

**PROSPECTIVE REGULATION OF ARTIFICIAL INTELLIGENCE IN THE EUROPEAN UNION AND ITS POSSIBLE IMPLICATIONS FOR UKRAINE**

**Vladyslav Teremetskyi<sup>1</sup>, Yurii Burylo<sup>2</sup>, Mykola Stefanchuk<sup>3</sup>, Olha Zozuliak<sup>4</sup>, Zhanna Udovenko<sup>5</sup>, Dmitro Zhuravlov<sup>6</sup> and Yevheniia Duliba<sup>7</sup>**

<sup>1</sup>Doctor in Law, Professor, leading research scientist of the Department of International Private Law, Academician F.H. Burchak Scientific Research Institute of Private Law and Entrepreneurship, National Academy of Legal Sciences of Ukraine, Kyiv, Ukraine

<sup>2</sup>Doctor in Law, Associate Professor, leading researcher of the Department of International Private Law, Academician F.H. Burchak Scientific Research Institute of Private Law and Entrepreneurship, National Academy of Legal Sciences of Ukraine, Kyiv, Ukraine

<sup>3</sup>Doctor in Law, Professor, leading researcher of Department of Private Law Problems, Academician F.H. Burchak Scientific Research Institute of Private Law and Entrepreneurship, National Academy of Legal Sciences of Ukraine, Kyiv, Ukraine

<sup>4</sup>Doctor in Law, Professor, head Scientific researcher of the laboratory, Academician F.H. Burchak Scientific Research Institute of Private Law and Entrepreneurship, National Academy of Legal Sciences of Ukraine, Kyiv, Ukraine.

<sup>5</sup>Doctor in Law, Associate Professor, Associate Professor of the Department of Criminal and Criminal Procedure Law of the National University of «Kyiv-Mohyla Academy», Kyiv, Ukraine

<sup>6</sup>Doctor in Law, Professor, Head of the Department on Amnesty Issues of the Office of the President of Ukraine, Kyiv, Ukraine

<sup>7</sup>Doctor in Law, Professor, professor of the Department of Constitutional Law and Field-Related Disciplines, Institute of Law, National University of Water and Environmental Engineering, Rivne, Ukraine.

<sup>1</sup>ORCID ID: <https://orcid.org/0000-0002-2667-5167>, <sup>2</sup>ORCID ID: <https://orcid.org/0000-0001-8743-7739>,

<sup>3</sup>ORCID ID: <http://orcid.org/0000-0002-2983-2770>, <sup>4</sup> ORCID ID: <https://orcid.org/0000-0002-6108-4442>,

<sup>5</sup>ORCID ID: <https://orcid.org/0000-0002-4100-0723>, <sup>6</sup>ORCID ID: <https://orcid.org/0000-0002-2205-6828> and

<sup>7</sup>ORCID ID: <https://orcid.org/0000-0003-2651-4977>

**ABSTRACT**

*The purpose of the article is to assess the main provisions of the draft Artificial Intelligence Act as well as the implications of its adoption for the EU candidate countries like Ukraine. The methodology of the study includes the method of system analysis and synthesis, the historical legal method as well as the comparative legal method. It has been established that the prospective legal regulation of artificial intelligence in the EU is aimed at preventing harm to individuals from artificial intelligence while fostering innovation and investment in this field. This is expected to be achieved following a risk-based approach, which allows to lay down different legal requirements and obligations for different categories of artificial intelligence systems depending on the level of risk they pose for the safety and fundamental rights of people. Besides, it has been concluded that despite all imperfections of the draft Artificial Intelligence Act its adoption will be a major step forward. It has also been concluded that the new regulation of artificial intelligence in the EU will have significant implications for further development of the national law (both public and private) of the EU candidate countries like Ukraine having to bring its national legislation in line with the relevant EU law.*

*Keywords: artificial intelligence, AI systems, EU law, risk-based approach, legislative alignment*

**RESUMEN**

El propósito del artículo es evaluar las principales disposiciones del proyecto de Ley de Inteligencia Artificial, así como las implicaciones de su adopción para los países candidatos a la UE como Ucrania. La metodología del estudio incluye el método de análisis y síntesis de sistemas, el método jurídico histórico y el método jurídico comparado. Se ha establecido que la futura regulación legal de la inteligencia artificial en la UE tiene como

objetivo prevenir daños a las personas debido a la inteligencia artificial y al mismo tiempo fomentar la innovación y la inversión en este campo. Se espera lograrlo siguiendo un enfoque basado en el riesgo, que permita establecer diferentes requisitos y obligaciones legales para diferentes categorías de sistemas de inteligencia artificial en función del nivel de riesgo que plantean para la seguridad y los derechos fundamentales de las personas. Además, se concluyó que, a pesar de todas las imperfecciones del proyecto de ley sobre inteligencia artificial, su aprobación será un gran paso adelante. También se ha concluido que la nueva regulación de la inteligencia artificial en la UE tendrá implicaciones significativas para un mayor desarrollo de la legislación nacional (tanto pública como privada) de los países candidatos a la UE, como Ucrania, que tendrán que adaptar su legislación nacional a las normas pertinentes. Derecho de la UE.

**Palabras clave:** inteligencia artificial, sistemas de IA, legislación de la UE, enfoque basado en riesgos, alineación legislative

## 1. INTRODUCTION

Artificial intelligence (AI) is no longer science fiction. It is already changing the landscape of the modern world, even though it is still at the initial stage of its evolution. Its future impact on our daily lives can hardly be overestimated. Clearly, AI has the potential to transform the economy, society and many other fields. According to some studies the use of AI and related technologies can even have some far-reaching consequences for the climate and the environment (Galaz et al., 2021). It's no surprise that AI is already a huge industry that is growing at a tremendous pace. In 2023 the global AI market was valued at 150.2 billion USD with a prospect of compound annual growth rate at 36.8% till 2030 (Artificial Intelligence Market, 2023).

It is clear that as an emerging technology AI can bring about a lot of benefits for the mankind. At the same time, it can also cause a lot of damage. This gives rise to numerous concerns over its safety for individuals, fundamental rights violations as well as its negative effects on the society in general. Hence, there is a question of how to control AI in order to prevent its harmful effects. Naturally, when it comes to introducing control over something there need to be some rules and that's where law has a major role to play.

As AI is transforming various industries, markets and the lives of ordinary people the national governments around the world as well as some supra-national organizations like the European Union are beginning to consider the introduction of legal regulation for AI. The authorities in the USA, China and the EU are exploring different ways of using the law as a tool to control the development, placing on the market and use of AI. So far, their search for the best approach to regulate AI has not resulted in the adoption of any rules and regulations due to a large extent to the novelty and complexity of AI as well as the business interests of AI industry's stakeholders.

However, compared to other countries the EU has made the biggest progress in terms of preparation for the introduction of a legal framework for regulating AI. The European Commission first presented its draft regulation on AI, which is commonly known as the AI Act, in April 2021. Following the adoption of the common position by the Council in December of 2022 and the negotiating position by the Parliament in June of 2023 (Artificial intelligence act, 2023) the Council and the Parliament reached a provisional agreement on the AI Act on 9 December 2023. Now the AI Act is supposed to be finally adopted by both the Parliament and the Council in order to become the law (EU AI Act: first regulation on artificial intelligence, 2023).

After it is adopted the AI Act will lay down a comprehensive legal framework for AI in the EU. Moreover, it will act as a guidance for the development of relevant national laws in countries aspiring for the EU membership. Therefore, the purpose of this study is to highlight the most important provisions of the draft AI Act and figure out its possible implications for the EU-candidate countries like Ukraine.

## 2. METHODOLOGY

The methods of scientific research used in this study comprise the method of system analysis and synthesis, historical legal method as well as comparative legal method. Using system analysis and synthesis the problems of preparing a legal framework for artificial intelligence are examined and as a result conclusions and solutions to

the identified problems are suggested. This method is also used for analyzing various proposals regarding legal regulation of artificial intelligence. The historical legal method is used for the examination of the main stages in the process of preparation and adoption of the AI Act. The application of the comparative legal method allows to find differences and similarities in the proposals to the draft AI Act prepared by different EU institutions.

### **3. LITERATURE REVIEW**

In recent years AI has been the focus of attention of many researchers. In particular systemic risks created by the development of AI were examined by V. Galaz, M.A. Centeno, P.W. Callahan, A. Causevic, T. Patterson, I. Brass, S. Baum, D. Farber and others (Galaz et al., 2021). The provisions of the draft AI Act were analyzed by N. Smuha, E. Ahmed-Rengers, A. Harkens, W. Li, J. MacLaren, R. Piselli, K. Yeung, M. Ebers, V. Hoch, F. Rosenkranz, H. Ruschemeier, B. Steinrötter, M. Veale, F. Zuiderveen Borgesius and many other legal experts (Smuha et al., 2021; Ebers et al., 2021; Veale, Zuiderveen Borgesius, 2021). Some legal issues of regulating biometric AI systems were considered by N. Santalu, issues concerning the regulation of AI systems generating deep fakes were scrutinized by M. Łabuz. and regulatory issues concerning generative AI in the draft AI Act were examined by M. Barani, D. Van Boven, and P. Van Dyck (Santalu, 2023; Łabuz, 2023; Barani, Van Boven, Van Dyck, 2023). However, due to the recent updates of the draft AI Act the legal research in this area is not complete yet. Besides, there is a need to assess the implications of the AI Act for further development of the national legislation of countries like Ukraine aspiring for the EU membership.

### **4. RESULTS AND DISCUSSION**

#### **General Approach to the Aegulation of AI**

As the EU may soon become the first regional economic power to set the standards for AI regulation, it is important understand the main objectives of this regulation. Based on the analysis of the proposal for the AI Act it is possible to say that the EU regulatory framework on AI aims on the one hand to ensure that AI systems placed on the EU market are safe for consumers and respect their fundamental rights as well as the values of the EU and on the other hand to ensure legal certainty in order to facilitate investment and innovation in AI (Proposal for a Regulation, 2021). Achieving those two goals simultaneously requires a complex and versatile legal regime that can address the concerns of individuals (AI users) and businesses (AI developers and providers) alike. This is a delicate balancing act and a challenging task for the EU authorities.

Since legal regulation of AI has to be sufficiently comprehensive and at the same time needs to have a clear scope it has to be based on a general definition of artificial intelligence. However, there is no such definition in the draft AI Act. Instead, there is a definition of an artificial intelligence system (AI system), which means software that is developed with one or more of the techniques and approaches listed in Annex I and can, for a given set of human-defined objectives, generate outputs such as content, predictions, recommendations, or decisions influencing the environments they interact with. The list of AI techniques and approaches in Annex I comprises machine learning approaches, including deep learning, logic- and knowledge-based approaches as well as statistical approaches. The main advantage of this legal definition is that it is technology-neutral, which is good for the AI industry, as it does not discriminate against any particular AI technology (Proposal for a Regulation, 2021).

However, as it is rightly pointed out by a number of legal scholars, this definition is incredibly broad, as it covers virtually all kinds of software algorithms, and the list of artificial intelligence techniques and approaches in Annex I does not make much of a difference, as logic-based and statistical approaches are not necessarily associated with artificial intelligence and can be used for simple automation purposes (Smuha et al., 2021, p.14). Therefore, in theory such a broad definition of AI systems can apply to most computer programs.

On the one hand it may be argued that such a broad definition of AI systems can contribute to better protection of the fundamental rights of AI users due to a wide coverage of potential threats stemming from all sorts of software (regardless of whether software applications are based on machine-learning, which is normally associated with artificial intelligence), on the other hand this may also result in overregulation (Ebers et al., 2021, p. 590).

Overregulation is not good for the AI industry as it hampers investment and innovation in AI. Therefore, it turns out that the current definition of AI systems in the draft AI Act is not fully in line with one of the main objectives of the proposed Regulation. So, there certainly needs to be a more specific definition of AI systems. Giving a more specific and precise definition of an AI system may in turn require a general definition AI and a more specific list of AI techniques and approaches (perhaps even confining this list to machine learning variations).

### **Different Legal Regimes for Different Levels of Risk**

Ensuring consumer safety and protecting fundamental rights of AI users while trying to foster investment and innovation in AI at the same time may seem like two different policies contradicting each other. Striking a balance between these two goals of the proposed AI Act requires a certain compromise, which as the draft AI Act itself implies can be achieved following a risk-based approach.

The regulatory framework for AI does not necessarily have to be the same for all types of AI systems. As some AI applications present more risks for the safety and fundamental rights of individuals than other AI applications, the stringency of the legal requirements for different types of AI systems must also be different. That's why the draft AI Act imposes different legal regimes for different types of AI applications depending on the level of risk they pose. To this end all AI systems are supposed to be divided into four risk-based categories, namely AI applications presenting unacceptable risk, high risk, limited risk, low or minimal risk.

The most harmful AI practices posing a direct threat to the safety and fundamental rights of individuals are banned by article 5 of the AI Act, proposed by the Commission. These practices include placing on the market, putting into service or use of AI systems that deploy subliminal techniques, AI systems that exploit any of the vulnerabilities of a specific group of persons due to their age, physical or mental disability, AI systems by public authorities for the evaluation or classification of natural persons for social scoring purposes as well as the use of the use of 'real-time' remote biometric identification systems in public places for law enforcement purposes with some exceptions (targeted search for potential crime victims, prevention of a threat to the life or physical safety of natural persons or of terrorist attacks, detection, localization, identification or prosecution of perpetrators or suspects of certain crimes) (Proposal for a Regulation, 2021).

Although the list of prohibited AI systems may seem quite impressive at first sight, many legal scholars point out that this list has a number of loopholes and does not go far enough to protect the safety and fundamental rights of people from the most dangerous AI applications.

Even though the draft AI Act prohibits manipulative AI practices involving subliminal techniques and exploitation of certain groups' vulnerabilities, such practices are considered illegal only when they cause or are likely to cause physical or psychological harm. However, a number of legal scholars rightly observed that there are other types of harm that can be caused by manipulative AI systems, such as, for instance, economic, cultural and collective harm etc. That's why they suggested that the prohibition of manipulative AI technologies should extend to all kinds of harm and human rights interference (Smuha et al., 2021, p. 21). Eventually, this issue has been addressed in the amendments to the draft AI Act, proposed by the European Parliament, which changed the wording from 'physical or psychological harm' to 'significant harm' (Amendments adopted by the European Parliament, 2023).

The ban on the use of AI systems for social scoring purposes also raises some questions, as it applies only to public authorities and does not apply to companies from the private sector. The use of such AI systems by private entities in some high-risk areas can also result in the violations of fundamental rights. For this reason, some experts and legal scholars express their concerns and call on the Commission to re-evaluate the potential risks from private social scoring applications and the way these risks are dealt with in the draft AI Act (Ebers et al., 2021, p.592). These concerns have apparently been heard by the members of the European Parliament, as public authorities are no longer mentioned in the amended text of the draft AI Act (Amendments adopted by the European Parliament, 2023).

Similar concerns have been raised with regards to the prohibition of ‘real-time’ remote biometric identification systems in publicly accessible spaces. According to the initial draft AI Act proposed by the Commission this prohibition would apply only to the use of such systems by law enforcement agencies. Therefore, this ban would not affect any other public or private entities. This piecemeal approach sparked a lot of debate. As a result, the European Parliament proposed a complete ban on the use of real time remote biometric identification AI systems in public spaces, affecting both private and public entities (Santalu, 2023). So, it remains to be seen which of these approaches prevails in the final text of the AI Act.

Another category of AI systems that is going to be regulated by the AI Act encompasses high-risk AI systems posing a significant hazard to the safety and fundamental rights of people. High-risk AI systems are no going to be banned in the EU. Instead, they will be subject to a set of legal requirements.

Under Title III of the draft AI Act there are two types of high-risk AI systems with some distinctions in their legal regimes. They include AI systems used as a safety component of a product, or are themselves products covered by the EU harmonization legislation (toys, radio equipment, pressure equipment, personal protective equipment, medical devices, agricultural and forestry equipment etc.) as well as AI systems used in the areas listed in Annex III (biometric identification and categorization of natural persons; management and operation of critical infrastructure; education and vocational training; employment, workers management and access to self-employment; access to and enjoyment of essential private services and public services and benefits; law enforcement; migration, asylum and border control management; administration of justice and democratic processes).

The main legal difference between those two types of high-risk AI systems stems from the requirements for conformity assessment. According to article 6 (1) of the draft AI Act the requirement for a third-party conformity assessment applies to high-risk AI systems that are safety components of products, or are themselves products, falling within the scope of the existing EU harmonization legislation (toys, lifts, medical devices etc.). At the same time, other high-risk AI systems, which are listed in Annex III, are subject to the conformity assessment procedure based on internal control (also known as self-assessment) by their providers. Besides, such stand-alone high-risk AI systems are also subject to the registration requirement, which means that their providers are expected to enter the necessary information about these AI systems into the relevant EU database, maintained by the Commission, before placing them on the market or putting them into service (Proposal for a Regulation, 2021).

Conformity of high-risk AI systems with the essential requirements of the draft AI Act can also be demonstrated by way of compliance with the relevant harmonized standards, developed by European standardization organizations. Due to the presumption of conformity with the essential requirements of high-risk AI systems complying with the harmonized standards the providers of such AI systems not have to meet conformity assessment requirements. As it has been rightly observed by legal experts, even though providers are not required by the draft AI Act to follow harmonized standards and can interpret its essential requirements by themselves, it is easier and cheaper for them to apply these standards and enjoy the presumption of conformity (Veale & Zuiderveen Borgesius, 2021, p. 105).

The essential requirements for high-risk AI systems are set out in Chapter 2 of Title III of draft AI Act. They include requirements regarding risk-management systems, criteria for data used for training models, technical documentation of high-risk AI systems, their logging capabilities, transparency and provision of information to users, human oversight, accuracy, robustness and cybersecurity. These requirements are complemented by the obligations of providers of high-risk AI systems laid down in Chapter 3 of Title III. In particular, operators have obligations to ensure that high-risk AI systems undergo the relevant conformity assessment procedures, prior to their placing on the market or putting into service; affix the CE marking to their high-risk AI systems to indicate the conformity with the requirements of the draft AI Act; take the necessary corrective actions, if the high-risk AI system is not in conformity with the established requirements etc. (Proposal for a Regulation, 2021).

In comparison with high-risk AI systems being subject to a great number of requirements AI systems posing limited risk are subject only to transparency requirements. In particular under the draft AI Act providers of AI systems intended to interact with natural persons (better known as ‘chatbots’) must ensure that such systems designed and developed in a way that allows to inform natural persons that they are dealing with chatbots, unless it is obvious from the circumstances and context of use. Unlike chatbots with the disclosure obligations imposed on their providers the use of emotion recognition systems and biometric categorisation systems implies the obligations of their users to inform people exposed to such systems of their operation.

Disclosure obligations also apply to users of AI systems generating or manipulating images, audio or video content that resembles existing persons, objects, places or other entities or events and may falsely appear to be authentic or truthful (better known as ‘deep fake’). According to article 52(3) of the draft AI Act proposed by the Commission the users of such AI systems are expected to disclose that the content has been artificially generated or manipulated (Proposal for a Regulation, 2021). At the same time, the amendments proposed by the European Parliament suggest that the name of the natural or legal person that generated or manipulated the content should also be disclosed whenever possible and the content itself must be appropriately labelled (Amendments adopted by the European Parliament, 2023). Moreover, considering the potential harm from deep fakes to fundamental rights there are currently debates on whether deep fake AI systems or at least some of them should be reclassified as high-risk AI systems. As a solution to this problem some experts suggest to single out the most harmful deep fakes and move them to a higher category of risk, which will allow to provide for additional protection of election candidates or even completely ban some deep fakes (for example, deep porn) (Łabuz, 2023, p. 29).

Despite all potential threats posed by AI systems the vast majority of AI applications, like spam-filters, purchase-recommendation systems or AI-assisted video-games etc., are relatively harmless. Therefore, they don’t really need to be regulated as rigorously as AI systems posing a higher level of risk. As article 69 of the proposed draft AI Act implies the providers of minimal-risk AI systems may voluntarily choose to adhere to the codes of conduct (Díaz-Rodríguez et al., 2023, p. 5). Following such codes of conduct the providers of minimal-risk AI systems apply the mandatory requirements for high-risk AI systems set out in Chapter 2 of Title III on a voluntary basis (Artificial intelligence act, 2023).

In recent years due to the rapid development of generative AI systems like ChatGPT capable of generating text, images and videos, it has become apparent that there is a need for special rules regarding such AI systems. There were no such rules in the initial draft AI Act proposed by the Commission in 2021. Nonetheless, these rules eventually appeared in the Parliament’s amendments in 2023 (Amendments adopted by the European Parliament, 2023). The Parliament suggested to define generative AI systems as a variety of foundation models intended to generate, with varying levels of autonomy, content such as complex text, images, audio, or video. As it can be inferred from the European Parliament’s amendments, generative AI systems are subject to three sets of requirements, including general requirements for AI systems, requirements for foundation models and specific requirements (obligations) for generative AI systems. The providers of generative AI systems will have specific obligations to train, design and develop the generative AI system in such a way that there are safeguards against the generation of illegal content, document and make available for the public a detailed summary of the use of training data protected by copyright and comply with stronger transparency requirements designed for chatbots (Barani, Van Boven, Van Dyck, 2023).

### **Governance and Enforcement**

The implementation of the provisions of AI Act will depend to a large extent on proper governance in the area of AI. Under the draft AI Act the governance structure includes the centralized EU level as well as the national level of the EU Member States. According to the draft AI Act the EU is planning to establish a European Artificial Intelligence Board, which is supposed to provide assistance and advice to the Commission and contribute to the cooperation of national supervisory authorities on matters concerning AI. For the purpose of ensuring the application and implementation of the AI Act at national level the EU Member States are expected to establish or designate the national competent authorities, which include the national supervisory authority, the notifying

authority and the market surveillance authority. The national supervisory authority will assume the powers of the national notifying authority and the market surveillance authority unless they are designated by the EU Member State.

The market surveillance authorities, as their name suggests, will have the responsibility to oversee the compliance of the AI systems' providers with their obligations and requirements for high-risk AI systems and investigate non-compliances. For this purpose, they will have full access to the training, validation and testing datasets used by the providers of AI systems. Furthermore, they can even gain access to the source code of a high-risk AI system upon request. In case non-compliance the marketing surveillance authority has the powers to order the AI system provider to take corrective actions such as bringing the AI system into compliance, withdraw it from the market or recalling it.

The enforcement of the provisions of the AI Act is expected to be strengthened with the application of penalties such as administrative fines. As it can be inferred from the amendments to the draft AI Act proposed by Parliament administrative fines may range from 40 million EUR (7 % of worldwide annual turnover in case of companies) for non-compliance with the prohibitions of the most harmful AI practices or 20 million EUR (4 % of worldwide annual turnover in case of companies) for non-compliance with data and data governance requirements to 5 million EUR (1 % of worldwide annual turnover) for providing incorrect, incomplete or misleading information to the competent authorities. Other enforcement measures along with or instead of fines may include non-monetary measures like orders and warnings (Amendments adopted by the European Parliament, 2023).

The draft AI Act proposed by the Commission was criticized for the lack of the right to lodge a complaint to and make use of judicial remedies against the national supervisory authority (Veale, Zuiderveen Borgesius, 2021, p. 111). This issue has been addressed in the amendments proposed by the European Parliament by completing the enforcement mechanism with two new articles on lodging complaints and using judicial remedies.

### **Implications for the National Law of Ukraine**

Since the signing of the Association Agreement with the EU Ukraine has been working hard to carry out reforms and bring its national legislation in line with EU law. After receiving its EU candidate status in June 2022 and opening accession negotiations in December 2023 (Ukraine. EU enlargement policy, 2023) Ukraine needs to pay even more attention to the alignment of its national law with EU law in order to meet the EU membership criteria. Therefore, sooner or later depending on when the AI Act is finally adopted by the EU, Ukraine will have to align its national law with the provisions of the AI Act. We want to emphasize that Ukraine has all the opportunities for further development of computer technologies and legislation that can work for the benefit of the country. There are already programs that have a certain set of AI characteristics and assist lawyers and judges before and during legal proceedings (Udoenko & Rudenko, 2023, p. 258). The same applies to all other EU candidate countries.

The legislative alignment with the EU in the field of AI will require the adoption of the relevant Law of Ukraine laying down provisions on the risk-based categorization of AI systems, their conformity assessment, requirements for training data, technical documentation, logging, transparency, human oversight, cybersecurity, providers' obligations etc. This will also require making numerous amendments to the existing legislation on information and communications technologies, data protection, governance, administrative fines etc.

Such comprehensive legislative changes will affect both public and private law of Ukraine. From the perspective of public law, the legislative developments will involve establishing the legal basis for the functioning of the national supervisory authority, the notifying authority and the market surveillance authority, providing for the possibility of lodging complaints, laying down rules on the application of administrative fines and other penalties etc. As for the private law it is essential to provide for protections against possible infringements of copyright and related rights covering all sorts of data used for training AI models as well as to ensure that there is a proper redress mechanism in the event damages or the violations of fundamental rights resulting from the use of AI systems.

## 5. CONCLUSION

In recent years the EU has made a significant progress in the development of the first comprehensive AI regulatory framework. Trying to find a balance between the need to ensure the safety and protect the fundamental rights of people on the hand and the need to foster investment and innovation in AI on the other hand, the draft AI Act employs a risk-based approach, which allows to impose legal requirements and obligations depending on the level of risk created by an AI system. Although the draft AI Act, proposed by the Commission, has a number of imperfections, such as the lack of the general definition of AI, loopholes in the list of prohibited AI practices, insufficient disclosure obligations for certain manipulative AI systems, lack of complaint mechanism and judicial remedies etc., many of which have already been addressed by the European Parliament, it is, nonetheless, a great step towards a safer and better future with AI.

The adoption of the AI Act by the EU will also have significant implications for the national law of Ukraine and other EU candidate countries. In particular, Ukraine will have to adopt its own law on AI and make amendments to the existing national legislation based on the relevant provisions of the AI Act. Along with the requirements for different risk-based categories of AI systems and the obligations of AI systems' providers the relevant legal changes will affect public law with regards to public governance, complaints, judicial remedies and penalties as well as private law regarding the protection of copyright and related rights covering training data and redress for damages caused by AI systems.

## 6. BIBLIOGRAPHIC REFERENCES

*Amendments adopted by the European Parliament on 14 June 2023 on the proposal for a regulation of the European Parliament and of the Council on laying down harmonised rules on artificial intelligence (Artificial Intelligence Act) and amending certain Union legislative acts.* (2023). Retrieved January 28, 2024, from [https://www.europarl.europa.eu/doceo/document/TA-9-2023-0236\\_EN.html](https://www.europarl.europa.eu/doceo/document/TA-9-2023-0236_EN.html)

*Artificial intelligence act. EU legislation in progress.* (2023). Retrieved January 28, 2024, from [https://www.europarl.europa.eu/RegData/etudes/BRIE/2021/698792/EPRS\\_BRI\(2021\)698792\\_EN.pdf](https://www.europarl.europa.eu/RegData/etudes/BRIE/2021/698792/EPRS_BRI(2021)698792_EN.pdf)

*Artificial Intelligence Market (AI) by Offering (Hardware, Software), Technology (ML (Deep Learning (LLM, Transformers (GPT 1, 2, 3, 4)), NLP, Computer Vision), Business Function, Vertical and Region – Global Forecast to 2030.* (2023). Retrieved January 28, 2024, from [https://www.marketsandmarkets.com/Market-Reports/artificial-intelligence-market-74851580.html?gad\\_source=1&gclid=Cj0KCCQiAtaOtBhCwARIsAN\\_x-3KyDeUT\\_mCYLryaXQNBC6Wk6NV7\\_z7gH5AkVb76SpHJg4ezTVwBHJAaApQOEALw\\_wcB](https://www.marketsandmarkets.com/Market-Reports/artificial-intelligence-market-74851580.html?gad_source=1&gclid=Cj0KCCQiAtaOtBhCwARIsAN_x-3KyDeUT_mCYLryaXQNBC6Wk6NV7_z7gH5AkVb76SpHJg4ezTVwBHJAaApQOEALw_wcB)

BARANI, M., VAN BOVEN, D., VAN DYCK, P. (2023). *GENERATIVE AI AND THE EU AI ACT - A CLOSER LOOK.* RETRIEVED JANUARY 28, 2024, FROM <HTTPS://WWW.ALLENOVERY.COM/EN-GB/GLOBAL/BLOGS/TECH-TALK/GENERATIVE-AI-AND-THE-EU-AI-ACT-A-CLOSER-LOOK#:~:TEXT=THE%20PARLIAMENT%20PROPOSAL.-,HOW%20DOES%20THE%20EU%20AI%20ACT%20DEFINE%20GENERATIVE%20AI%3F,USED%20FOR%20MAN Y%20DIFFERENT%20TASKS>

Díaz-Rodríguez, N., Del Ser, J., Coeckelbergh, M., López de Prado, M., Herrera-Viedma, E., Herrera, F. (2023). Connecting the dots in trustworthy Artificial Intelligence: From AI principles, ethics, and key requirements to responsible AI systems and regulation. *Information Fusion*, Vol. 99, <https://doi.org/10.1016/j.inffus.2023.101896>

Ebers, M.; Hoch, V.R.S.; Rosenkranz, F.; Ruschemeier, H.; Steinrötter, B. (2021). The European Commission's Proposal for an Artificial Intelligence Act—A Critical Assessment by Members of the Robotics and AI Law Society (RAILS), 4, 589-603. <https://doi.org/10.3390/j4040043>

*EU AI ACT: FIRST REGULATION ON ARTIFICIAL INTELLIGENCE.* (2023). RETRIEVED JANUARY 28, 2024, FROM <HTTPS://WWW.EUROPARL.EUROPA.EU/NEWS/EN/HEADLINES/SOCIETY/20230601STO93804/EU-AI-ACT-FIRST-REGULATION-ON-ARTIFICIAL-INTELLIGENCE>

Galaz, V., Centeno, M. A., Callahan, P. W., Causevic, A., Patterson, T., Brass, I., Baum, S., Farber, D., Fischer, J., Garcia, D., McPhearson, T., Jimenez, D., King, B., Larcey, P., & Levy, K. (2021). Artificial intelligence,



---

*International Journal of Applied Engineering & Technology*

---

systemic risks, and sustainability. *Technology in Society*, 67, Article 101741. <https://doi.org/10.1016/j.techsoc.2021.101741>

Łabuz, M. (2023). Regulating Deep Fakes in the Artificial Intelligence Act. *Applied Cybersecurity & Internet Governance*, 2(1), 1-42. <https://doi.org/10.60097/ACIG/162856>

*Proposal for a Regulation of the European Parliament and of the Council laying down harmonized rules on artificial intelligence (Artificial Intelligence Act) and amending certain union legislative acts* (2021). Retrieved January 28, 2024, from <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52021PC0206>

SANTALU, N. (2023). *BIOMETRICS UNDER THE EU AI ACT*. RETRIEVED JANUARY 28, 2024, FROM <HTTPS://IAPP.ORG/NEWS/A/BIOMETRICS-UNDER-THE-EU-AI-ACT/>

Smuha, N.A., Ahmed-Rengers, E., Harkens, A., Li, W., MacLaren, J., Piselli, R., Yeung, K. (2021). *How the EU Can Achieve Legally Trustworthy AI: A Response to the European Commission's Proposal for an Artificial Intelligence Act*. Retrieved January 28, 2024, from <https://ssrn.com/abstract=3899991>

Udovenko, Zh, Rudenko, N. (2023). *Advantages and isadvantages of the implementation of an artificial intelligence system in the judiciary of Ukraine*. *Current Issues in Modern Science* 4(10), 2023, 252-262.

*Ukraine. EU enlargement policy* (2023). Retrieved January 28, 2024, from <https://www.consilium.europa.eu/en/policies/enlargement/ukraine/>

Veale, M., Zuiderveen Borgesius, F. (2021). Demystifying the Draft EU Artificial Intelligence Act. *Computer Law Review International*, 4, 97-112. <https://arxiv.org/ftp/arxiv/papers/2107/2107.03721.pdf>