MODERN APPROACHES TO THE LEGAL REGULATION OF ARTIFICIAL INTELLIGENCE IN THE FIELD OF INFORMATION SECURITY

DOI: 10.63407/738884

NUGMAN NUGMANOV
Professor of the Department of International Law and Public Law Disciplines, UWED.

VENERA SAYFULLAYEVA
Doctoral researcher of UWED

Abstract. *Within the framework of international law, the legal regulation of artificial intelligence (AI) and the development of ethical standards governing its application remain among the most pressing challenges. When examining the issue of regulating AI in the field of information security, several key concerns emerge: the protection of algorithms and neural networks, the degree of data transparency, the functioning and accountability of AI and information agents, the security implications of using Chat GPT and other chatbots, the impact of AI-driven robotics and emerging AI technologies on human rights in the digital era, questions of international responsibility, and the broader challenges of information security. The aim of this article is to conduct a comprehensive analysis of different state approaches and offers conclusions on proposing a distinctive national approach for Uzbekistan that is scientifically grounded, compatible with the country's legislation and legal norms, and responsive to the requirements of modern times. The conclusion provides a broad overview of the legal framework for defining the international legal approach to artificial intelligence in the field of information security. The conclusion provides the reasons for the international legal gaps in the development of international legal approaches to artificial intelligence in the field of information security, as well as proposals and conclusions for the development of a legal approach.*

Keywords. *artificial intelligence; international legal regulation; approaches of AI; AI principles, information security; Chat GPT; neural networks; data transparency; protection of algorithms; chatbots, human rights in the digital era; AI-driven robotics; algorithmic hallucination; legal hypotheses; cybersecurity; sandbox; a high-risk AI system.*

Introduction.

International legal issues concerning information security remain a pivotal focus of contemporary international law. The expanding capabilities of Artificial Intelligence (AI) and its burgeoning impact on security frameworks are compelling the international community to address the legal challenges of regulating AI technologies. In this context, the primary objective remains the establishment of new, peremptory international principles and

conventions. Furthermore, fostering international cooperation is essential for the peaceful resolution of cyberspace conflicts in accordance with international law, the optimization of information exchange, the reduction of "information weaponry" and the protection of data privacy.

The Global Cybersecurity Outlook 2025 report provides a deeper analysis of the most important drivers of complexity and provides valuable insights into the most pressing cyber challenges and their potential implications for leaders in the coming year. 71 percent of Chief Risk Officers (CROs) surveyed by the Global Cybersecurity Outlook (GCO) report that cyber risks have increased. The survey found that cybercrime is increasing in both frequency and sophistication, with ransomware attacks, AI-enhanced tactics – phishing, vishing and deepfakes – and a significant increase in supply chain attacks. This Visual Review reports a lack of cyber resilience (The Global Cybersecurity Outlook report 2025):

Fig 1. A visual overview of the reporting insufficient cyber resilience.

Within the framework of international law, scholars define information security as a state in which the vital interests of individuals, society, and the state are protected from information-driven threats that impede sustainable development. This definition encompasses the resilience of information infrastructure, including Information and Communication

Technologies (ICT) and the data therein (Nugmanov N.A 2023). There is an emphasized need for a harmonized international legal framework to govern interstate relations in the sphere of global information exchange. Such a framework, adapted to the rapidly evolving technological landscape, aims to eliminate regulatory lacunae in the dissemination of information and ensure robust national and international information security through the oversight of international organizations (Nugmanov N.A 2015)

To date, there has been no clearly defined approach developed and applied by states to the legal regulation of artificial intelligence (AI) in the field of information security based on international legal norms and principles. The absence of a legal definition for the concept of artificial intelligence, the lack of established legal norms determining the boundaries of its use by subjects of international law, the vulnerability of AI due to potential risks, and phenomena such as algorithmic hallucination influence the development of a clear approach within international law.

At present, numerous scientific studies in the European Union, the USA, China, and Russia examine the legal regulation of artificial intelligence through the approaches of the European Union, the United States, China, and Russia. In recent years, the experience of foreign countries has demonstrated the emergence of modern models of such approaches. This paragraph presents a scientific analysis of contemporary approaches to the legal regulation of artificial intelligence in the context of Arab states, the African Union, the Commonwealth of Independent States (CIS), and Central Asia, along with legal hypotheses derived from these findings.

Scope of Research

Within the scope of this research, we emphasize several key elements:

Firstly, concerning the field of information security, artificial intelligence (AI) proposes an international legal approach within international law. This is achieved through a deep scientific analysis of foreign experience, aiming to address legal and ethical issues, develop international legal approaches to AI, and define a unified international legal mechanism.

Secondly, in the realm of international law, the research scientifically analyzes the necessary importance of transformation and modernization processes in the field of information security. This includes identifying internal and external political and legal factors of states influencing the development of international legal regulation mechanisms for AI.

Thirdly, the study establishes a clear legal approach for the creation of modern technical mechanisms to protect human rights and freedoms. This addresses the risks of data privacy breaches and racial and gender discrimination (bias) arising from the use of AI technologies in information security.

Fourthly, it demonstrates the importance and impact of applying a European approach to ensure the security of personal data, cross-border data exchange, the international legal basis for data security, and to establish legal liability for illegal acts during data acquisition, reception, and distribution.

Fifthly, based on the experience of China, the USA, Europe, and the CIS countries, the research proposes ideas for defining specific international legal principles in regulation and applying these principles in an international approach to fill legal gaps related to AI and information security in international law.

Sixthly, the research highlights legal hypotheses such as the international ethical aspects of AI use, specifically the integration of analytical ethical norms proposed as a result of scientific research into the imperative norms of international law.

Seventhly, it proves that AI in the field of information security is a global turning point (phenomenon), that the balance of law in regulating rapidly developing technologies has been lost, and that this is one of the necessary factors for developing legal approaches.

Eighthly, the legal approach covers the study of problems such as ensuring data privacy and cybersecurity when applying AI technologies in various fields (economy, advertising, banking, services, medicine, transport, agriculture, production, insurance, law enforcement, and judicial bodies).

Literature Review

Certain doctrinal perspectives and scholarly studies categorize legal approaches to artificial intelligence into two main

approaches: universal (proactive) and targeted approaches, which are designed for specific systems and sectors. The universal approach envisions the establishment of a comprehensive legal regime for the use, production, and development of AI, adopted by states at a broad level. The targeted approach, in contrast, requires the development of specific sectoral regulations that take into account the type, nature, and scope of AI used in the particular sector, as well as the interests of the state and society. The conceptualization of artificial intelligence is grounded in various theories, such as the knowledge-based view, the theory of the social present, the Unified Theory of Acceptance and Use of Technology (UTAUT), Social Response Theory (SRT), Social Cognitive Theory (SCT), and the Uses and Gratifications Theory (UGT). Each AI model may have distinct potential applications, challenges, and limitations in supporting specific classical policy frameworks (Kingsley Ofosu-Ampong 2024).

The Joint Research Centre (JRC) is actively studying new AI applications, such as deep learning models (deepfakes), to enhance data processing, analysis, and early warning capabilities. In doing so, the research center relies on experience derived from the most advanced statistical and digital models (GRABOVA, O., URSO, G., CORBANE, C., DALMASSO, S., KEMPER 2025).

The results of our scientific analysis suggest that future legal approaches to regulating artificial intelligence in the field of information security should be grounded in the opinions and expert analyses of representatives of the exact sciences. This is because AI, by nature, is grounded in the exact sciences and expert analysis. Therefore, the development of legal regulatory norms must rely on rigorous scientific research conducted by specialists, rather than merely on social perceptions. Rules and principles should be established based on precise statistical analyses and the results of testing conducted by reputable research centers.

Core issue

The increase in cyberattacks, deep spoofing, voice cloning, synthetic fraud in the use of information systems, the emergence of malicious programs, training kits filled with false information, the weakness of information protection and the increase in technological difficulties, operational gaps in information exchange in the field of information security are pushing for the development of legal approaches to artificial intelligence

technologies in the field of information security. The rapid development of ICT technologies and the weakness of the legal sphere in the development of regulatory rules, the inability of stakeholders to reach an agreement and lack of consensus, the diversity of legal and ethical norms, the lack of development of the concept of artificial intelligence and transparency, the presence of legal gaps in international law at the global level, the weakness of mechanisms for cross-border information exchange have a significant negative impact on the development of a legal approach by the international community.

Scientific research on the European Union approach to legal regulation of AI.

The European Union distinguishes itself from other approaches by adhering to the principles of a universal system and by developing a comprehensive legal regime for artificial intelligence. Numerous scientists state that the European Union's approach has proven to be effective. The Artificial Intelligence Act developed by Natalie Smuha also encompasses general-purpose AI models. Although these were not part of the initial draft of the regulation, the rapid spread of generative artificial intelligence—especially after the launch of ChatGPT in November 2022—motivated the European Union to introduce obligations for providers of such AI models. In summary, these obligations require developers to prepare and maintain technical documentation, comply with the European Union's copyright legislation, and provide brief information about the data used in training their models. Smuha emphasizes that if a model is considered to pose a "systemic risk," it becomes necessary to conduct a model evaluation, ensure detailed reporting, disclose significant risks, and guarantee cybersecurity. Systems that do not fall within these categories are exempt from new requirements. In her view, the Artificial Intelligence Act reflects the essence of product safety law: the higher the risk posed by the system, the stricter the applicable requirements (Nathalie A. Smuha 2025)

According to Anna Pirozzoli, the European Union aims to promote the ethical and responsible use of artificial intelligence through effective regulations and investments in digital education. A cautious approach to AI implementation, along with the inclusion of various stakeholders, is crucial to maintaining a balance between innovation and societal principles. By adopting this approach, it becomes possible to strike a harmonious balance

between technological development and the protection of human well-being. Although artificial intelligence offers fascinating technological opportunities, it is essential to remember that humans should remain at the center of all regulatory efforts. It is essential to recognize that people are not only the beneficiaries of AI development but also its architects. To ensure that artificial intelligence contributes to the welfare of society, it is necessary to maintain a balance that relies on human intelligence, wisdom, and rational reasoning (Anna Pirozzoli 2024, p 105-116).

Miguel Angel Presno Linera argues that the European Union should employ a risk-based approach, which tailors the type and content of its regulations to the intensity and scope of potential risks posed by artificial intelligence systems. He also emphasizes that this approach is closely linked to the EU's well-known "precautionary principle", which guides much of its regulatory activity (Miguel Ángel Presno Lineraa, Anne Meuwese 2025). The researcher correctly highlights the EU's adherence to this principle, as the Union requires that for high-risk AI systems, a risk management system must be established, implemented, documented, and maintained. According to the Artificial Intelligence Regulation, a risk management system is defined as a continuous and repetitive process that must be planned and carried out throughout the entire lifecycle of a high-risk AI system, requiring regular systematic review and updating. In accordance with the regulation, potential additional risks are to be assessed based on the analysis of data collected through an appropriate monitoring system (Regulation (EU) 2024/1689).

Research on the American approach to AI regulation

Lori Harris suggests that the U.S. federal government's approach focuses more on monitoring its own use of artificial intelligence rather than regulating the use of AI in the private sector. From the perspective of regulatory approaches, she proposes that federal activity in the area of artificial intelligence can be broadly categorized into three areas: direct regulation of AI technologies, regulation of AI use across various sectors, and regulation of AI use within specific industries (Laurie Harris 2025).

Harris's views on sectoral regulation are well-founded. According to expert analyses by AI specialists Yingjie Hu, Wenwen Li, Dawn Wright, Orhun Aydın, legal approaches play a crucial role in balancing risks associated with artificial intelligence. Considering that transnational crimes—including cybercrime (such as hacking,

fraud, and the dissemination of malware) and terrorism (criminal acts committed for political purposes at the international level)—are typically based on the misuse of confidential information, there is a clear need for legislation that ensures data protection and encryption measures (Yingjie Hu, Wenwen Li, Dawn J Wright, Orhun Aydin 2019).

In her scholarly works, Tatevik Davtyan notes that the U.S. approach to AI regulation reflects ongoing efforts to strike a balance between innovation and the responsible management of AI-related risks. She argues that in order to maintain global leadership, the United States must move beyond executive actions and prioritize robust legislative solutions that codify essential safeguards while promoting innovation and cross-border cooperation (Tatevik Davtyan 2025).

In our view, legal approaches play a crucial role in balancing risks associated with artificial intelligence. Considering that transnational crimes—including cybercrime (such as hacking, fraud, and the dissemination of malware) and terrorism (criminal acts committed for political purposes at the international level)—are typically based on the misuse of confidential information, there is a clear need for legislation that ensures data protection and encryption measures.

Marcin Szchepanski examines the political dimensions (Republican and Democratic perspectives) of legal approaches to artificial intelligence, emphasizing the necessity of data privacy legislation to ensure the creation of effective and sustainable AI systems. His views are considered both timely and significant. In the era of globalization, ensuring data confidentiality has become one of the most critical tasks facing every state. According to our scientific projections, as geopolitical tensions, international relations, and AI technologies continue to evolve, it is expected that a new stage of discussions will begin—focused on improving security operations in the processes of data collection, dissemination, and storage, as well as developing guidelines and rules to assess autonomous functions, AI-based deception, and insider threats. Therefore, it is necessary to establish an appropriate legal framework for regulating artificial intelligence in the field of information security and to develop technologically adaptive norms ensuring data privacy (Marcin Szczepański 2024).

Kasim Balarabe emphasizes the need to develop clear definitions and categories of cybercrimes and cyberwarfare in accordance

with international law, along with appropriate legal responses and enforcement mechanisms. He also explores the tensions between state sovereignty and global internet governance, proposing a balanced framework that supports states' legitimate security interests while upholding the fundamental principles of human rights, transparency, and multistakeholder cooperation (Kasim Balarabe 2025).

Isabella Brunner revisits the concept of cyber attribution by analyzing the impact of international law on cyberspace in the context of the so-called "Five Eyes" countries (Australia, Canada, New Zealand, the United Kingdom, and the United States), as well as Japan and China, taking into account recent political and legal developments in their national approaches. Furthermore, she provides an interpretation of the legal rules of attribution within the framework of international law (Isabella Brunner 2025, p 26-43).

Stefan R. Badza argues that future efforts should focus primarily on integrating artificial intelligence into the education system, investing significantly in research infrastructure, and strengthening international cooperation. He proposes approaches that demonstrate the ethical and legal foundations necessary to ensure the responsible use of artificial intelligence, taking into account potential differences and challenges. His conclusions are well-grounded, as the continuous support of the government, educational institutions, and the economic sector is essential for the further development and application of AI technologies within a country. Among the key challenges are the need to further regulate, educate, and enhance the infrastructure to ensure the safe and ethically acceptable use of artificial intelligence (Stefan R. Badža 2024). A study of Serbia's legal regulation of AI technologies and its measures to ensure information security in various sectors suggests that focusing on issues such as data confidentiality, the accuracy of AI-generated information, and the prevention of bias can lead to the development of effective guidelines for the appropriate use of artificial intelligence in relevant fields, yielding promising results (Namanja Sladaković, Bojan Tutić 2024).

China's Approach to AI Regulation

Huw Roberts, Josh Cowls, Jessica Morley, Mariarosaria Taddeo, Vincent Wang, and Luciano Floridi provided an extensive analysis of the structural, cultural, and political factors shaping China's

approach to artificial intelligence (AI). They emphasize that ethics plays a central role in China's AI policy. The AIDP outlines the intention to clearly define ethical norms and standards; however, efforts toward implementation remain in an early phase, largely confined to high-level principles and not yet realized in practice. Examining China's existing approaches, as well as the debates emerging in areas such as privacy and medical ethics, allows for an understanding of the types of frameworks that may arise. Regarding privacy, recently introduced protections may appear robust, with definitions of personal data even broader than those used in the GDPR. Nevertheless, upon closer inspection, numerous loopholes and exceptions emerge that enable the government (and indirectly approved companies) to bypass privacy protections, reflecting a lack of accountability and granting the government virtually unrestricted authority over mass surveillance decisions (Huw Roberts, Josh Cowls, Jessica Morley, Mariarosaria Taddeo,Vincent Wang, Luciano Floridi 2020).

N.V. Volodin identifies several risks associated with the use of AI systems, including breaches of data confidentiality, discrimination and bias, erroneous automated decisions with significant implications in fields such as medicine and law, cyber threats like data leaks, and unpredictable outcomes that may intensify existing challenges. The researcher notes that in China, neural networks are utilized in the development of legal documents, analysis of judicial practice, speech recognition, and processing of large volumes of diverse data within prosecutorial and judicial institutions. Consequently, Volodin argues that the legal framework regulating AI must evolve in tandem with technological development, taking into account its ethical aspects. It is also stated that in 2023, China introduced 24 regulations mandating the labeling and registration of algorithms (N.V. Volodin 2024, p 158-160). According to Tracey Tang, although both China and the US possess distinct legal frameworks, they should acknowledge that AI requires strict regulation concerning personal data and the use of algorithms (Tracey TANG 2025). Vladimirov emphasizes the need to establish clear boundaries of rights and obligations among parties involved in the creation, training, and use of AI systems and related services. He highlights the importance of studying how AI evolves under the influence of user-provided data, as well as the potential for AI to be deliberately trained on unlawful data to degrade its integrity or disseminate harmful content. He also notes the problematic factor of interaction between AI systems

operating independently out of human control across different jurisdictions (Vladimirov 2025, p 177-178).

Legal approaches of the Commonwealth of Independent States and its influence on new legislation

Sergey Lebedev recognizes the considerable potential of AI for the economic development of CIS countries and emphasizes the need for enhanced cooperation in this field. He asserts that collaboration in AI must develop within the framework of universally recognized principles and norms of international law. CIS member states, showing a sense of responsibility for the future of humanity, must ensure the proper protection of data during the creation and training of AI models, as well as maintain state oversight to prevent AI from making decisions involving ethical issues or matters related to human welfare and life.

Sergey Kruglikov underscores the importance of first reaching a consensus on conceptual frameworks before drafting legislation. Every project, he argues, requires a clear and realistic conceptual foundation that respects national interests. He highlights that a dictionary reflecting the fundamental concepts in the field of AI will play a significant role in the subsequent development of AI-related legislation.

Belarusian scholars participating in the CIS discussions on model laws and norms for AI technologies emphasize that legal regulation in this domain should both respect citizens' rights and ensure security while establishing fundamental approaches to governing the creation and application of AI technologies across various economic and social spheres. The researchers studied several fundamental issues arising from AI adoption, such as data ownership, privacy and protection, antimonopoly legislation concerns, data management to ensure high quality throughout its lifecycle, state intervention and personal data protection, civil and criminal liability, neutrality and impartiality of AI, and the use of AI in safeguarding national security (Ablomeyko S.V, Ablomeyko M.S, Belotserkovsky A.M, Golenkov V.V, Kasanin S.N, Kruglikov S.V, Minko N.S, Mikhaleva T.N (2024).

Gleb Lyannoy asserts that Western countries are striving to monopolize AI technologies as a means of exerting dominance over other nations. In contrast, Russia, China, and India occupy leading positions in promoting joint efforts toward the development and legal regulation of AI technologies. He argues

that administrative and legal institutions should oversee the regulation of AI technology development and that the state's regulatory role in this process should be expanded (Lyannoy 2024).

Chikvin A.B. draws attention to the challenges faced by CIS countries in adopting a unified code in his scientific analyses. By conducting a comparative study on the concepts of informatization, artificial intelligence, and information codes among CIS member states, he highlights the absence of comprehensive comparative legal analyses in current legislation. Furthermore, he identifies shortcomings in Russia's "Information Code" concept. According to him, the fragmentation of legislation—where existing regulatory documents do not form a coherent system—complicates the application of laws. Legal gaps persist, as many aspects of digital legal relations, such as the use of artificial intelligence and big data, remain fundamentally unregulated at the legislative level. Chikvin A.B. emphasizes the necessity of aligning Russian legislation in the fields of the digital economy and cybersecurity with international standards (Chikvin 2025).

According to Z.I. Khisamova and I.R. Begishev, the most appropriate approach among the existing ones is to establish a separate legal regulatory mechanism that clearly delineates areas of responsibility between AI system developers, users, and the technology itself. They stress the importance of implementing unified ethical principles for all AI developers and users. The researchers point to the Asilomar Principles as the most effective framework in this regard, suggesting that these principles could serve as a foundation for international mechanisms governing the legal regulation of AI development and implementation (Khisamova ZI, Begishev IR 2019).

N.Nugmanov and V.Sayfullaeva scientifically confirmed it is time to focus on ensuring Central Asia's information security by developing a unified mechanism for regulating artificial intelligence in the field of information security in Central Asia and concluding a multilateral regional agreement on information security and cybersecurity among Central Asian countries. (N.Nugmanov and V.Sayfullaeva 2026).

The Impact of AI on the Legislation of the United Arab Emirates (UAE) and Legal Approaches

Modafar Shaker Akhoirshieda, Ku Muhammad Naim Ku Khalif, and Suryanti Awang note that since 2018, scientific research on artificial intelligence has increased, and from 2019 onwards, publications on AI in the UAE's public sector have grown significantly. The researchers have found that AI studies in the UAE primarily focus on enhancing efficiency, reducing costs, improving decision-making and service delivery, and increasing safety and accuracy while minimizing human error. Identified challenges include data-related issues, privacy and security concerns, technical and infrastructural limitations, and user-centered barriers. They also observe that most existing research and publications have focused on automating the management of open data portals, adapting to dynamic state policies, and improving user experience in public services (Modafar Shaker Akhoirshieda, Ku Muhammad Naim Ku Khalif, Suryanti Awang (2024).

Adel Salem Al-Louzi, Karima Krim, and Mohammad Abdalhafid Al-Khamaiseh argue that the evolution of artificial intelligence and intelligent systems requires legal systems to respond not only by applying traditional doctrines of legal personality but also by developing frameworks specific to this innovative context (Adel Salem Allouzi, Karima Krim 2023).

Heva Abdulkhaleq Ahmad contends that the disruptive nature of artificial intelligence necessitates firmness, rationality, and design principles to prevent risks such as addiction to self-destructive behavior, scarcity-based competition, and unnatural inequality. The researcher views artificial intelligence as a dangerous technology, comparing unregulated AI to alarming prospects like nuclear weapons, bioengineering, and gene-editing technologies (Hewa Abdulkhaleq Ahmed, Hewa Abdulkhaleq 2025). In our opinion, author's focus on risks is well-grounded, as unregulated artificial intelligence possesses the potential to intensify nuclear conflicts, representing a modern, human-approved, yet covert weapon. Only comprehensive policies by state leaders aimed at mitigating these risks, along with transparency in AI operations and the assurance of information security, can help prevent such threats.

Islam Al Khatib attempted to conduct a scientific analysis of the political governance of artificial intelligence, highlighting the UAE's position against the background of regional geopolitical transformations, such as the U.S.–China competition and the

impact of Israel's military operations in Gaza. The researcher notes that the UAE is striving to strengthen its status as a leader in artificial intelligence, emphasizing that the country's efforts go beyond the sphere of political economy and are part of a broader strategy aimed at fostering growth and progress through extensive cooperation related to complex political relations and regional dynamics (Islam Al Khatib 2024).

African Approaches to AI and Information Security

Caroline Ncube, Isaak Rutenberg, Tobias Schonwetter, and Desmond Osaretin Oriaxogba, analyzing the issue from the perspective of data integrity through security, point out that despite Africa's achievements in data protection and cybersecurity, the level of adoption and effectiveness remains insufficient. The researchers note that within the African Union, only 15 out of 54 states have developed national cybersecurity strategies (laws), and the entry into force of the Malabo Convention in 2023 indicates the continent's general approach to regulating the digital world (Caroline Ncube, Isaak Rutenberg, Tobias Schonwetter, and Desmond Osaretin Oriaxogba 2024).

Benjamin C. Guinhouya, in his analysis of Kenya's Digital Health Act, explains that health data refers to a person's physical or mental condition, including past, present, or future medical records, information collected during medical services, or data linking an individual to specific healthcare services. According to him, persistent inefficiency in data management remains a major issue. Many healthcare systems still rely on paper documentation, which slows down diagnostic processes and hinders rapid decision-making during crises. However, despite their promising nature, such innovations pose significant challenges in terms of personal data protection and fair use of technology. Furthermore, in French-speaking countries, the processing and use of health data still require substantial progress (Benjamin C. GUINHOUYA 2024).

Mohammed Karimkhan Pathan and Aman Shah, in their research paper "Ethical Considerations and Responsible Governance of Generative Artificial Intelligence: A Systematic Analysis", use the "Crawford and Paglen" image dataset example to illustrate how real-world cases reveal the risks of inaccurate generative artificial intelligence. Their analysis shows that poorly selected datasets can lead to disproportionate errors in image recognition systems. For instance, such flaws may result in currency recognition models

that fail to identify currencies from certain regions, or license plate recognition systems that disproportionately misidentify vehicles belonging to minority groups. These cases highlight the ethical imperative of designing fair and inclusive artificial intelligence systems (Mohammed Karimkhan Pathan and Aman Shah 2025). In our view, the authors' arguments are valid. The existence of algorithmic errors demonstrates the need for a multifaceted approach. Providing clear explanations to ensure transparency and accountability is crucial, as the rapid development of technology means that generative AI, under the guise of technological advancement, can bring numerous hidden risks.

Executive Summary

Based on the aforementioned research, expert opinions, and empirical studies, the following conclusions can be drawn: The United States promotes innovative ideas and supports the development of guidelines and legislative initiatives to ensure the safety of AI. Although there is no unified federal law, it can be concluded that the country may develop a single safety model for artificial intelligence in the future. Moreover, in order to balance AI regulation with information security and data confidentiality, the U.S. is striving to develop unified standards across its diverse jurisdictions, grounded in national priorities and values. The rapid advancement of ChatGPT and generative AI has intensified competition between the U.S. and China for global leadership, significantly elevating American efforts on the global stage.

China's approach, by contrast, is distinguished by its speed and the effectiveness of state policies aimed at addressing AI-related challenges. However, the absence of potential stability in China's AI regulatory framework may hinder the activities of both domestic and foreign companies in developing the AI sector, attracting investment, and ensuring stability in the field of information security.

The Interparliamentary Assembly of the CIS is currently developing a model law on artificial intelligence, aiming to establish unified rules and definitions for the field. CIS countries tend to support the European Union's approach, as the draft law classifies AI systems into unacceptable, high, limited, and minimal risk categories. At present, the CIS applies a flexible "sandbox" approach and adheres to UNESCO principles. Given that the operation of AI relies on three essential elements—databases, models, and access to information (usage)—we believe that the

law must include provisions on personal data protection, as well as requirements for data collection, storage, and processing.

On March 10, 2026, the Presidential Decree "On Defining the Cybersecurity Strategy of the Republic of Uzbekistan and Improving the Cybercrime Prevention System" was adopted to effectively protect the interests of individuals, society, and the state in cyberspace, ensure the stability of the information infrastructure, identify priority areas for further strengthening cybersecurity in digital economy sectors, improve the cybercrime prevention system, and develop and strengthen a culture of cybersecurity among citizens. In accordance with the document, a Cybersecurity Strategy for 2026-2030 and a Roadmap for implementing the Cybersecurity Strategy for this period were adopted. The Decree sets the tasks for heads of government agencies and organizations to apply effective methods and means of protection against modern cyberthreats and cybersecurity issues, as well as to strengthen oversight of organizational information security policies and develop requirements for ensuring information and cybersecurity during the integration of government systems within the digital government by January 2027. (N. Nugmanov 2026).

The Republic of Uzbekistan should develop a national model for AI legal regulation based on national legislation. To do so, amendments must be made to the laws "On Informatization" (Law of the Republic of Uzbekistan 2003). "On Personal Data" Law of the Republic of Uzbekistan 2019) and "On Copyright and Related Rights," (Law of the Republic of Uzbekistan 2006) as well as to administrative legislation. In our opinion, before joining the draft law proposed within the CIS framework, it must undergo another round of expert legal review.

The United Arab Emirates, in its approach to regulating AI, strives to strike a balance between promoting innovation and ensuring responsible governance. Currently, the UAE's Council for Artificial Intelligence is integrating AI into state institutions and the education sector. The Charter on Artificial Intelligence, adopted in 2024, defines 12 key principles, including "Privacy and Data Protection" and "Security." The UAE's Law on the Protection of Personal Data serves as the foundation of its national data protection framework. Furthermore, instead of developing a single law, the UAE has opted for a complex model, formulating a set of

rules that combine norms related to information security and intellectual property protection.

The African Union's approach to regulating artificial intelligence is based on the principles of information security and cybersecurity. It supports accession to conventions adopted in the field of cybersecurity.

Upon conducting a scientific analysis of the African Union's approach, the following conclusions were drawn: despite the adoption of the Continental Strategy on Artificial Intelligence, the Malabo Convention aimed at cybersecurity and personal data protection, as well as the resolution on human rights and artificial intelligence, there may still be challenges in developing regulatory and legal frameworks. The reason is that the Strategy has a consultative character, and the adopted norms do not possess an imperative nature.

Other factors within the continent also affect the absence of comprehensive legislation. For example, weak electricity supply and low-speed internet limit the ability to collect necessary information. Moreover, the shortage of experts in ethics and law negatively impacts the capacity to monitor and regulate artificial intelligence.

The most significant aspect that draws our attention in the African Union's approach is its reliance on transparency, the protection of human rights, and the principles of non-discrimination. Additionally, the African Union aims to establish its national approach to the legal regulation of artificial intelligence technologies while strictly adhering to data protection laws.

In our estimation, adapting the approaches of the European Union and the United States to the African context would not be appropriate. Therefore, the African Union should develop its own national approach.

References

1. The Global Cybersecurity Outlook., 2025. Available at: https://www.weforum.org/publications/global-cybersecurity-outlook-2025/ [Accessed 9 February 2024].
2. Nugmanov N.A., 2023. International Legal Regulation of Information Security within the UN // International Affairs: Politics, Economics, Law. Volume number 9-10 / 2023. - Nugmanov N.A. Information Security Concept Major

Aspects and Specifics // International Affairs: Politics, Economics, Law. Volume number 1-2 / 2024. - P. 118-136.
3. Nugmanov N.A., 2015. International legal regulation of cooperation in the field of international information exchange // Bulletin of the Volga Region Institute of Management under the Russian Presidential Academy of National Economy and Public Administration. – Saratov, 2015. Available at: http://vestnik.pags.ru/vestnik/archive/vestnik-47.php [Accessed 30 March 2015].
4. Kingsley Ofosu-Ampong., 2024. Artificial intelligence research: A review on dominant themes, methods, frameworks and future research directions. Alliance Bioversity International & CIAT, Ghana, Heritage Christian University ,Ghana. Available at: https://www.sciencedirect.com/science/article/pii/S2772503024000136 [Accessed March 2024].
5. Grabova, O., Urso, G., Corbane, C., Dalmasso S., Kemper., 2025. Artificial Intelligence approaches for disaster risk management, European Commission, Bruxelles. Available at: https://publications.jrc.ec.europa.eu/repository/handle/JRC142778 [Accessed 25 June 2025].
6. Nathalie A. Smuha., 2025. Regulation 2024/1689 of the Eur. Parl. & Council of June 13, 2024 (Eu Artificial Intelligence Act). Cambridge University Press. Available at: https://www.cambridge.org/core/journals/international-legal-materials/article/regulation-20241689-of-the-eur-parl-council-of-june-13-2024-eu-artificial-intelligence-act/64F1F6734F8C66CA3EEA149C9759194E [Accessed 10 March 2025].
7. Anna Pirozzoli., 2024. The Human-centric Perspective in the Regulation of Artificial Intelligence European Papers Vol. 9, 2024, No 1, pp. 105-116 (European Forum, 20 May 2024), pp. 105-116. Available at: https://www.europeanpapers.eu/europeanforum/human-centric-perspective-regulation-artificial-intelligence [Accessed 20 May 2024].
8. Miguel Ángel Presno Lineraa, Anne Meuwese., 2025. Regulating AI from Europe: a joint analysis of the AI Act and the Framework Convention on AI. Department of Constitutional Law, University of Oviedo, Oviedo, Spain. The Theory and Practice of Legislation. Available at: https://www.tandfonline.com/doi/full/10.1080/20508840.2025.2492524#abstract [Accessed 25 April 2025].
9. 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. Available at: https://eur-lex.europa.eu/eli/reg/2024/1689/oj/eng [Accessed 13 June 2024].
10. Laurie Harris., 2025. Regulating Artificial Intelligence: U.S. and International Approaches and Considerations for Congress. Available at: https://www.congress.gov/crs_external_products/R/PDF/R48555/R48555.2.pdf [Accessed 4 June 2025].
11. Yingjie Hu, Wenwen Li, Dawn J Wright, Orhun Aydin., 2019. Artificial Intelligence Artificial Intelligence Approaches. Available at: https://www.researchgate.net/publication/335089772_Artificial_Intelligence_Approaches [Accessed July 2019].

12. Tatevik Davtyan., 2025. The U.S. Approach to AI Regulation: Federal Laws, Policies, and Strategies Explained, 16 Case W. Res. J.L. Tech. & Internet 223. Available at: https://scholarlycommons.law.case.edu/jolti/vol16/iss2/2/ [Accessed 9 June 2025].
13. Marcin Szczepański., 2024. United States approach to artificial intelligence. EPRS European Parliamentary Research. Available at: https://www.europarl.europa.eu/RegData/etudes/ATAG/2024/757605/EPRS_ATA(2024)757605_EN.pdf [Accessed January 2024].
14. Kasim Balarabe., 2025. Digital borders and beyond: Establishing normative grounds for cybersecurity and sovereignty in international law. Available at: https://www.sciencedirect.com/science/article/abs/pii/S2212473X25000537 [Accessed September 2025].
15. Isabella Brunner., 2025. Attributing cyber operations under International law: Political and legal aspects. Jindal Global Law School, O P Jindal Global University, Sonipat, Haryana, India. Page 26-43. Computer Law & Security Review. Volume 58. Available at: https://www.sciencedirect.com/science/article/abs/pii/S2212473X25000537 [Accessed September 2025].
16. Stefan R. Badža., 2024. Development of Artificial Intelligence in Serbia. Serbia as the Regional Leader. Available at: https://fondacijasnd.rs/wp-content/uploads/2024/09/01-Stefan-Badza-engleski.pdf [Accessed 9 August 2024].
17. Namanja Sladaković, Bojan Tutić., 2024. Serbia: What is the understanding or definition of AI in your jurisdiction? Available at: https://www.ibanet.org/medias/anlbs-ai-working-group-report-september-2024-26-serbia.pdf?context=bWFzdGVyfFB1YmxpY2F0aW9uUmVwb3J0c3w2NTUzM3xchHBsaWNhdGlvbi9wZGZ8YURWbEwyaG1OUzg1TVRVMk16WTVORGd4TnpVNEwyRnViR0p6TFdGcExYZHZjbXRwYm1jdFozSnZkWEF0Y21Wd2IzSjBMWE5sY0hSbGJXSmxjaTB5TURJMExUSTJMWE5sY21KcFlTNXdaR1l8NTQ0YmI5MTEyMmY3Nzc3MTZkNWFlMWNlZjBhZDEzMjgzMjI1ZDBmNDJkMmQ4MDU3OGZlNDY0MGNiNGRiNGFlNQ
18. Huw Roberts, Josh Cowls, Jessica Morley, Mariarosaria Taddeo,Vincent Wang, Luciano Floridi., 2020. The Chinese approach to artificial intelligence: analysis of policy, ethics, and regulation. Available at: //https://www.researchgate.net/publication/342246048_The_Chinese_approach_to_artificial_intelligence_an_analysis_of_policy_ethics_and_regulation [Accessed 17 June 2020].
19. Volodin., 2024. Features of the Chinese approach to artificial intelligence security. Development strategy in relation to law and standardization. Pp. 158-160. Available at: https://search.rads-doi.org/showfile/ru/68671 [Accessed 6 October 2024].
20. Tracey TANG (2025). China and the U.S. – Different Approaches to Regulating AI. Available at: https://www.chinalawvision.com/2025/04/digital-economy-ai/china-and-the-u-s-different-approaches-to-regulating-ai/ [Accessed April 3, 2025].
21. Bryukhovetsky, I.V.,2025. On China's approaches to regulating generative artificial intelligence. Pp. 177-178 . Available at: https://cyberleninka.ru/article/n/o-podhodah-knr-k-regulirovaniyu-generativnogo-iskusstvennogo-intellekta [Accessed 30 May 2025].
22. Ablomeiko S.V., Ablomeiko M.S., Belotserkovsky A.M., Golenkov V.V., Kasanin S.N., Kruglikov S.V., Minko N.S., Mikhaleva T.N., 2024. Main provisions

of the model law "On Artificial Intelligence" Tenth International Scientific and Practical Conference "BIG DATA and Advanced Analytics. BIG DATA and high-level analysis". Available at: https://libeldoc.bsuir.by/bitstream/123456789/54718/1/Ablomejko_Osnovnye.pdf [Accessed 13 March, 2024].
23. G. G. Lyanna., 2024. Administrative and legal regulation of the development and use of artificial intelligence technologies. Siberian Legal Review. Vol. 21, No. 3. UDC // https://cyberleninka.ru/article/n/administrativno-pravovoe-regulirovanie-razrabotki-i-ispolzovaniya-tehnologiy-iskusstvennogo-intellekta/viewer [Accessed 25 June 2024].
24. Chikvin, A.B., 2025. Comparative legal analysis of draft information and digital codes of the CIS countries. Humanities, socio-economic and social sciences. No. 6. Available at: https://cyberleninka.ru/article/n/sravnitelno-pravovoy-analiz-proektov-informatsionnyh-i-tsifrovyh-kodeksov-stran-sng/viewer [Accessed 25 June 2025].
25. Khisamova Z.I., Begishev I.R., 2019. Legal regulation of artificial intelligence. Baikal Research Journal. No. 2. Available at: https://cyberleninka.ru/article/n/pravovoe-regulirovanie-iskusstvennogo-intellekta [Accessed 15 July 2019].
26. N.Nugmanov and V.Sayfullaeva 2026. International legal initiatives of Central Asian countries in the development of artificial intelligence and ensuring information security. Vol. 7 No. 3 (2026): The interdisciplinary electronic scientific journal "Society and Innovations". Available at: https://doi.org/10.47689/2181-1415-vol7-iss3-pp136-141 [Accessed June 2026].
27. Modafar Shaker Akhoirshieda, Ku Muhammad Naim Ku Khalif, Suryanti Awang., 2024. Artificial intelligence in the United Arab Emirates public sector: a systematic literature review. IAES International Journal of Artificial Intelligence (IJ-AI) Vol. 13, No. 3. Available at: https://www.researchgate.net/publication/383632890_Artificial_intelligence_in_the_United_Arab_Emirates_public_sector_a_systematic_literature_review [Accessed 3 September 2024].
28. Adel Salem Allouzi, Karima Krim., 2023. The role of artificial intelligence and emerging technologies in UAE commercial transactions law. Research Journal in Advanced Humanities 5(4). Available at: https://www.researchgate.net/publication/393772196_The_role_of_artificial_intelligence_and_emerging_technologies_in_UAE_commercial_transactions_law_2023 [Accessed November 2024].
29. Hewa Abdulkhaleq Ahmed, Hewa Abdulkhaleq., 2025. The Role of Artificial Intelligence in Public Policy Management: The United Arab Emirates as a Model. Available at: https://www.mabdaa.edu.iq/wp-content/uploads/2025/05/41-The-Role-of-Artificial-Intelligence-in-Public-Policy-Management-The-United-Arab-Emirates-as-a-Model-1.pdf [Accessed May 2025].
30. Islam Al Khatib., 2024. Beyond Techwashing: The UAE's AI Industrial Policy as a Security Regime. Available at: https://ainowinstitute.org/publications/research/ai-nationalisms-global-industrial-policy-approaches-to-ai [Accessed 12 March 2024].
31. Mohammed Karimkhan Pathan and Aman Shah., 2025. Ethical Considerations and Responsible Governance of Generative AI: A Systematic Review 2025. Page 1-7. Available at: https://premierscience.com/wp-content/uploads/2025/04/pjai-25-800-1.pdf [Accessed 16 April 2025].

32. Caroline Ncube, Isaak Rutenberg, Tobias Schonwetter, and Desmond Osaretin Oriaxogba (2024). Artificial Intelligence and the Law in Africa. Available at: https://www.researchgate.net/publication/378555631_Artificial_Intelligence_and_the_Law_in_Africa [Accessed February 2024].
33. Benjamin C. Guinhouya (2024). Health data in sub-Saharan Africa: challenges, risks, and opportunities. Africa data protection report - December 2024. Available at: //chrome-extension://efaidnbmnnnibpcajpcglclefindmkaj/https://www.africadataprotection.org/africadataprotection_report_en_december_2024.pdf [Accessed December 2024].
34. Law of the Republic of Uzbekistan (2003). On informatization, 11 December 2003. Available at: https://lex.uz/ru/docs/6808124 [Accessed 11 December 2003].
35. Law of the Republic of Uzbekistan (2019). On personal data, April 16, 2019. Available at: https://lex.uz/docs/4831939 [Accessed 1 October 2019].
36. Law of the Republic of Uzbekistan (2006). On copyright and related rights, March 23, 2006. Available at: https://lex.uz/ru/docs/6123336 [Accessed 20 July 2006].