Modern American Journal of Business, Economics, and Entrepreneurship
ISSN (E): 3067-7203
Volume 2, Issue 6, June, 2026
Website: usajournals.org

INTERNATIONAL LEGAL STANDARDS AND ETHICAL PRINCIPLES FOR REGULATING ARTIFICIAL INTELLIGENCE IN THE FIELD OF INFORMATION SECURITY

Sayfullayeva Venera Nimatjonovna
PhD Candidate, Teacher,
The University of World Economy and Diplomacy
ORCID: 0009-0005-9796-1223
ORCID: https://orcid.org/0009-0005-9796-1223
venera@uwed.uz

Abstract

One of the main problems of international legal regulation of artificial intelligence within the framework of international law is the definition of international standards and ethical principles for the use of artificial intelligence. International standards and ethical principles are still being deeply debated by international law entities. World leaders and heads of state emphasize the ethics of artificial intelligence, maintaining a balance between technological progress and security, avoiding discrimination as a result of the use of technologies, and maintaining human control over technologies. This article is devoted to the legal analysis of international standards and ethical principles regulating artificial intelligence. The article puts forward the theory of developing imperative norms that ensure compliance with ethical principles and international standards in the international legal regulation of artificial intelligence.

Keywords: Artificial intelligence, international legal regulation of artificial intelligence, ethical principles, international standards, phishing, deepfake fraud, adaptive and polymorphic malware, automated vulnerability scanning, information security, technical risks and threats.

Modern American Journal of Business, Economics, and Entrepreneurship
ISSN (E): 3067-7203
Volume 2, Issue 6, June, 2026
Website: usajournals.org

Introduction

In the field of information security, there are ethical issues regarding the balance between the use of artificial intelligence and human rights, data privacy, algorithmic transparency and liability for errors. In an era of advanced artificial intelligence, new modern threats are emerging in the field of information security under the influence of artificial intelligence, namely, attacks on the AI system itself (adversarial AI). Currently, using artificial intelligence as a tool for cyberattacks, artificial intelligence is used to counter offensive threats such as hyper-personalized phishing, deepfake, fraud, adaptive and polymorphic malware, automated vulnerability scanning, and threats against artificial intelligence systems: direct and indirect rapid injection, data poisoning, model inversion (decoupling), and excessive agency. Preventing these types of threats and ensuring data integrity is one of the most important tasks of the information security sector. Information security needs international standards and ethical norms to ensure the confidentiality, integrity and availability of information. In our opinion, the establishment of international legal standards and ethical requirements in the international legal regulation of artificial intelligence in the field of information security will create an opportunity not only to use the advantages of artificial intelligence, but also to prevent negative consequences affecting human rights as a result of irresponsible use.

Main part

The establishment of ethical principles for artificial intelligence and ensuring information security around the world is a key aspect of international standards (ISO). In practice, international standards are considered as documents that define abstract ethical principles. It is no exaggeration to say that international standards provide organizations with a legal framework for the responsible and ethical development and use of artificial intelligence systems. This is because international standards require compliance with ethical principles in the use of artificial intelligence, and serve as an effective safeguard in ensuring information security. International standards aim to eliminate risks before technological disasters arise.

Modern American Journal of Business, Economics, and Entrepreneurship
ISSN (E): 3067-7203
Volume 2, Issue 6, June, 2026
Website: usajournals.org

International standards

Given the complexity of data and security, the increasing capabilities of AI demonstrate the need for responsible and ethical AI standardization. International standards are developed by **the International Organization for Standardization, Joint Technical Committee (JTC) Information Technology Subcommittee (SC) 42 of the International Electrotechnical Commission (ISO/IEC).** SC 42 has established relations with **UNESCO, the Organization for Economic Cooperation and Development (OECD), and the European Commission**. The Subcommittee includes representatives from the United States, the United Kingdom, Germany, China, the Russian Federation, and Kazakhstan as full members, as well as Uzbekistan, Belarus, and other countries as observers. Currently, there are the ISO/IEC 42001:2023 standard "Artificial Intelligence Management System" [1], the ISO/IEC 22989:2022 standard "Artificial Intelligence Concepts and Terminology" [2], the ISO/IEC 23053:2022 standard "Fundamentals of Artificial Intelligence Using Machine Learning" [3], and the ISO/IEC TR 24030 "Technical Report on Artificial Intelligence Use Cases" [4].

According to the ISO/IEC 22989:2022 standard "Information Technology-Artificial Intelligence-Artificial Intelligence Concepts and Terminology", which provides standardized concepts and terminology to help a wider range of stakeholders better understand and use artificial intelligence technology, artificial intelligence is a highly interdisciplinary field that draws extensively on computer science, data science, natural sciences, humanities, mathematics, social sciences, and others. The standard defines an AI system as an engineering system that generates outputs such as content, predictions, recommendations, or decisions for a set of human-defined goals. This standard provides detailed information about the AI system lifecycle and data management concepts.

The ISO/IEC 27001 is the world's most popular standard for information security management systems (ISMS). This international standard defines the requirements that information security management systems must meet. The ISO/IEC 27001 standard provides guidance to companies of all sizes and in all sectors of activity on how to establish, implement, maintain and continually improve an information security management system. Compliance with

Modern American Journal of Business, Economics, and Entrepreneurship
ISSN (E): 3067-7203
Volume 2, Issue 6, June, 2026
Website: usajournals.org

ISO/IEC 27001 means that an organization or business has implemented a system to manage the risks associated with the security of the information it owns or processes, and that this system respects all the best practices and principles enshrined in this International Standard. With cybercrime on the rise and new threats constantly emerging, managing cyber risks may seem difficult - or even impossible. ISO/IEC 27001 helps organizations to identify risks and proactively address vulnerabilities. ISO/IEC 27001 promotes a holistic approach to information security (people, policy and technology review). An information security management system implemented in accordance with this standard is a tool for risk management, cyber resilience and operational excellence.

The world's first digital standard, ISO/IEC 42001:2023, which defines requirements for the creation, implementation and improvement of artificial intelligence and covers issues of ethics, security and transparency, is being developed by the Joint Technical Committee (ISO/IEC JTC 1) and the Subcommittee SC 42, specialized in artificial intelligence, at the initiative of the International Organization for Standardization (ISO) and the International Electrotechnical Commission (IEC).

According to the international standard, artificial intelligence can give rise to the following specific considerations:

-the use of artificial intelligence for automated decision-making, sometimes in a non-transparent and incomprehensible way, may require special management beyond the control of classic information and communication systems;

-the use of data analysis, insight and machine learning in the design of systems instead of human-coded logic increases the applicability of artificial intelligence systems and changes the way such systems are developed, justified and deployed;

-AI systems that continuously learn change their behavior during use.

Clause B.7.2 of the International Standard (Data for the development and improvement of AI systems) states that organizations should define, document and implement processes for managing data related to the development of AI systems. It offers the following guidance for implementation:

- the privacy and security implications of using data, some of which may be sensitive in nature;

Modern American Journal of Business, Economics, and Entrepreneurship
ISSN (E): 3067-7203
Volume 2, Issue 6, June, 2026
Website: usajournals.org

- the potential safety and security threats that may arise from developing AI systems that depend on data;
- transparency and accountability aspects, including the origin of the data and the ability to explain how the data is used to determine the output of the AI system, if the system requires transparency and accountability;
- the representativeness of the training data relative to the operational use case;
- accuracy and integrity of data.

The main benefits of implementing an AI management system in accordance with the ISO/IEC 42001:2023 standard include:

- AI governance: ensures the ethical and responsible use of AI;
- reputation management: increases trust in AI applications;
- AI governance: supports compliance with legal and regulatory standards;
- practical guidance: effectively manages AI-related risks;
- encourages innovation within defined boundaries.

The ISO/IEC 23894:2023 digital document provides guidance on how organizations that develop, deploy or use products, systems and services that use AI can manage risks, in particular those related to AI. The standard aims to help organizations integrate risk management into their AI-related activities and functions. It also describes the processes for effectively implementing and integrating AI risk management.

From a legal perspective, it is desirable to responsibly develop and deploy AI technologies in accordance with globally recognized standards that support safety, ethics, and public interest. This requires the development of a certification ecosystem, given the complexity of implementing international standards. This is because AI can improve the quality of systems, proactively address risks, and create a safer path for innovation.

Information security experts believe that organizations should consider combining the EU AI law, which sets out legal obligations and deadlines, with ISO/IEC 42001, which provides the operational framework and evidence needed to comply with them. If organizations can quickly demonstrate a credible management position that links the EU AI law and ISO/IEC 42001 (clear inventory and role mapping, GPAI data and controls, a test compliance file for high-risk candidates, and an AIMS that measures, reviews, and improves).

Modern American Journal of Business, Economics, and Entrepreneurship
ISSN (E): 3067-7203
Volume 2, Issue 6, June, 2026
Website: usajournals.org

The development and use of seemingly safe AI systems have significant impacts on individuals, groups of individuals, and society at large. To increase the transparency and trustworthiness of systems that use AI technologies, organizations that develop and use these technologies can take steps to ensure that affected stakeholders are adequately informed about these impacts. AI system impact assessments play an important role in a broader ecosystem of governance, risk, and compliance assessment activities that, together, can build trust and accountability. ISO/IEC 38507, ISO/IEC 23894, and ISO/IEC 42001 are important parts of this ecosystem. Performing AI system impact assessments and using their documented results is an integral part of building trustworthy and transparent AI systems at all organizational levels. To this end, ISO/IEC 42005:2025 provides guidance on how an organization can implement a process for completing such assessments and promotes a common understanding of the components needed to conduct an effective assessment. The standard supports transparency, accountability and trust in AI by helping organizations identify, assess and document potential impacts throughout the life cycle of an AI system. Artificial intelligence technologies also raise ethical concerns. ISO/IEC 42005 plays a key role in ensuring that these concerns are addressed responsibly. It provides guidance to organizations through structural impact assessments, enabling them to align AI development with values such as fairness, security and human-centered design [5].

International standards play an important role in addressing ethical issues. However, recent research and practice suggest that a separate "AI Ethics" code should be developed to fully address the ethical issues surrounding the use of AI. Due to growing global awareness, the focus AI ethics has shifted from philosophical to legal theories in 2023-2026. Establishing legal and technical standards and ethical principles for the ethics of artificial intelligence in order to protect human rights has become the most urgent task of international law entities, as the establishment of ethical principles is the most effective strategy for proactive risk reduction.

AI Ethics of the Organization for Economic Cooperation and Development. In May 2019, 42 countries adopted the first set of principles for ethical artificial intelligence from the Organization for Economic Cooperation and Development

Modern American Journal of Business, Economics, and Entrepreneurship
ISSN (E): 3067-7203
Volume 2, Issue 6, June, 2026
Website: usajournals.org

(OECD). The set includes five key OECD principles for AI, agreed upon by Argentina, Brazil, Colombia, Costa Rica, Peru and Romania [6]: Inclusive growth, sustainable development and prosperity, Human-centered values and fairness, Transparency and explanation, Clarity, robustness and cybersecurity, and Accountability [7]. In May 2024, the organization updated its principles, focusing on combating disinformation (deepfakes) and ensuring information security [8]. These principles include investing in AI research and development, developing an ecosystem that supports inclusive AI, creating a conducive, interoperable governance and policy environment for AI, building human capacity and preparing for labor market transformation, and principles for international cooperation for trustworthy AI.

AI Ethics of the UNESCO

In November 2019, the UNESCO General Conference, at its 40th session, adopted 40 C/Resolution 37, tasking the Director-General with "preparing an international standard-setting instrument in the form of a Recommendation on the Ethics of Artificial Intelligence," which will be considered by the General Conference at its 41st session in 2021. The "Recommendation on the Ethics of Artificial Intelligence" addresses ethical issues related to artificial intelligence to the extent that they fall within UNESCO's mandate. Artificial intelligence systems raise new ethical issues, including, but not limited to, impacts on decision-making, employment and labor, social interaction, healthcare, education, media, access to information, the digital divide, personal data and consumer protection, the environment, democracy, the rule of law, security and policing, dual use, as well as human rights and fundamental freedoms, including freedom of expression, privacy and non-discrimination. In addition, new ethical issues arise due to the potential of AI algorithms to reproduce and reinforce existing biases, while reinforcing existing discrimination, prejudice and stereotypes. To address these ethical challenges, UNESCO proposes ethical principles focused on Proportionality and Non-Harm, Safety and Security, Fairness and Non-Discrimination, Sustainability, Privacy and Data Protection, Human Control and Resilience, Transparency and Explanation, Responsibility and Accountability, Awareness and Literacy, Multi-Stakeholder and Adaptive

Modern American Journal of Business, Economics, and Entrepreneurship
ISSN (E): 3067-7203
Volume 2, Issue 6, June, 2026
Website: usajournals.org

Governance and Collaboration [9]. In 2025, UNESCO adopted a Readiness Assessment Methodology and set out its goals for ethical governance to ensure that AI technologies do not violate human rights and contribute to sustainable development [10].

AI Ethics of the European Union

On 8 April 2019, the High-Level Expert Group on Artificial Intelligence presented the "Ethical Guidelines for Trustworthy Artificial Intelligence". According to the guidelines, trustworthy AI should be legal – complying with all applicable laws and regulations; ethical – adhering to ethical principles and values, and robust from a technical perspective, taking into account its social environment [11].

The 2022 European Declaration on Digital Rights and Principles for the Digital Decade, in Chapter 3, paragraph 9(a), calls for promoting human-centered, trustworthy and ethical artificial intelligence, and in paragraph f, calls for measures to be taken to ensure that research in the field of artificial intelligence complies with the highest ethical standards and relevant EU law [12].

Since the above documents set out rules for compliance with ethical principles and values, the EU's 2024 Artificial Intelligence Law essentially states that this law should promote human-centered, trustworthy and ethical artificial intelligence, and that Article 60(3) requires measures to ensure that research in the field of artificial intelligence complies with the highest ethical standards and relevant EU law [13].

Conclusion

International standards play an important role in solving ethical problems. However, recent scientific research and practice emphasize the need to develop a separate "Artificial Intelligence Ethics" code to fully address the ethical problems of using artificial intelligence. Due to growing global awareness, the development of ethical principles of artificial intelligence ethics in 2023-2026 has moved from philosophical views to legal theories. Establishing legal and technical standards and ethical principles of artificial intelligence ethics in order to protect human rights has become the most urgent task of international law

Modern American Journal of Business, Economics, and Entrepreneurship
ISSN (E): 3067-7203
Volume 2, Issue 6, June, 2026
Website: usajournals.org

entities. Because the establishment of ethical principles is the most effective strategy for proactive risk reduction.

The use of artificial intelligence in information security raises ethical issues (discrimination, black box problem-transparency, confidentiality and data collection, allocation of responsibility, dual use, over-reliance) related to trust in automated decisions, protection of privacy and liability for potential errors. In particular, the protection and maintenance of the confidentiality of personal data demands clear ethical principles.

Scientific research currently shows that the use of artificial intelligence in ensuring information security in a cross-section of industries (finance, economics, medicine, education) provides effective results. In our opinion, ethical principles should be established and a "Code of Ethics" should be developed for the use of artificial intelligence in the fields of medicine, education, and finance.

References

1. ISO/IEC 22989:2022(en) Information technology — Artificial intelligence — Artificial intelligence concepts and terminology // https://www.iso.org/obp/ui/en/#iso:std:iso-iec:22989:ed-1:v1:en
2. ISO/IEC 42001:2023 Система менеджмента искусственного интеллекта // https://media.eurocert.gr/images/0/0/certifications/iso_42001_2023_rus.pdf
3. ISO/IEC 23894:2023 Information technology — Artificial intelligence — Guidance on risk management // https://www.iso.org/standard/77304.html
4. ISO/IEC 42005:2025(en) Information technology — Artificial intelligence (AI) — AI system impact assessment // https://www.iso.org/obp/ui/en/#iso:std:iso-iec:42005:ed-1:v1:en
5. OECD Released New AI Principles: How Will They Impact the Ethics of AI? Daniel Newman (2019) // https://futurumgroup.com/insights/oecd-ai-principles/
6. OECD AI Principles // https://documentations.seclea.com/seclea-user-documentation/supported-ai-regulations/oecd-ai-principles

Modern American Journal of Business, Economics, and Entrepreneurship
ISSN (E): 3067-7203
Volume 2, Issue 6, June, 2026
Website: usajournals.org

7. UNESCO Recommendation on the Ethics of Artificial Intelligence SHS/BIO/REC-AIETHICS/2021 // https://unesdoc.unesco.org/ark:/48223/pf0000380455
8. European Declaration on Digital Rights and Principles POLICY AND LEGISLATION Publication 15 December 2022 // https://digital-strategy.ec.europa.eu/en/library/european-declaration-digital-rights-and-principles
9. UNESCO Recommendation on the Ethics of Artificial Intelligence SHS/BIO/REC-AIETHICS/2021 // https://unesdoc.unesco.org/ark:/48223/pf0000380455
10. Launching the Readiness Assessment Methodology in Uzbekistan for the UNESCO Recommendation on the Ethics of Artificial Intelligence 2025 // https://www.unesco.org/en/articles/launching-readiness-assessment-methodology-uzbekistan-unesco-recommendation-ethics-artificial
11. TechDispatch #2/2023 - Explainable Artificial Intelligence 2023 // https://www.edps.europa.eu/data-protection/our-work/publications/techdispatch/2023-11-16-techdispatch-22023-explainable-artificial-intelligence_en
12. European Declaration on Digital Rights and Principles POLICY AND LEGISLATION Publication 15 December 2022 // https://digital-strategy.ec.europa.eu/en/library/european-declaration-digital-rights-and-principles
13. Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonised rules on artificial intelligence and amending Regulations (EC) No 300/2008, (EU) No 167/2013, (EU) No 168/2013, (EU) 2018/858, (EU) 2018/1139 and (EU) 2019/2144 and Directives 2014/90/EU, (EU) 2016/797 and (EU) 2020/1828 (Artificial Intelligence Act) (Text with EEA relevance) PE/24/2024/REV/1 // https://eur-lex.europa.eu/eli/reg/2024/1689/oj/eng