle of non-discrimination in the context of the application of artificial intelligence systems, identification of gaps in the existing normative framework, and formulation of proposals for improving universal and regional standards.

Objectives: to systematize the main risks of human rights violations associated with the lifecycle of AI systems; to conduct a comparative legal analysis of universal (UN, UNESCO) and regional (Council of Europe, EU) regulatory instruments; to assess the dynamics of the transition from soft law to legally binding norms; to identify key gaps and systemic challenges; and to propose directions for the further development of international human rights law in the context of digitalization.

The greatest threats to the right to privacy posed by AI systems include mass collection and processing of personal data without proper informed consent; creation of detailed digital profiles through behavioral profiling and predictive analytics; use of real-time biometric identification in public spaces; and inference of sensitive information from seemingly neutral datasets (e.g., online activity, typing patterns, movement data) [2].

Regarding the principle of non-discrimination and equality, the main risks involve the transfer of historical biases from training datasets into AI models (for example, lower facial recognition accuracy for people with darker skin); indirect discrimination through proxy indicators (such as postal codes reflecting socio-economic or ethnic background); reinforcement of the digital divide between developed and developing states; and discriminatory effects of automated decisions in high-risk areas such as lending, employment, criminal justice, and social benefits [2].

The first global step in international regulation was the UNESCO Recommendation on the Ethics of Artificial Intelligence (2021), which enshrined principles of privacy, fairness, non-discrimination, transparency, and bias mitigation. Although it is a soft law instrument, it has become an important normative benchmark [2].

A major breakthrough was the Framework Convention of the Council of Europe on Artificial Intelligence and Human Rights, Democracy and the Rule of Law, adopted on 17 May 2024 and opened for signature on 5 September 2024 in Vilnius. As of February 2026, it has been signed by more than 40 states and the European Union. The Convention establishes binding standards on privacy, data protection, equality, and non-discrimination, introduces a risk-based approach, and requires safeguards throughout the AI lifecycle [3].

At the EU level, Regulation (EU) 2024/1689 (AI Act), in force since 1 August 2024, prohibits unacceptable-risk systems (including social scoring and certain biometric uses) from February 2025 and applies core obligations to high-risk systems

from August 2026. It requires fundamental rights impact assessments, transparency, explainability, and redress mechanisms [4].

At the universal level, important contributions include UN General Assembly resolutions (78/265, 79/239), reports of the UN Working Group on Business and Human Rights, and the work of Special Rapporteurs on privacy and racism [3].

However, the main problems today remain several key gaps in international law regulating artificial intelligence (AI) in the context of human rights protection:

1. Absence of a universal binding international treaty under the UN. International human rights law on AI relies mainly on non-binding "soft law," such as the 2021 UNESCO Recommendation on the Ethics of AI, OECD principles, UN General Assembly resolutions (e.g., 78/265, 79/239), reports from the UN Working Group on Business and Human Rights, and the 2024/2025 High-level Advisory Body report "Governing AI for Humanity," which highlights a global governance deficit. These instruments affirm principles of privacy, non-discrimination, transparency, and accountability but lack enforceability, allowing states to ignore or selectively apply them.

2. Regional fragmentation of standards. The EU and Council of Europe establish high standards. In contrast, many regions (Asia, Africa, Latin America, parts of the US) have no regulation or only voluntary/sectoral rules. This fosters a "race to the bottom," where companies shift high-risk AI to low-protection jurisdictions, leaving citizens outside Europe without effective safeguards against discrimination or privacy violations. Reports (e.g., Freedom Online Coalition 2025) warn that fragmentation worsens inequality and the digital divide.

3. Limited application to the private sector in the Council of Europe Framework Convention. Article 3 fully covers the public sector and state-linked private entities, but for other private actors (e.g., Google, Meta, OpenAI), states may apply weaker "appropriate measures" or opt out via reservations. This leaves commercial AI protection dependent on national laws, creating "double standards" compared to the directly applicable EU AI Act.

4. Excessively broad exemptions for national security and defense. Both the Framework Convention (Art. 3.2) and EU AI Act exclude AI systems tied to national security or defense across their entire lifecycle.

5. Uncertainty in liability for algorithmic bias harm. No clear international rules assign responsibility (developer, data provider, deployer, or state). The Framework Convention calls for accountability and redress but lacks specifics. Victims struggle to prove causation or secure remedies due to missing global explainability and audit standards.

6. Challenges of extraterritoriality and global AI supply chains. AI involves global data, development (often in the US), and deployment worldwide. The EU AI Act has extraterritorial reach, but most jurisdictions do not. Global supply chains complicate bias control, privacy enforcement, and liability, leading to norm conflicts and regulatory gaps in developing countries (per Brookings, CIGI, UN Advisory Body reports).

7. Lack of effective global redress mechanisms for victims. No universal forum exists for algorithmic harm (e.g., discrimination in hiring/lending or privacy breaches

via profiling). The Framework Convention mandates national remedies, but transnational access remains limited to UN special rapporteurs or regional courts (e.g., ECHR). Vulnerable groups especially lack real justice, rendering protection largely declarative (OHCHR, Freedom Online Coalition 2025, CoE reports) [4].

In our view, the key step should be the initiation of negotiations on a universal UN convention on human rights and artificial intelligence, modeled on the Council of Europe Framework Convention. Also necessary are: development of binding international standards for algorithmic impact assessments that necessarily take into account non-discrimination and privacy; harmonization of requirements for transparency, explainability, and independent auditing of AI models; creation of an international monitoring and redress mechanism for victims of algorithmic harm; strengthening the role of UN special procedures in the field of AI; integration of non-discrimination and data protection principles into technical standards (ISO, IEEE) and public procurement.

Contemporary international human rights law is at a turning point: from UNESCO's ethical recommendations to the first legally binding instruments—the Council of Europe Framework Convention and the EU AI Act. These documents create important precedents; however, without a universal binding treaty under the UN, algorithmic discrimination and the erosion of privacy risk becoming systemic phenomena. Therefore, further harmonization of standards, strengthening of liability mechanisms, and the creation of effective protection tools are not only a scientific but also a moral imperative of modern legal science.

REFERENCES:

1. United Nations. (1948). Universal Declaration of Human Rights (UDHR).https://www.un.org/en/about-us/universal-declaration-of-human-right s

2. UNESCO. (2021). Recommendation on the Ethics of Artificial Intelligence. Adopted by the General Conference at its 41st session. Paris:UNESCO.https://unesdoc.unesco.org/ark:/48223/pf0000380455.

3. Council of Europe. (2024). Framework Convention on Artificial Intelligence and Human Rights, Democracy and the Rule of Law (CETS No. 225). https://www.coe.int/en/web/artificial-intelligence/the-framework-convention-o n-artificial-intelligence

4. European Union. (2024). Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonised rules on artificial intelligence (Artificial Intelligence Act) and amending certain Union legislative acts. https://eur-lex.europa.eu/eli/reg/2024/1689/oj