Legal challenges of artificial intelligence in the European Union's digital economy

Tamara Kortukova[1], Maryna Dei[2], Volodymyr I. Kudin[3], Andrii Onyshchenko[4], Petro Kravchuk[5]

[1]Department of International, Civil and Commercial Law, Kyiv National University of Trade and Economics, Kyiv, Ukraine
[2]Department of Constitutional and Administrative Law, National Aviation University, Kyiv, Ukraine
[3]Department of Intellectual Technologies, Taras Shevchenko National University of Kyiv, Kyiv, Ukraine
[4]Department of Information Systems and Technologies, Taras Shevchenko National University of Kyiv, Kyiv, Ukraine
[5]Law Department of the Faculty of Law, Private Institution of Higher Education European University, Kyiv, Ukraine

Article Info

ABSTRACT

This article critically examines the legal and regulatory challenges posed by artificial intelligence (AI) within the European Union's (EU) digital economy, focusing on the recently adopted EU Ai Act (Regulation 2024/1689). While previous studies have addressed AI's ethical and theoretical dimensions, this research fills a gap by analyzing the Act's practical application across its temporal, personal, material, and territorial scopes. The study adopts a qualitative legal methodology, integrating doctrinal interpretation, comparative analysis, and systemic review of EU and international legal instruments. Key findings reveal that the EU AI Act establishes a pioneering risk-based regulatory framework, distinguishing itself through strong safeguards for fundamental rights, transparency, and human oversight. However, critical limitations remain, including ambiguous high-risk classifications, reliance on provider self-assessment, and exemptions for national security that may undermine human rights protections. The article compares the EU approach with those of the United States and China, illustrating divergent models of AI regulation and their global implications. It argues that while the EU AI Act sets an ambitious precedent, its success depends on effective enforcement, stakeholder compliance, and international regulatory convergence. By addressing these challenges, the EU can shape a globally influential framework for ethical and responsible AI deployment. This study contributes to the evolving academic and policy debate on AI governance by offering practical insights and recommendations for future research and legal development.

Corresponding Author:

Volodymyr I. Kudin
Department of Intellectual Technologies, Taras Shevchenko National University of Kyiv
01033, 60 Volodymyrska Str., Kyiv, Ukraine
Email: volodymyr_kudin@edu-knu.com

1. INTRODUCTION

The rapid development of artificial intelligence (AI) has triggered significant transformations in the global digital economy, reshaping the way individuals, governments, and businesses interact with data, automate processes, and make decisions. From autonomous vehicles and predictive policing to algorithmic credit scoring and biometric identification, AI systems are increasingly embedded into critical domains of life. Within the European Union (EU), AI is being leveraged to enhance the efficiency of justice systems, streamline border management, and improve public sector service delivery. According to Eurostat, in 2023, approximately 8% of EU businesses and over 30% of large enterprises adopted some form of AI technology,

highlighting its growing influence across sectors. Simultaneously, public concern over privacy, accountability, discrimination, and control of AI systems has intensified. A significant majority of EU citizens - over 75% - believe that public authorities should ensure that AI technologies uphold fundamental rights and reflect democratic values.

Amid these advances, the risks associated with unregulated AI deployment have become more pronounced. Studies have documented algorithmic bias in facial recognition, opaque decision-making in automated credit and welfare assessments, and potential abuses in AI-assisted surveillance. These risks are especially concerning in domains such as migration, law enforcement, and border control, where vulnerable populations may be disproportionately impacted. The Court of Justice of the European Union (CJEU) has already issued rulings emphasizing the need for AI to respect human rights and adhere to principles of proportionality and data protection.

Recognizing both the transformative potential and the systemic risks of AI, the EU introduced the AI Act (Regulation 2024/1689), marking the first attempt at a comprehensive horizontal legal framework specifically aimed at governing AI technologies across member states. The Act adopts a risk-based approach, categorizing AI systems into prohibited, high-risk, and low-risk classes and imposing corresponding obligations on providers, users, and deployers. It also extends its jurisdiction beyond EU borders through extraterritorial provisions, requiring non-EU entities to comply with its standards when operating in the EU market. The Act's design reflects an effort to harmonize national regulations, safeguard fundamental rights, and promote innovation through legal certainty.

However, while the EU AI Act represents a regulatory milestone, important legal and practical questions remain. Existing academic literature has focused extensively on ethical AI frameworks, sectoral codes of conduct, and aspirational principles, but there is a relative lack of detailed legal analysis concerning the operational structure of the EU AI Act. Key areas of uncertainty include the practical application of its high-risk classification, the adequacy of enforcement mechanisms, the impact of its extraterritorial scope on international cooperation, and the consistency of its personal scope - particularly with regard to military AI, small and medium-sized enterprises (SMEs), and public-private AI partnerships.

Moreover, few studies have critically compared the EU's approach with alternative models of AI governance, such as the innovation-focused and decentralized system in the United States, or the centrally controlled, algorithm-accountability-based framework in China. These jurisdictions provide contrasting regulatory environments that shape how AI is designed, deployed, and monitored, both domestically and internationally. Understanding these differences is essential for assessing the global influence of the EU AI Act and for identifying the feasibility of international harmonization of AI standards.

This study seeks to address these scholarly and policy gaps by undertaking a structured legal analysis of the EU AI Act, focusing on four fundamental regulatory dimensions: ratione temporis (temporal scope), ratione personae (personal scope), ratione materiae (material scope), and ratione loci (territorial or geographical scope). It examines how the Act functions as a legal instrument within the EU's digital strategy and assesses its broader implications for AI governance beyond the EU. Drawing on doctrinal legal research and comparative methodology, this article evaluates how the Act responds to emerging legal risks, to what extent it advances the protection of fundamental rights, and whether it establishes a workable framework for responsible innovation. In doing so, the paper contributes to the ongoing academic discourse on AI regulation by providing a critical, multi-dimensional evaluation of the EU AI Act and offering insights that are directly relevant for legal scholars, policymakers, technology developers, and civil society advocates engaged in shaping the future of AI governance.

2. LITERATURE REVIEW

The EU presented harmonized standards for AI applications, committed to ensuring safety and protecting basic rights in line with EU principles, in response to the exponential growth of the technology [1]. The European Parliament and Council's Regulation (EU) 2024/1689 (hereinafter - EU AI Act), which establishes harmonized rules on AI and was passed on June 13, 2024, aims to guarantee that AI systems used in the EU market are safe, comply with laws regarding fundamental rights and values within the EU, are low risk, and do not violate human or citizen rights and freedoms (Regulation 2024/1689).

The EU AI Act, with its focus on protecting fundamental rights and mitigating risks, possesses the capacity to influence the future of responsible AI development and deployment globally. The EU AI Act is an attempt to horizontally govern AI for the first time in history. Nijweide [2] mentioned, that, the EU AI Act is a significant step forward in a space with little regulation, which will reduce the harm caused by design oversights and biased training data while also ensuring AI systems are carefully monitored [3], [4].

However, the EU AI Act has been criticized for its heavy-handed approach, placing potentially burdensome regulations on AI development. Some argue that the Act's strict requirements could stifle innovation and hinder the growth of AI technologies [5], [6]. Another criticism of EU AI Act is that it

contains significant gaps, particularly regarding the classification of high-risk AI systems. Providers can self-assess their systems as low-risk, circumventing stringent regulations. Additionally, the Act lacks mechanisms to mitigate potential harms to fundamental rights and fails to ensure transparency in sensitive areas like law enforcement and border control. The EU AI Act's restrictions on facial recognition technology have significant loopholes. While law enforcement use is limited, it still allows for broad surveillance, even in sensitive areas. This raises concerns about privacy violations and potential discrimination. Overall, the EU AI Act's approach to facial recognition technology is insufficient to protect human rights [7], [8].

Hancher *et al.* [9] enacting laws governing AI is essential to guaranteeing its morally and safely applied applications. Haataja and Bryson [10], Fraser and Villarino [11] discuss how the EU's ostensibly "ethical" regulation of AI connects to more conventional regulatory goals, particularly those centered around the single market and the elimination of obstacles to competition. Ciurea [12], Wang [13] analysis, the AI Act has the potential to constantly scale up improved practices for goods with intelligent components in the EU through the force and strength of product legislation. However, there is also a possibility that the law will just serve as window dressing, targeting a select few elite players after the fact. The EU AI Act's approach to risk management and risk tolerance for high-risk AI systems that endanger people's safety and fundamental rights is severely examined [14].

The EU AI Act is a major step forward in reshaping the global regulatory environment for AI. Despite all challenges, there is a growing consensus that international AI regulations are necessary to guarantee the ethical creation and application of AI. As AI technology continues to develop, it is likely that we will see more and more international initiatives to develop AI regulations. There are a number of researchers, who analyzed AI regulation on the global level and the place of EU AI Act in international regulation of AI. For instance, [15] examined how the EU AI Act affected the 2030 UN sustainable development goals. The legislative and policy environment around AI in the EU and other international jurisdictions was studied [16]. Furthermore, the approach that regional and United Nations agencies have taken to AI was detailed in a study conducted among international organizations. Since AI legislation is still in its early stages, rules, codes of ethics, and declarations and acts by governments and their agencies regarding AI were also discussed [17], [18].

Numerous scientists conducted research on a comparative examination of the EU's laws governing AI and other countries of the world. For example, Kusche [19] made the comparison of EU and China approaches from the standpoint of how to make AI rules and regulations applicable outside national borders. Stewart [20] compared the aims and ethical outcomes of the regulating AI in China and the EU.

3.   RESEARCH METHOD

This study employed a qualitative research design that integrates a systematic legal doctrinal approach and comparative legal analysis. The primary aim was to critically examine the legal challenges associated with the EU AI Act in the context of the digital economy. The research followed a structured sequence: (i) collection and selection of academic publications, legal texts, and policy reports relevant to AI regulation in the EU, US, and China; (ii) classification of sources into thematic categories such as scope (ratione temporis, personae, materiae, and loci), fundamental rights, risk-based classification, and extraterritoriality; (iii) application of legal interpretation techniques - particularly teleological and systemic interpretation - to analyze the objectives, consistency, and implementation challenges of the EU AI Act; (iv) cross-jurisdictional comparison with US and Chinese AI legislation to identify gaps, divergences, and best practices. Each step was documented and reviewed to ensure transparency and reproducibility of the legal analysis. This rigorous methodological approach ensures that findings are robust and replicable by other scholars examining AI legal frameworks.

The dialectical method is based on the basic principles of dialectics, studying the EU AI Act from the perspective of unity. Within its structure, analysis and synthesis are actively used, which help to separate the EU AI Act into individual elements and explore their relationships. In the article, we divided the analysis the EU AI Act for the subsequent elements, such as ratione temporis, ratione personae, ratione loci, and ratione materiae. The logical method assumes that the EU AI Act is studied using formal logic. The techniques used in this methodology are deduction and induction, the principles of analogy and identity. The analysis of the EU AI Act as a part of the EU digital market serves as the main guide for the systematic approach. The EU AI Act was examined as a fundamental component of EU law with the assistance of the systemic-structural technique of EU AI Act research.

Using the legally historical method, the EU AI Act was examined from the perspective of its temporal development. Considering the features of the fourth and fifth industrial revolutions, the logic by which the Act was written and its necessity for modern regulation was understood. Moreover, legally historical method helped to identify when certain requirements of the EU AI Act would come into effect.

With the help of the comparative legal method analysis of legislative methods for regulating AI in countries such as the USA and China was carried out, as well as compared its approaches with the EU one. The findings from this multi-faceted research methodology serve as the basis for the discussion and recommendations presented in the article.

A comprehensive analysis of scholarly works, official papers, and business reports pertaining to AI legislation in the EU was carried out. Key sources included primary and secondary EU legislation, journal articles, books, EU policy papers, and publications from think tanks. The literature review focused on identifying the major legal and regulatory issues surrounding the governance of AI technologies in the context of the EU's digital economy.

This research utilized a qualitative approach, analyzing academic and policy literature, official EU documents, and comparative legislative practices to understand the regulatory dimensions of AI within the EU's digital economy. Key methods included dialectical and systemic-structural analysis, dividing the EU AI Act into its temporal, personal, material, and geographical scopes. Additionally, a comparative legal method was employed to examine AI governance frameworks in the US and China. Historical and logical methods provided insights into the evolution and rationale of the EU AI Act, while specific systemic principles such as induction and deduction clarified its implications.

4. RESULTS

The study highlights that the EU AI Act's emphasis on fundamental rights contrasts with the more innovation-driven US approach and the state-centric Chinese model. For instance, the Act's high-risk classification provides stricter controls but lacks detailed mechanisms for ongoing oversight. This differs from China's detailed algorithmic accountability framework or the US's flexible but fragmented regulatory environment. This analysis identifies several limitations in the EU AI Act, such as ambiguity in defining "high-risk" systems, reliance on self-assessment by providers, and insufficient safeguards against AI misuse in sensitive sectors like migration and border control. Additionally, its implementation may disproportionately burden SMEs, potentially stifling innovation.

4.1. Ratione temporis of the EU AI Act

The ratione temporis refers to the time period over which the legislation will apply. Drafted in accordance with the objectives of the digital single market, the European commission released a proposal for a regulation of the European parliament and of the council on April 21, 2021, laying out unified regulations on AI [21]. Following the adoption by the European parliament on March 13, 2024, by a vote of 523 in favor, 46 against, and 49 abstentions, as per the ordinary legislative procedure and approval of the council on 21 May 2024 this regulation became an enforceable law in EU on 1 August 2024, 20 days later in official journal of the EU after the publication, that was made on 12 July 2024. Therefore, all time counts and requirements established by the EU AI Act will be counted from the day the law went into effect in EU AI Act (August 1, 2024) (Regulation 2024/1689) [22].

The EU AI Act's provisions will go into effect gradually: states will have six months to outlaw AI systems that are outlawed, a year to impose regulations on "general-purpose AI systems," such as chatbots, and a maximum of 36 months for AI systems that the law has classified as "high risk". Article 56 of the EU AI Act stipulates that codes of practice shall be finalized within 9 months of the EU AI Act's entry into force (Regulation 2024/1689). However, the EU AI Act has been highly debated and discussed in view of the ratione temporis. Some have expressed concerns with respect to retrospective application, referring to a situation when newly enacted legislation modifies rights acquired earlier (before the time of enactment of the new regulations) or changes legal consequences for events that occurred in the past. According to researchers it could impose serious compliance issues on organizations that already had developed or deployed an AI system before the enactment date of such a law [23].

Others have favored the more graduated approach whereby such regulation applies to AI systems only when these are in development or brought into operation after the date of enforcement of the law. In this way, businesses and organizations have a clear timeframe for compliance and can make transition arrangements to adapt to the new regulatory framework over time. As a result, it was determined that the gradual application of the EU law on AI is the most acceptable for all parties [24].

It should be mentioned, that while numerous countries have enacted AI legislation around the same time, their approaches to regulation vary significantly. The EU, US, and China, for instance, have adopted distinct strategies. To compare, the US adopted the federal AI in government Act and the national AI initiative Act in 2020. However, it has focused on promoting AI research and development rather than directly regulating private sector AI use. It encourages use of AI and support AI education and research through subsidies.

China adopted the first major binding regulation on algorithms "provisions on the management of algorithmic recommendations in internet information services" in 2021. This regulation, motivated by concerns about algorithms controlling online content, marked a significant step in China's efforts to regulate AI. China's "measures for the management of generative AI services," enacted in 2023, is a pioneering piece of legislation specifically targeting generative AI. It mandates that providers ensure both the training data and generated content are accurate and truthful. In 2024 China adopted its first comprehensive national-level rules on AI through the AI law of the People's Republic of China. The EU AI Act stands out with its emphasis on transparency, accountability, and human oversight. This comprehensive approach aims to ensure that AI is developed and used ethically and responsibly, setting a global standard for AI regulation.

4.2. Ratione personae of the EU AI Act

Ratione personae refers to the entities and individuals that are subject to the Act's requirements and obligations, that are listed in art. 2 of the EU AI Act (Regulation 2024/1689). The EU AI Act regulates the creation, application, and usage of AI systems both inside and outside of the EU (extraterritoriality and Brussels impact) in a wide and thorough manner. The EU AI Act omits several important details [25]. Unintentionally discovered regulatory gaps may call for discussion on how best to close them, while other times, the discovery of such gaps may indicate a policy choice. At the same time, determining precisely which actors will fall under the Act's purview is crucial for ensuring effective and consistent implementation [26].

One of the primary considerations is the inclusion of both public and private sector entities. Both governmental and private institutions that develop, implement, or utilize AI systems will be subject to the AI Act. This includes technology companies, software developers, research institutions, and any other stakeholders in the AI ecosystem. The Act encompass the providers (developers) and deployers of AI, such as businesses, public authorities, and individuals who incorporate AI into their products, services, or decision-making processes for the professional purposes only as well as distributors and importers of AI systems, as well as any individuals impacted, who are based in the EU (Regulation 2024/1689) [27].

Such a wide personal scope serves to deal with the intricately interconnected value chain of AI and the associated complexity. The EU aims to create an expansive regulatory framework capable of restricting risks and maintaining ethical standards associated with the AI technology, while also making all relevant parties accountable. Another essential point in personal scope is the policy concerning SMEs. The EU AI Act acknowledges that SMEs are relevant stakeholders to improve innovation and competition in the AI market. Therefore, it provides for special guidance, support, and possible exemptions for SMEs due to their more limited resources and capacities, compared to large business firms [28].

However, it has to be borne in mind that AI for specifically military purposes will fall completely outside the scope of the EU's AI Act. The major reason for this is the recognition of national sovereignty and the competency of the member states with regard to defense and security. At least the EU has recognized that the regulation of military AI lies outside the scope of its competencies, these areas lying in the exclusive domain of national authorities. The exclusion of military AI from the EU AI Act essentially defers to the different procedures and guidelines of the national governments with respect to regulating the development and application of these technologies within their respective armed services [29].

In this regard, it has been noted that the AI Act's exemption for national security undermines its effectiveness in protecting human rights [30]. This exemption allows governments to use AI for surveillance without the same level of scrutiny as other AI applications. This could lead to the abuse of AI for purposes that violate fundamental rights, such as mass surveillance and discrimination of EU citizens, immigrants, refugees, and anyone else inside EU territory, without any justification [31].

It should be also mentioned, that the EU AI Act will not cover individuals, that use AI for personal, non-professional purposes, social scoring leading to detrimental/unfavorable treatment, AI system for research, biometric identification systems. The ultimate objective is to provide a comprehensive and flexible regulatory framework that can protect European people' rights and interests while also promoting innovation. A key element in achieving this goal and influencing the direction of AI in the EU and abroad is the AI Act's personal scope [32].

While the US on the federal level has not adopted a comprehensive AI law like the EU AI Act, its regulatory approach involves a diverse range of actors and mechanisms [33]. Inter alia, the national AI initiative Act of 2020 primarily impacts federal agencies, research institutions, and educational institutions in the US. The Act directs these entities to coordinate their efforts in AI research, development, and education. While the Act does not directly regulate private sector AI activities, it can indirectly influence the industry through the development of standards and the promotion of AI research [34]. The Act's focus on promoting US leadership in AI suggests that it may have a less direct impact on businesses compared to more prescriptive regulations, such as those in the EU. The AI law of the People's Republic of China, 2024

primarily targets entities involved in the AI lifecycle, including developers, providers, users, and data providers. The law seeks to regulate the development, application, and use of AI technologies, addressing issues such as data privacy, algorithm transparency, and ethical considerations.

4.3. Ratione loci of the EU AI Act

AI regulation in the EU has both internal and external dimensions. Internally, the EU AI Act provides a comprehensive framework for regulating AI systems. Externally, the EU's influence extends through extraterritoriality, "Brussels Effect" of EU AI Act, as well as Digital cooperation agreements with third countries.

The EU AI Act is directly effective and applicable in all 27 EU Member States as it was enacted through the ordinary legislative procedure as a regulation. However, two EU members, Denmark and Ireland are opted-out from parts of the EU AI Act's rules, as stated in paragraphs 21 and 40 of the Act (Regulation 2024/1689). This means that Ireland and Denmark won't be bound by the rules of EU AI Act related to the use of biometric systems and process of personal data for police and criminal justice. It was stipulated as well in articles 2 and 2a of protocol no. 22 and article 6a of protocol no. 21, which are appended to the TEU and to the TFEU [35]. It is worth noting, that the application of the EU AI Act is not limited only by EU borders. It will have a variety of effects on the development of AI regulation globally due to its extraterritorial application and the so-called "Brussels effect" for policy makers.

Article 2 of the EU AI Act defines the extraterritorial reach of the Act in an effort to impose duties on non-EU businesses that supply the EU market or offer AI products and services to EU users. This necessarily implies that compliance with the requirements of the EU AI Act would be of prime importance for placing and marketing AI-enabled products in the EU internal market. By setting the standard of rules, which other countries have to match to get access to the EU internal market, EU legislators aim to protect the EU citizens.

However, the EU AI Act's extraterritorial scope is limited, meaning that AI systems exported outside the EU may not be subject to the same regulations. These limitations could undermine the EU's commitment to human rights and global ethical standards for AI. The Brussels effect is a legal term that describes the ability of EU legislation to have an impact on the legal landscape of other countries. The Brussels effect is particularly relevant for the present analysis related to the EU AI Act since the EU is a key player in the global AI market, and its legislation may have great effects on AI development and deployment worldwide.

In practice, the EU AI Act could encourage other countries to adopt their own AI regulations that are aligned with the EU's principles, leading to a more harmonized global regulatory framework for AI, as it was, for instance, with general data protection regulation. Nonetheless, there are many discussions in general society on whether the EU AI Act would have a Brussels effect. For example, Bradford argues that the EU AI Act would have Brussels effect and inspire other countries to adopt similar to EU laws. Renda said the EU has to develop and promote the EU (semi-open) technology stack; increase its strategic counsel and foresight rather than only relying on the Brussels effect; and maintain policy consistency both inside and outside of EU territory [36].

Conversely, five components of the Brussels effect have been identified: market size, regulatory capacity, stringency, inelastic target, and the non-divisibility of the regulated object. After analizing it, the scholars came to the conclusions, that EU AI Act would have the limited Brussels effect [37]. Similar conclusions have been drawn, with some scholars stressing that portions of the EU's AI law are likely subject to both de facto and de jure Brussels effects. The Brussels effect, the researchers said, will probably have a greater impact than either the Washington Effect or the Beijing effect. According to one analysis, competition is expected to arise as different countries and international bodies enact regulations pertaining to AI [38]. In this piece, he said that rather than claiming to be "racing" to regulate, the EU would stand to win more by indicating that it is more willing to collaborate and listen to criticism from the rest of the democratic world. If not, the EU might end up completely by itself at the finish line.

Anyway, one of the key reasons for the Brussels effect is the size and importance of the EU's economy. As the world's second-largest economy, the EU represents a sizable market that global companies cannot afford to ignore. When the EU enacts strict laws like the general data protection regulation, businesses often choose to comply globally rather than create separate products or services for the European market. This is because the reputational and competitive risks of non-compliance can be significant, as customers and partners may become wary of working with firms that do not meet the EU's benchmarks.

It should be also mentioned, that the Brussels effect is not without its challenges. Smaller companies and startups, particularly those based outside the EU, may struggle to meet the AI Act's compliance requirements, potentially hindering innovation and limiting access to the European market. Policymakers will need to carefully balance the need for robust regulation with the goal of fostering a thriving and inclusive AI ecosystem. The EU's capacity to enforce its restrictions against noncompliant corporations and the global

adoption of the EU's AI development and deployment standards will determine how powerful the Brussels impact is.

4.4. Ratione materiae of the EU AI Act

In addition to referencing EU principles and the EU charter on fundamental rights, the first article of the EU AI Act highlights the necessity for innovation to coexist peacefully with the avoidance of any unintended negative effects that AI may have. The material scope, or ratione materiae, of the law is one of the main areas of attention for the EU AI Act. This is a reference to the particular kinds of AI applications and systems that will be covered under the law. Several scientists questioned the EU AI Act's reach. It was stated, for instance, that the existing definition of AI may be unduly inclusive and cover a large variety of standard data processing jobs. This might result in an unduly broad scope when data processing is the sole thing that all regulated systems have in common. Consequently, it may become more difficult to recognize and eliminate applications that, according to the EU AI Act's criteria, do not really qualify as AI systems.

The EU AI Act takes a risk-based strategy. The EU AI Act's material scope includes AI that is expressly forbidden under the EU AI Act and is considered inappropriate. These are programs that negatively impact people's behavior, including social scoring or real-time biometric identification used for widespread surveillance. High-risk AI applications, which seriously jeopardize people's safety, basic rights, and well-being, are at the center of the Act's material scope. These include AI systems utilized in vital industries including healthcare, banking, law enforcement, and transportation, where mistakes or abuse can have dire repercussions. A number of requirements pertaining to risk management systems (article 9), data governance (article 10), technical documentation (article 11), record-keeping (article 12), transparency and providing deployers with necessary information (article 13), human oversight (article 14), accuracy, robustness, and cybersecurity (article 15), should be met by ai systems that are considered high-risk. Furthermore, the proposed rule lays forth a list of responsibilities for suppliers, importers, distributors, and users of high-risk AI systems (articles 16–49). It has been pointed out that the EU AI Act does not include a general risk assessment for fundamental rights across all AI systems covered by the Act, but limits such assessment to high-risk AI only. AI-powered chatbots and recommender systems are into the next group of low-risk AI applications covered under the EU AI Act's material scope. Article 95 of the EU AI Act recommends a voluntary code of behavior for regulating low-risk AI systems, as they are not subject to the EU AI Act's regulations [39].

It has been noted that while the EU AI Act uses fundamental rights as a benchmark, it struggles to concretely define and measure the associated harms. The categorization of AI systems into high-risk and low-risk categories, based on potential impact on fundamental rights, is inherently subjective and relies on political judgments rather than objective criteria. This reliance on implicit value judgments can lead to unintended consequences and limit the Act's effectiveness in addressing future AI-related challenges.

To compare the EU AI Act, it should be noted, that the national AI initiative Act of 2020 primarily focuses on advancing US leadership in AI research and development. Key areas of focus include investing in AI research, developing a skilled AI workforce, fostering international collaboration, and promoting responsible AI development. While the Act does not directly regulate private sector AI, it provides a framework for federal coordination and support of AI initiatives. The AI law of the People's Republic of China comprehensively regulates various aspects of AI, including algorithm development, data privacy, ethical considerations, system safety, and social impact assessment. The law aims to foster responsible AI development and use, promoting innovation while mitigating potential risks.

5. DISCUSSION

While AI regulation has gained increasing scholarly attention, existing literature often lacks a detailed examination of the practical implications of the EU AI Act's provisions across its full scope. Prior studies have focused primarily on ethical frameworks or theoretical principles underpinning AI legislation, without systematically addressing how the EU AI Act affects specific sectors or stakeholders, such as SMEs, law enforcement agencies, or cross-border technology providers. This study investigates the effects of the EU AI Act from a legal-doctrinal and comparative perspective, specifically targeting underexplored areas such as extraterritoriality, personal and material scope, and fundamental rights protection in operational contexts [40].

The analysis found that the EU AI Act introduces a robust regulatory structure based on a risk-tiered model, with high-risk systems facing strict obligations concerning data governance, transparency, and human oversight. We also found that the Act's scope - ratione personae, materiae, loci, and temporis - is designed to ensure broad application across actors, use cases, and geographies. However, the study highlights ambiguities in the definition of high-risk systems and significant gaps in enforcement mechanisms. The Act allows self-assessment by AI providers, raising concerns about compliance integrity, especially in high-impact sectors

like migration and border control. Furthermore, extraterritoriality creates implementation friction for non-EU actors, while national security exemptions introduce inconsistencies in human rights protection.

In comparison with regulatory frameworks in the United States and China, the EU AI Act presents a unique blend of ethical prioritization and formal legal obligation. Unlike the US approach, which emphasizes innovation and self-regulation, or China's model, which enforces top-down algorithmic accountability under state oversight, the EU framework seeks to embed normative human rights values into enforceable obligations. These differences highlight a trade-off: while the EU model may provide stronger safeguards for fundamental rights, it may also result in higher compliance burdens, especially for SMEs and startups.

This study adopts a primarily qualitative legal analysis and is therefore limited in empirical scope. While the comparative review provides valuable insights into legislative structures, it does not evaluate the effectiveness of implementation or stakeholder compliance behavior. Additionally, due to the EU AI Act's recent adoption, data on real-world application remains scarce. Future updates to the Act or evolving case law, especially by the CJEU, may alter its interpretation and practical effect. Moreover, the study does not account for sector-specific AI applications (e.g., medical devices, autonomous vehicles) in detail, which could exhibit regulatory nuances not captured in the general provisions.

The findings point to several key areas for further investigation. Future research should examine how different sectors interpret and operationalize the EU AI Act's high-risk classifications and how SMEs adapt to its requirements. Empirical studies measuring the Act's deterrent or incentivizing effects on innovation would be valuable. Comparative legal analyses could explore the convergence or divergence of global AI norms, especially through the lens of the Brussels effect. Research should also assess the effectiveness of national supervisory bodies in enforcing AI regulations and the potential role of a centralized EU AI agency in ensuring consistency and compliance across member states.

However, the Act's effectiveness will depend on several factors, including its implementation and enforcement mechanisms. The gradual implementation timeline provides flexibility for businesses to adapt, but it also raises concerns about potential delays in addressing emerging risks. Additionally, the Act's reliance on self-assessment by providers for high-risk AI systems could undermine its effectiveness if not properly monitored and enforced [41].

The EU, US, and China have adopted distinct approaches to AI regulation, reflecting their unique technological, economic, and political contexts. The EU's risk-based approach, the US's focus on innovation and market-driven solutions, and China's emphasis on state control and social impact assessment highlight the diverse regulatory landscapes. The EU AI Act's more stringent regulations and its focus on human rights and ethical considerations could potentially give the EU a competitive advantage in the global AI market. However, it may also lead to regulatory burdens and hinder innovation. It could also pose challenges primarily for AI developers. Initial compliance costs, increased administrative burdens, and potential delays in product launch may hinder innovation. Additionally, stricter regulations compared to other regions could create a competitive disadvantage.

The US, on the other hand, has opted for a more flexible approach, prioritizing innovation and market-driven solutions. This approach may lead to faster development and deployment of AI technologies but could also result in a less regulated and potentially less ethical AI ecosystem. China's approach, which combines market-based incentives with strict government control, aims to foster domestic AI innovation while ensuring alignment with the country's social and political goals.

The EU AI Act provides a foundational framework for regulating AI, emphasizing human-centric principles. However, The EU AI Act introduces a concerning double standard for AI deployed by law enforcement, migration, and national security authorities. Exemptions from transparency requirements and the broad national security exemption allow for the unchecked use of surveillance technologies, particularly against marginalized groups. This could lead to increased discrimination, surveillance, and human rights abuses. The Act's failure to adequately address these issues sets a dangerous precedent for the future of AI regulation and raises concerns about the potential for misuse of AI technologies.

As AI technology rapidly evolves, it is crucial to continually assess and adapt regulatory approaches. To ensure the EU AI Act's effectiveness, it is crucial to establish robust oversight mechanisms, strengthen international collaboration, and continuously adapt to the evolving landscape of AI technology. Future research should explore international cooperation to harmonize regulations, effective enforcement mechanisms, the regulation of emerging AI technologies, and the role of international organizations in shaping global AI governance. By addressing these challenges, policymakers can ensure that AI is developed and used responsibly for the benefit of society.

In summary, this study provides a structured and comprehensive legal examination of the EU AI Act's multidimensional scope and its potential global impact. While the Act sets a high regulatory benchmark and emphasizes human rights and ethical design, its success will depend on the robustness of enforcement, adaptability to evolving AI technologies, and international cooperation. The study highlights the need for

further doctrinal and empirical work to assess the Act's effectiveness, identify implementation challenges, and guide regulatory refinements in the face of rapid AI advancement.

6. CONCLUSION

This article has undertaken a comprehensive legal and comparative examination of the EU AI Act, focusing on its temporal (ratione temporis), personal (ratione personae), material (ratione materiae), and territorial (ratione loci) scopes. Employing a structured qualitative methodology grounded in doctrinal analysis, comparative legal methods, and systemic interpretation, the study provides an in-depth understanding of how the EU AI Act seeks to balance innovation, human rights, and market harmonization in an increasingly automated digital economy.

The findings show that the EU AI Act introduces a pioneering risk-based framework aimed at regulating AI applications based on their potential to cause harm. This includes robust provisions for high-risk systems, transparency obligations, and the integration of human oversight in automated decision-making processes. The Act also asserts its influence extraterritorially through the Brussels effect, thereby extending its regulatory footprint beyond the EU's borders. By comparing this framework with those in the US and China, the study highlights the EU's distinctive focus on ethics, accountability, and regulatory harmonization, which contrasts with the more innovation-driven or state-controlled approaches observed elsewhere.

At the same time, the research reveals significant implementation challenges. These include ambiguities in the classification of high-risk systems, limited enforcement mechanisms due to reliance on provider self-assessments, and exemptions for national security and law enforcement that may compromise fundamental rights. Additionally, the burden of compliance may disproportionately affect SMEs and third-country providers, potentially leading to unintended consequences for innovation and market access.

This analysis emphasizes that while the EU AI Act is a milestone in AI regulation, it is not without limitations. Its effectiveness will hinge on ongoing oversight, clear guidance, capacity-building for national enforcement authorities, and adaptive legal mechanisms capable of evolving with AI technologies. Moreover, future revisions must address regulatory gaps, particularly in the areas of biometric surveillance, data-driven border control, and algorithmic accountability.

Ultimately, the EU AI Act represents a significant step toward creating a responsible, transparent, and human-centered framework for AI governance. It establishes a regulatory blueprint that other jurisdictions may draw upon in shaping their own AI laws. However, to ensure global alignment and effectiveness, a coordinated international effort is essential. By fostering collaboration and embracing continual legal innovation, the EU and its global partners can build resilient AI governance systems that safeguard rights while enabling technological progress.

FUNDING INFORMATION

AUTHOR CONTRIBUTIONS STATEMENT

Name of Author	C	M	So	Va	Fo	I	R	D	O	E	Vi	Su	P	Fu
Tamara Kortukova		✓	✓			✓		✓	✓	✓	✓	✓		
Maryna Dei	✓		✓	✓	✓		✓		✓	✓	✓		✓	✓
Volodymyr I. Kudin	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓			✓	
Andrii Onyshchenko			✓								✓			✓
Petro Kravchuk	✓						✓							✓

C : **C**onceptualization	I : **I**nvestigation	Vi : **Vi**sualization
M : **M**ethodology	R : **R**esources	Su : **Su**pervision
So : **So**ftware	D : **D**ata Curation	P : **P**roject administration
Va : **Va**lidation	O : Writing - **O**riginal Draft	Fu : **Fu**nding acquisition
Fo : **Fo**rmal analysis	E : Writing - Review & **E**diting	

CONFLICT OF INTEREST STATEMENT

The authors declare they have no financial and competing interests.

DATA AVAILABILITY

The data that support the findings of this study are available on request from the corresponding author, Volodymyr I. Kudin. The data, which contain information that could compromise the privacy of research participants, are not publicly available due to certain restrictions.

REFERENCES

[1]   C. S. Morgan, P. Dushime, and C. Di Chiro, "10 key takeaways: navigating the future of AI law: understanding the EU AI Act and AIDA," *Lexology*, 2024. https://www.lexology.com/library/detail.aspx?g=9e54ed1e-f9fc-47ad-abb8-2b2102b0ff52.

[2]   F. P. J. Nijweide, "The EU artificial intelligence act: a step in the right direction, but not far enough," *University of Cambridge*, 2022, doi: 10.13140/RG.2.2.20958.72003.

[3]   Y. Karamitsios, *Time for a European Federation, Brussels: Peter Lang Verlag*. Bruxelles, Peter Lang, 2022.

[4]   J. De Cooman, "Humpty dumpty and high-risk AI systems: the ratione materiae dimension of the proposal for an EU artificial intelligence act," *Market and Competition Law Review*, vol. 6, no. 1, pp. 49–88, 2022, doi: 10.34632/mclawreview.2022.11304.

[5]   J. Scott, "Extraterritoriality and territorial extension in EU law," *American Journal of Comparative Law*, vol. 62, no. 1, pp. 87–125, 2013, doi: 10.5131/ajcl.2013.0009.

[6]   "Charter of fundamental rights of the European Union," *European Union*, 2000. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:12012P/TXT (accessed Mar. 19, 2024).

[7]   J. Gesley *et al.*, "Regulation of artificial intelligence in selected jurisdictions," *University of Nebraska-Lincoln*, vol. 5080, no. January, p. 132, 2019, [Online]. Available: https://www.loc.gov/law/help/artificial-intelligence/index.php.

[8]   T. Krarup and M. Horst, "European artificial intelligence policy as digital single market making," *Big Data & Society*, vol. 10, no. 1, Jan. 2023, doi: 10.1177/20539517231153811.

[9]   L. Hancher, K. Talus, and M. Wüstenberg, "Retrospective application of legal rules in the European Union: recent practice in the energy sector," *Journal of Energy and Natural Resources Law*, vol. 39, no. 1, pp. 65–81, 2021, doi: 10.1080/02646811.2020.1804712.

[10]   M. Haataja and J. J. Bryson, "The European Parliament's AI regulation: should we call it progress?," *Amicus Curiae*, vol. 4, no. 3, pp. 707–718, 2023, [Online]. Available: https://journals.sas.ac.uk/amicus/article/view/5612.

[11]   H. Fraser and J.-M. Bello y Villarino, "Acceptable risks in europe's proposed AI Act: reasonableness and other principles for deciding how much risk management is enough," *European Journal of Risk Regulation*, vol. 15, no. 2, pp. 431–446, Jun. 2023, doi: 10.1017/err.2023.57.

[12]   I.-C. Ciurea, "The impact of the EU AI Act on the UN sustainable development goals for 2030 – a text analysis," *Proceedings of the International Conference on Business Excellence*, vol. 18, no. 1, pp. 2857–2870, Jun. 2024, doi: 10.2478/picbe-2024-0237.

[13]   Y. Wang, "Do not go gentle into that good night: the European Union's and China's different approaches to the extraterritorial application of artificial intelligence laws and regulations," *Computer Law & Security Review*, vol. 53, p. 105965, Jul. 2024, doi: 10.1016/j.clsr.2024.105965.

[14]   H. Roberts *et al.*, "Governing artificial intelligence in China and the European Union: comparing aims and promoting ethical outcomes," *The Information Society*, vol. 39, no. 2, pp. 79–97, Mar. 2023, doi: 10.1080/01972243.2022.2124565.

[15]   European court of justice, "C-817/19 - Ligue des droits humains," 2022.

[16]   R. Roßkopf, "The EU pact on migration and asylum:an overview," *Quarterly on Refugee Problems*, vol. 63, no. 2, pp. 184–203, 2024.

[17]   T. Hagendorff, "The ethics of AI ethics: an evaluation of guidelines," *Minds and Machines*, vol. 30, no. 1, pp. 99–120, 2020, doi: 10.1007/s11023-020-09517-8.

[18]   M. Ebers, V. R. S. Hoch, F. Rosenkranz, H. Ruschemeier, and B. Steinrötter, "The European Commission's proposal for an artificial intelligence act—a critical assessment by Members of the Robotics and AI Law Society (RAILS)," *Multidisciplinary Scientific Journal*, vol. 4, no. 4, pp. 589–603, 2021, doi: 10.3390/j4040043.

[19]   I. Kusche, "Possible harms of artificial intelligence and the EU AI act: fundamental rights and risk," *Journal of Risk Research*, pp. 1–14, May 2024, doi: 10.1080/13669877.2024.2350720.

[20]   L. S. Stewart, "The regulation of AI-based migration technologies under the EU AI Act: (Still) operating in the shadows?," *European Law Journal*, vol. 30, no. 1–2, pp. 122–135, 2024, doi: 10.1111/eulj.12516.

[21]   A. Bradford, "Globalizing European digital rights through regulatory power," in *Digital Empires: The Global Battle to Regulate Technology*, Oxford Academic, 2023, pp. 324–359.

[22]   V. O. Pankratova, "General principles of law as a source of European Union Law," *Legal Horizons*, vol. 14, no. 2, pp. 111–117, 2021.

[23]   V. V. Makarchuk, "The concept of the legal status of law enforcement agencies," *Legal horizons*, no. 23, pp. 90–94, 2020, doi: 10.21272/legalhorizons.2020.i23.p90.

[24]   A. Musco Eklund, "Rule of law challenges of 'algorithmic discretion' & automation in EU Border control: a case study of ETIAS through the lens of legality," *European Journal of Migration and Law*, vol. 25, no. 3, pp. 249–274, 2023, [Online]. Available: https://brill.com/view/journals/emil/25/3/article-p249_1.xml.

[25]   V. O. Nahorna, "Formation and development of national minority rights protection in international law," *Legal horizons*, vol. 33, no. 20, pp. 159–166, 2020, doi: 10.21272/legalhorizons.2020.i20.p159.

[26]   A. Zhuk, "Navigating the legal landscape of AI copyright: a comparative analysis of EU, US, and Chinese approaches," *AI and Ethics*, vol. 4, no. 4, pp. 1299–1306, 2024, doi: 10.1007/s43681-023-00299-0.

[27]   I. Y. Stanko, "Theoretical and legal analysis of the principles of law as an integrating element of the legal system," *Legal horizons*, vol. 33, no. 20, pp. 15–22, 2020, doi: 10.21272/legalhorizons.2020.i20.p15.

[28]   "Special Eurobarometer 551: The digital decade." European Commission, 2024, [Online]. Available: https://www.europa.eu/eurobarometer.

[29]   A. Engler, "The EU AI Act will have global impact, but a limited Brussels Effect," *Brookings*, 2022. https://www.brookings.edu/articles/the-eu-ai-act-will-have-global-impact-but-a-limited-brussels-effect/ (accessed Jul. 03, 2024).

[30]   "EU pact on migration and asylum: member's states." European Commission, pp. 1–5, 2024.

[31]   I. Sopilko and K. Tokarieva, "Epistemological Development of administrative-legal principles in research on law enforcement agencies," *Journal of International Legal Communication*, vol. 11, no. 4, pp. 33–43, 2023, doi: 10.32612/uw.27201643.2023.11.4.pp.33-43.

[32]   J. P. Meltzer and A. Tieleman, "The European Union AI Act: next steps and issues for building international cooperation in AI," *Brookings*, 2022. https://www.brookings.edu/articles/the-european-union-ai-act-next-steps-and-issues-for-building-international-cooperation-in-ai/ (accessed Jul. 05, 2024).

[33] N. Medvedenko and O. Medvedenko, "Features of analysis and modeling of management processes in law enforcement," *Journal of International Legal Communication*, vol. 11, no. 4, pp. 55–64, 2023, doi: 10.32612/uw.27201643.2023.11.4.pp.55-64.

[34] R. I. Tashian, Y. S. Tavolzhanska, O. V. Tavolzhanskyi, S. V. Grynchak, and N. V. Smetanina, "Scientific doctrine as a source of law in international law and legal systems of the world," *Revista Juridica Portucalense*, no. special issue, pp. 232–252, 2023, doi: 10.34625/issn.2183-2705(ne)2023.ic-12.

[35] "The second quantum revolution: the impact of quantum computing and quantum technologies on law enforcement," 2023.

[36] Y. Popko, "Development of the State jurisdictional immunity institution in private international law," *Legal Horizons*, vol. 17, no. 2, pp. 051–063, 2023, doi: 10.54477/lh.25192353.2023.2.pp.051-063.

[37] J. Mökander, P. Juneja, D. S. Watson, and L. Floridi, "The US algorithmic accountability act of 2022 vs. the EU artificial intelligence act: what can they learn from each other?," *Minds and Machines*, vol. 32, no. 4, pp. 751–758, 2022, doi: 10.1007/s11023-022-09612-y.

[38] M. A. Pozhydaeva, "Evolution of the use of electronic payment instruments: financial and legal aspect," *Legal horizons*, no. 20, pp. 82–87, 2020, doi: 10.21272/legalhorizons.2020.i20.p82.

[39] N. O. Popova, "International legal regulation of artificial intelligence: current status and prospects," *Juridical scientific and electronic journal*, no. 4, pp. 443–447, 2024, doi: 10.32782/2524-0374/2024-4/105.

[40] V. Galaz *et al.*, "Artificial intelligence, systemic risks, and sustainability," *Technology in Society*, vol. 67, p. 101741, Nov. 2021, doi: 10.1016/j.techsoc.2021.101741.

[41] V. V. Myrgorod-Karpova and Y. A. Shevtsov, "E-government in Ukraine: current achievements, reform issues and activities of the Ministry of digital transformation of Ukraine," *Legal horizons*, no. 22, pp. 35–42, 2020, doi: 10.21272/legalhorizons.2020.i22.p35.

BIOGRAPHIES OF AUTHORS

Tamara Kortukova is a specialist in international law. She is an Associate Professor at the Department of International Civil and Commercial Law, where she inspires and educates students, paving the way for the next generation of legal scholars and professionals. She has been appointed as a Member of the Expert Council at the Commission of Verkhovna Rada of Ukraine on Human Rights, that allows her to contribute to the development and enhancement of human rights policies within her country. She has also been honored as a Member, Leader, and Trainer of various Jean Monnet Projects, showcasing her expertise in EU legislation. This role provides her with the opportunity to share the understanding of EU legislation, as well as contribute to the field through research and academic collaboration. She actively engages with legal institutions, participates in conferences, and shares her knowledge through various publications both nationally and internationally. She can be contacted at email: t.kortukova@ukr.net.

Maryna Dei received her Ph.D. in law (Candidate of Juridical Sciences, specialty 12.00.05) in 2002. She has held leading academic positions, including Professor at the National Aviation University (2018–2024), Head of the Department of Education and Law at the University of Educational Management (2016–2018), and Dean of the Faculty of International Relations at the Kyiv University of Law, NAS of Ukraine (2010–2015). She has over 20 years of experience in legal education, curriculum development, and international academic cooperation. Her research interests include international law, European integration, labor and social security law, cross-border legal relations, and academic policy. Prof. Dei is regularly participates in Erasmus + mobilities and international projects focused on legal modernization and education. She can be contacted at email: maryna.dei@npp.nau.edu.ua.

Volodymyr I. Kudin a graduate of Taras Shevchenko State University of Kyiv, he studied applied mathematics, laying the foundation for his future contributions to the field. His academic journey includes the successful defense of a Ph.D. thesis on the development and application of procedures for analyzing large-scale linear programming models, followed by a doctoral dissertation focused on numerical algorithms for linear model analysis based on the basis matrix method. His professional path began in 1977 as a Software Engineer at the Kyiv Branch of the Scientific Production Association "Chimautomatics". He then continued as a Senior Mathematical Engineer at the Republican Information Computing Center of the Ministry of Procurement. From 1983 to 1999, he advanced through research positions at the Glushkov Institute of Cybernetics of the National Academy of Sciences of Ukraine, contributing to key developments in the field. Between 1999 and 2015, he served as a senior and then leading researcher in the Laboratory of Computational Methods in Mechanics of Solid Media at Taras Shevchenko National University of Kyiv, where he played an essential role in advancing numerical methods and their application in engineering and the natural sciences. His career reflects a deep commitment to scientific progress, education, and the practical application of technical knowledge. He can be contacted at email: Volodymyr_kudin@edu-knu.com.

Andrii Onyshchenko graduate of Volodymyr Korolenko Poltava National Pedagogical University, he earned his degree as a teacher of mathematics and computer science, which laid a strong interdisciplinary foundation for his academic and research career. His scholarly journey began with the defense of a Ph.D. thesis in economic and mathematical modeling, where he focused on creating models for ecologically balanced economic development. He later earned his Doctor of economic sciences degree in the specialty of mathematical methods, models, and information technology in economics, with a dissertation dedicated to ecological and economic modeling in the context of implementing the provisions of the Kyoto Protocol. From 2003 to 2008, he worked at Yuriy Kondratyuk Poltava National Technical University, holding positions as assistant, senior lecturer, and assistant professor. Between 2008 and 2011, he pursued doctoral studies at Taras Shevchenko National University of Kyiv. He then joined the National Technical University of Ukraine "Kyiv Polytechnic Institute" as an Assistant Professor from 2011 to 2014, continuing his contributions to academic teaching and research. He can be contacted at email: andriy.onyshchenko@ukr.net.

Petro Kravchuk graduated from the Law Faculty of Kharkiv National University of Internal Affairs and the Faculty of Finance of the National Academy of the State Tax Service of Ukraine. In 2015, he defended his dissertation on the topic: "The use of special knowledge in the investigation of robberies and assaults" and received a Ph.D. in law in the specialty 12.00.09 "criminal procedure, criminalistics, forensic science, operational and investigative activities". In 2019, he was awarded the academic title of associate professor. Author of more than 50 scientific publications. He can be contacted at email: p.kr@ukr.net.