International Scientific Conference
UNITECH`2024

BUILDING TRUST IN AI: THE EU'S PATH TO HARMONIZED LEGAL FRAMEWORKS

Violeta Stojanović [1], Ratko Ivković [2,3], Nikola Milić[3], Dijana Kostić[4], Bojan Prlinčević[5], Zoran Milivojević[6]

[1] Department of Environmental Protection Academy of Applied Technical and Preschool Studies, Niš, Serbia;
[2] Department of Software Engineering, Faculty of Economics and Engineering Management, University Business Academy in Novi Sad, Novi Sad, Serbia;
[3] Department of Information Technology, MB University, Belgrade, Serbia;
[4] Šargan inženjering d.o.o, Niš, Serbia;
[5] Department of Information Technology Kosovo and Metohija Academy of Applied Studies, Leposavić, Serbia;
[6] Engineering Academy of Serbia, Department of Electrical and Computer Engineering, Belgrade, Serbia;

** Corresponding author: koricanac@yahoo.com*

Abstract

This paper analyses the legal framework for artificial intelligence (AI) in the European Union, focusing on the recently adopted Artificial Intelligence Act (AI Act) of 2024. The Act employs a risk-based classification approach to regulate AI systems, particularly high-risk ones, to safeguard public safety and fundamental rights. Additionally, it examines the Act's alignment with Directive (EU) 2019/770, which establishes complementary standards for AI-based software products through continuous updates and transparency. Through this legislation, the EU sets global standards for responsible AI development, fostering a secure digital ecosystem aligned with societal values and user rights.

Keywords: Artificial Intelligence, EU Artificial Intelligence Act, Software Products, Legal Framework, EU Directive 2019/770

INTRODUCTION

In the contemporary landscape of technological advancement, artificial intelligence (AI) has emerged as a transformative force across multiple sectors. From healthcare to finance, AI's rapid development has led to its widespread adoption, influencing innovation and operational practices. However, this proliferation of AI technologies has also highlighted significant legal and ethical concerns, particularly regarding the obligations and responsibilities of AI developers and users. As emphasized in recent studies, such as the analysis presented by the Law, Technology, and Policy journal, the need for comprehensive regulatory frameworks has never been more critical in addressing these challenges [1]. The European Union has responded to this necessity with the adoption of the Artificial Intelligence Act (AI Act) on August 1, 2024, marking a significant milestone in AI regulation. This groundbreaking legal framework classifies AI systems based on their potential risk to fundamental rights and public safety, implementing stringent controls, particularly for high-risk AI applications. High-risk systems, including those employed in sectors like healthcare or automated decision-making, must adhere to rigorous standards involving transparency, risk management, and ongoing human oversight [2] [3]. The AI Act works in concert with other EU directives, such as Directive (EU) 2019/770 which governs the

doi: www.doi.org/10.70456/JZUD1984

contractual obligations for digital content and services providers [4]. This directive mandates that AI-based software products undergo continuous updates to maintain their compliance with evolving technical standards and security requirements. The synergy between these legal instruments aims to safeguard users while promoting responsible AI development within the European digital ecosystem. Despite the advancements brought by the AI Act, its implementation raises several complex issues, such as distinguishing between mandatory updates and product enhancements [5] [6]. These challenges underscore the importance of clearly defined guidelines to ensure that AI systems remain secure, transparent, and aligned with ethical standards throughout their lifecycle. This paper seeks to delve deeper into these legal and practical dimensions, offering a comprehensive analysis of how the AI Act reshapes the landscape of AI-based software regulation.

EU AI GOVERNANCE: STRUCTURE AND EVOLUTION

Over the past two decades, the EU's approach to artificial intelligence (AI) governance has transformed from general regulations to a targeted, comprehensive framework. Initial policies were dispersed across sectors, including data protection, competition, and product liability [7]. A key milestone was the General Data Protection Regulation (GDPR) in 2018, which, though not AI-specific, established foundational principles of transparency, consent, and accountability, influencing future AI legislation.

By 2020, the European Commission pursued a coordinated AI strategy, promoting innovation while addressing ethical concerns. This led to the 2021 proposal and 2024 adoption of the Artificial Intelligence Act (AI Act), the world's first comprehensive AI regulatory framework. The Act categorizes AI systems into four risk levels—unacceptable, high, limited, and minimal—each with specific compliance requirements. High-risk systems, such as those in healthcare and law enforcement, face stringent obligations for risk management, data governance, and transparency, while "unacceptable" risk applications, like social scoring, are prohibited.

The EU's rights-based approach differentiates its framework from those of other global powers, emphasizing alignment with European values of accountability, fairness, and public trust. Extending beyond EU borders, the AI Act requires any AI system used within the EU to adhere to its standards, setting a global benchmark. The European Artificial Intelligence Board, established under the Act, ensures ongoing regulatory adaptability and harmonization across member states, reinforcing the EU's leadership in ethical AI governance.

COMPLIANCE REQUIREMENTS FOR AI SOFTWARE PROVIDERS IN THE EU

The European Union's Artificial Intelligence Act (AI Act) establishes a stringent set of compliance requirements for organizations that develop and deploy AI systems within its jurisdiction. This regulatory framework is specifically designed to ensure that AI technologies adhere to the principles of safety, transparency, and accountability while supporting responsible innovation in critical sectors. Under the AI Act, AI systems are categorized based on their level of risk to public safety and fundamental rights, with high-risk systems facing the most stringent regulations. Software providers developing these high-risk AI systems must implement comprehensive risk management protocols that address potential vulnerabilities at every stage of the AI lifecycle. This involves detailed assessments of data quality, algorithmic biases, security threats, and the potential impact on users, all of which must be continually updated to reflect evolving technological landscapes. One of the cornerstones of these obligations is the requirement for high-risk AI systems to undergo rigorous data governance procedures. Developers are mandated to use high-quality, unbiased data sets to train and validate their AI models, ensuring that outcomes are fair and free from discriminatory biases. These data sets must be carefully selected and continually monitored to maintain their relevance and accuracy, minimizing the risks associated with flawed or outdated information. In addition to data governance, software providers are required to maintain comprehensive technical documentation for their AI systems. This documentation serves as a detailed record of the system's design, development, testing, and deployment processes, and must be readily accessible to regulatory authorities upon request. The objective is to ensure transparency in how AI systems function, providing a clear audit trail that demonstrates compliance with the AI Act’s standards. Transparency extends beyond technical documentation; it also encompasses user interaction with AI systems. Providers must clearly inform users when they are engaging with an AI-driven system, particularly when these interactions have the potential to affect users' rights or well-being. This includes explaining the AI’s purpose, limitations, and any significant risks associated with its use in a way that is easily understandable even to non-expert users. Human oversight is another fundamental aspect emphasized by the AI Act. Software providers must integrate mechanisms that allow human operators to intervene in or override the AI system’s decisions when necessary, especially in high-stakes applications like healthcare or law enforcement. This requirement ensures that AI systems do not operate in isolation and that their decisions can be reviewed or altered to prevent unintended consequences. Before high-risk AI systems can be launched into the market, they must pass through a pre-market conformity assessment process. This evaluation verifies that the AI system complies with all applicable safety and ethical standards laid out by the AI Act. Such assessments are critical in mitigating potential risks and ensuring that AI solutions meet the Union’s strict guidelines before they reach end-users. For General-Purpose AI systems (GPAI), which can be adapted for various applications beyond their initial design, the compliance requirements are even more nuanced. Providers must implement continuous risk assessments, conduct regular system evaluations, and report any incidents that may compromise user safety or violate EU standards. This ongoing monitoring is essential to uphold the integrity of GPAI systems as they evolve and are repurposed for different uses. Violations of these obligations carry severe penalties, with fines reaching up to €35 million or 7% of a company’s global annual revenue, whichever is higher. This penalty structure underscores the EU’s commitment to holding software providers accountable and ensuring that AI technologies are developed and deployed with the utmost responsibility and care. By setting these high standards, the AI Act aims to position the European Union at the forefront of ethical AI governance, balancing the need for technological innovation with the imperative of safeguarding public trust and individual rights.

REGULATORY STANDARDS FOR VERSATILE AI TECHNOLOGIES

The regulation of General-Purpose AI systems (GPAI) under the European Union’s Artificial Intelligence Act presents unique challenges due to their versatility and adaptability across multiple sectors. Unlike specialized AI applications, these systems are designed to perform a broad range of tasks, making it essential for regulatory measures to be comprehensive yet flexible to accommodate diverse use cases. Providers of GPAI must adopt a proactive approach to risk management, continually evaluating the system's performance and identifying potential vulnerabilities that could arise from its deployment in different contexts. This involves implementing thorough risk assessments that not only consider the immediate functionality of the AI but also anticipate long-term implications, including ethical considerations, security threats, and unintended biases. Detailed technical documentation is a mandatory requirement for GPAI systems, serving as a blueprint that outlines the AI model's architecture, data sources, training methodologies, and adaptation strategies. This documentation is not just a regulatory formality; it acts as a crucial tool for ensuring transparency and accountability, providing a clear record of how these systems are developed and how they can be safely integrated into various environments. One of the core obligations for GPAI developers is to maintain ongoing monitoring and evaluation protocols. Given the dynamic nature of these AI systems, continuous auditing is necessary to ensure that they adhere to the latest standards of safety, reliability, and ethical use. This includes tracking the AI's decision-making processes, identifying any deviations from expected behavior, and implementing corrective measures promptly to mitigate risks. Incident reporting is another critical aspect of compliance for GPAI. Providers must have robust mechanisms in place to detect, document, and report any malfunctions or safety breaches to the relevant authorities. This process ensures that issues are addressed swiftly before they can escalate into significant problems that might impact users or compromise data integrity. Data governance also plays a pivotal role in managing GPAI systems. Developers are required to use high-quality, legally compliant datasets that reflect diversity and inclusivity to prevent bias and discriminatory outcomes. The AI Act stipulates strict guidelines on data handling, ensuring that the information used to train these models is both accurate and representative of the populations they affect, thereby reducing the risk of biased or unfair results. In line with the EU's commitment to ethical AI, GPAI systems must also prioritize transparency in their interactions with users. Providers need to ensure that users are fully aware when they are engaging with an AI-driven tool, particularly when such systems influence significant decisions in areas like healthcare, finance, or employment. Clear disclosures about the AI's role, its limitations, and the logic behind its outputs are essential to maintain user trust and to comply with EU transparency standards. To uphold these stringent requirements, the AI Act mandates that developers of GPAI systems undertake a lifecycle approach to compliance, continuously adapting their strategies in response to new risks and regulatory updates. This iterative process not only helps to maintain the AI's effectiveness but also ensures that it evolves in line with emerging technological and legal landscapes.

HARMONIZING AI REGULATIONS WITH DIRECTIVE (EU) 2019/770

The convergence of the EU Artificial Intelligence Act (AI Act) and Directive (EU) 2019/770 represents a strategic effort by the European Union to create a seamless regulatory environment for digital products and AI technologies. While these two legislative instruments address distinct aspects of digital and AI governance, their combined application aims to ensure that AI-powered solutions are both legally compliant and technologically sound. Directive (EU) 2019/770, often referred to as the Digital Content Directive, primarily focuses on defining the obligations of providers when supplying digital products, including software and AI-based services. Its key objective is to protect consumers by setting clear standards for the quality, functionality, and security of digital products. This directive mandates that software providers deliver regular updates and maintain the integrity of their products, ensuring that they conform to the agreed contractual terms throughout the product's lifecycle. On the other hand, the AI Act introduces a layered approach to AI regulation, categorizing AI systems by their level of risk. Its emphasis is on managing the ethical and safety concerns related to AI technologies, particularly those classified as high-risk. The Act imposes stringent requirements for transparency, accountability, and human oversight, especially in scenarios where AI systems could significantly impact public safety or individual rights. The integration of these two frameworks is not merely a coincidence but a deliberate strategy to create a holistic approach to digital governance. By aligning the principles of the Digital Content Directive with the AI-specific regulations of the AI Act, the EU aims to cover all aspects of AI deployment, from technical compliance to ethical considerations. This ensures that AI-based digital products are not only efficient and innovative but also secure, reliable, and aligned with user expectations. One of the critical intersections between these regulations lies in the area of software updates. Under Directive (EU) 2019/770, providers are obligated to issue updates to their digital products to ensure ongoing compliance with safety and performance standards. The AI Act complements this by adding an extra layer of requirements specifically for high-risk AI systems, which must undergo regular risk assessments and updates to maintain their operational integrity and safeguard against emerging threats. This combined regulatory framework also addresses the complexities involved in distinguishing between "updates" and "enhancements" of AI systems. While the Digital Content Directive focuses on the contractual obligation to provide updates that keep software functioning as promised, the AI Act introduces a nuanced view that considers both technological upgrades and the ethical implications of such changes. This dual approach ensures that any modifications to AI systems enhance their functionality without compromising user safety or introducing new risks. The AI Act and Directive (EU) 2019/770 work together to promote transparency in AI-driven digital services. Providers must not only ensure that their AI systems are understandable and fair but also that they provide clear communication to users about the role and limitations of these technologies. This transparency is essential for fostering trust in AI applications, especially in sensitive areas such as healthcare, finance, and public administration. By harmonizing these two sets of regulations, the EU establishes a unified legal framework that guides the development, deployment, and maintenance of AI-driven digital products. This comprehensive approach not only protects consumers but also supports innovation by providing clear guidelines for businesses to follow, reducing legal uncertainties and fostering a competitive digital market. Ultimately, the alignment between the AI Act and Directive (EU) 2019/770 reflects the EU’s broader vision of creating a safe and trustworthy digital ecosystem. It underscores the Union's commitment to setting global standards in AI and digital governance, ensuring that technological advancements do not come at the expense of ethical values or consumer rights.

CONCLUSION

The adoption of the EU Artificial Intelligence Act (AI Act) in 2024 signifies a transformative shift in how AI technologies are regulated, aligning technological progress with ethical standards and user safety. This legislation, combined with Directive (EU) 2019/770, establishes a robust framework that balances innovation with accountability, ensuring AI's integration into society does not compromise fundamental rights or public trust. By categorizing AI systems according to their risk levels, the AI Act enforces tailored compliance measures, particularly for high-risk applications. This nuanced approach highlights the EU’s dedication to fostering an ecosystem where AI development thrives within clearly defined boundaries, harmonizing technological capabilities with societal values. A crucial aspect of this regulatory landscape is the dual focus on continuous updates and transparency, as mandated by both the AI Act and the Digital Content Directive. This synergy between the two frameworks promotes a dynamic yet secure environment for AI-based digital products, encouraging their evolution while protecting consumers. Challenges remain in distinguishing between routine updates and significant enhancements, but the EU's adaptable guidelines aim to refine these aspects as AI technologies advance. The interaction between these regulations represents more than just legal oversight; it embodies the EU's strategic vision to position itself as a global leader in ethical AI governance. This comprehensive approach ensures that AI systems are not only compliant with current standards but are also designed to anticipate future challenges, fostering a culture of responsible innovation. As AI continues to evolve, the EU's commitment to refining its regulatory frameworks will be essential to addressing new risks, guiding sustainable development, and maintaining its role as a standard-bearer in digital ethics.

REFERENCE

[1] Ivković R, Ječmenić M. Obligation to update digital products in delivery agreements, PTP, vol. 41, no. 2, pp. 136–152, Jul. 2024.

[2] European Commission, Artificial Intelligence Act, Official Journal of the European Union, Aug. 2024, available at: https://ec.europa.eu/ai-act.

[3] European Parliament, Directive (EU) 2019/770 on contracts for the supply of digital content and digital services, Official Journal of the European Union, May 2019.

[4] Buchman F, Panfili C, Das neue Schuldrecht 2022 - Teil 2: Aktualisierungen bei digitalen Produkten, Kommunikation und Recht, vol. 25, no. 3, pp. 159-168, 2022.

[5 White & Case LLP, Long awaited EU AI Act becomes law after publication in the EU's Official Journal, Aug. 2024, available at: https://www.whitecase.com.

[6] European Commission, Excellence and trust in artificial intelligence,Press Release, Aug. 2024, available at: https://digital-strategy.ec.europa.eu.

[7] Lunk T, Meurer F, Dringender Handlungsbedarf für Unternehmen durch neue BGB-Vorschriften, Betriebs-Berater, vol. 77, no. 8, pp. 387-395, 2022.