УДК 347.9:004.8
DOI 10.33244/2617-4154.1(18).2025.268-279

S. G. Denysiuk,
Doctor of Political Science, Professor,
Professor of the Department of International Law
and the rights of the European Union,
State Tax University
e-mail: s.h.denysiuk@dpu.edu.ua
ORCID ID 0000-0002-1489-2236;
V. P. Kononenko,
Doctor of Law Sciences,
Professor of the Department of International Law and
the rights of the European Union, State Tax University,
Associate Professor, Department of International
Economic Relations and Tourist Business,
V. N. Karazin Kharkiv National University.
Associated Member of the Center for Constitutionalism
and Human Rights of the European Humanities
University (Vilnius, Lithuania)
e-mail: v.kononenko@karazin.ua
ORCID ID 0000-0002-6461-7072

THE PROBLEM OF LEGAL RESPONSIBILITY FOR THE HARMFUL CONSEQUENCES OF USING ARTIFICIAL INTELLIGENCE SYSTEMS

The article explores the issue of legal responsibility for damage caused by the use of artificial intelligence (AI) systems. It discusses the phenomenon of the „responsibility gap“ and its impact on legal regulation. The article analyzes conceptual approaches to determining the subject of responsibility in the context of autonomous AI functioning and the specifics of its learning process.

The challenges of law enforcement arising from the probabilistic nature of AI's operation, its ability to self-learn, and the „black box“ problem are examined. Special attention is given to the issue of AI hallucination, when the system generates false or non-existent data, complicating the establishment of causal relationships and identifying the responsible party.

The article examines three main forms of „responsibility gap“: true gap, apparent gap, and the „dilution of responsibility“ caused by multi-level interactions of different subjects. Possible legal mechanisms for addressing these issues are analyzed, including the introduction of special responsibility regimes for AI developers, owners, and users.

The international experience of regulating AI is also discussed, with a focus on the provisions of the new European AI Act, which establishes a risk-based approach to responsibility. The conclusion is made about the need to adapt existing legal concepts and develop new regulatory models capable of accounting for the characteristics of autonomous systems.

Keywords: *artificial intelligence, legal responsibility, responsibility gap, civil liability, technological hallucination, law enforcement challenges.*

Problem Statement. The rapid development and widespread use of artificial intelligence (AI) systems pose significant challenges to legal responsibility frameworks. Traditional legal doctrines, based on clear attribution of fault and causality, struggle to accommodate AI's probabilistic decision-making, self-learning capabilities, and opaque „black-box“ mechanisms. The concept of the „responsibility gap“ (or „accountability gap“) has emerged as a central issue, highlighting difficulties in assigning liability when AI systems cause harm without a clear human agent responsible for their actions.

A particularly complex issue arises with AI hallucination, where AI-generated outputs include false, misleading, or non-existent information without a discernible causal link to human intent or technical error. This phenomenon exacerbates the challenge of legal accountability, as neither developers, system owners, nor end-users can be directly attributed responsibility in such cases.

Furthermore, the classification of responsibility gaps remains unresolved. This study differentiates between (1) true responsibility gaps, where accountability is objectively impossible due to AI's autonomous nature; (2) perceived responsibility gaps, resulting from current technological limitations but potentially solvable in the future; and (3) responsibility diffusion, where multiple actors (developers, operators, users) share indirect responsibility without clear attribution.

International legal frameworks, including the European AI Act, attempt to address these issues by imposing risk-based regulations. However, existing legal instruments remain insufficient in defining AI liability models. This article explores possible legal solutions, emphasizing the need for new regulatory mechanisms that ensure accountability while considering AI's unique characteristics.

The purpose of the article is to analyze legal liability for harm caused by artificial intelligence systems, focusing on the „liability gap“ in legal regulation.

The current state of research on the topic. Recently, the issue of liability for damage (losses) that may be caused by the use of artificial intelligence (AI) systems and applications has been actively discussed in philosophical and legal literature. Advances in AI development can be applied in fields such as design, marketing, and medicine, as well as for committing unlawful actions, particularly in the sphere of information relations. Moreover, there is a possibility that AI itself may pose a potential threat.

In English-language legal literature, the term „responsibility gap“ is commonly used, which translates as a „gap in liability“ or „liability loophole“. In Ukrainian legal scholarship, this concept has not yet been explored in the context of civil liability, and accordingly, the term is not widely used. Therefore, the issue of assigning liability for harm caused by AI remains one of the most debated topics in academic circles.

Both foreign (Dyson G. , Barrat James, Calo R., Kumparak G., Vinge V.) and Ukrainian (P. Andrushka, V. Bryzhko, V. Hryshchuk, M. Karchevskyi, V. Kharchenko, et al.) scholars have devoted attention to the issue of information security protection.

However, the impact of AI development on legal relations and the question of AI liability remain insufficiently studied.

Presentation of the main material. To begin with, it is essential to define the scope and terminology of the issue. For example, what exactly causes harm—technologies or systems? Why is it difficult to assign liability? Why is it challenging to identify the responsible party? What does the term "responsibility gap" mean? How do legal consequences vary depending on the technological causes involved in the development and use of AI?

Experts note that the „responsibility gap“ leads to impunity for those who cause harm and creates legal uncertainty. Logically, in the era of widespread digitalization, this issue becomes particularly pressing.

In international legal practice, the term „artificial intelligence system“ refers to a computer program that incorporates AI technology as a component [1]. However, Ukrainian legislation does not use the term „AI system“.

For the purposes of this article, AI systems will be considered as software-hardware complexes that utilize machine learning algorithms, neural networks, expert systems, or other methods to analyze data, make decisions, and perform tasks that traditionally required human intelligence.

Such systems include:

Autonomous agents (e.g., robotic systems, unmanned vehicles);

Generative models (e.g., ChatGPT, DALL·E, Midjourney);

Recommendation systems (e.g., Netflix, YouTube, Amazon);

Financial and legal algorithms (e.g., automated contract analysis and risk assessment systems);

Medical AI systems (e.g., disease diagnostics, personalized treatment).

Thus, „AI systems“ is a broad concept that encompasses various types of technologies capable of adapting, learning, and making decisions. In the context of legal liability, it is crucial to determine whether the discussion pertains to individual algorithms, integrated systems, or autonomous agents.

Of course, AI technologies do not inherently make independent decisions, which means that harm is typically caused by a person, organization, or state as a result of using an AI system or application [2]. It is well known that AI technologies function within AI systems, which is a key distinction between AI systems and conventional computer programs. The specificity of AI technology lies in the following aspects.

Firstly, all AI technologies inherently produce probabilistic outcomes. Machine learning models perform computations that yield a predictive value with a given level of accuracy, which is then used by humans to make decisions. The probabilistic nature of this value is an intrinsic characteristic of AI technologies. This can be referred to as the „inherent error of an AI model“.

From the perspective of legal liability, the probabilistic nature of AI-generated results means that there is no direct causal link between the harm caused and the actions of the individual responsible for ensuring effective control over AI systems and applications. This becomes particularly relevant when an AI system produces an incorrect result within the acceptable margin of error defined by the model.

Moreover, the architecture of an AI model is dynamic at the operational stage and may change during the learning process. This learning can take place either with human involvement (supervised learning) or without it (unsupervised learning) [2]. In the case of supervised learning, an individual using the model can exercise effective control by either adapting the AI model to new data or modifying it. This should be taken into account when determining liability for adverse consequences resulting from the use of a non-self-learning model.

However, human oversight becomes significantly more difficult when dealing with AI models that evolve autonomously within self-learning systems integrated into autonomous devices. This creates challenges in identifying the party responsible for damages caused by the actions of such autonomous AI-driven devices.

Thus, AI technologies possess several unique features that complicate the identification of a liable party. These include: the probabilistic nature of AI-generated results, which inherently contain errors that do not stem from human fault; the dynamic properties of software architecture, which allow AI models to change their behavior throughout their lifecycle; the operational integration of machine learning models into software or hardware-software systems, making it difficult to pinpoint the specific component responsible for system failures leading to adverse outcomes. These characteristics of AI technologies contribute to the „accountability gap“ [3].

The accountability gap is a consequence of the „blurring“ of technological control domains caused by the technological characteristics of a program or device. Accountability is a specific technological phenomenon. The category of fault must be applied to the appropriate entity, whose identification falls within the realm of technical expertise. When technical expertise cannot identify the perpetrator of the harm, the legal phenomenon of the „responsibility gap“ arises. This term is associated with the problem of assigning responsibility for harm caused by AI.

The classic rule for assigning any responsibility, including civil responsibility, correctly asserts that an agent can be considered responsible only if they know specific facts related to their actions and if they are capable of freely making a decision to act and choose one of the available alternative actions based on those facts [3].

However, AI systems and applications create a new situation where the manufacturer is unable to predict their future behavior, leading to the legal issue of assigning legal responsibility for harm caused by the use of AI systems and applications to specific individuals or parties, especially when no unlawful behavior is present. As a result, society faces a responsibility gap that cannot be overcome using traditional concepts of accountability [4].

The „responsibility gap“ as a legal problem was accurately described by A. Matthias in 2004. He identified the main cause of the emergence of „responsibility gaps“ as the ability of autonomous AI systems to learn [3]. That is, it concerns the ability of systems to self-develop.

However, the existence of the described problem of the „responsibility gap“ concerning the adverse consequences of AI usage is not recognized by all experts. Therefore, three main approaches to this issue can be identified. Proponents of the „fatalism“ approach (F. Antonio de Sio and G. Mecacci) regard the „responsibility gap“ as an unsolvable problem [4; 5]. Proponents of the „defeationism“ approach reject the problem of the „responsibility gap“ as erroneous [6]. Those who adhere to the opinion that the existing legal regulation of AI is sufficient can be classified as proponents of „defeationism“ [7].

The approach, according to which the „responsibility gap“ is recognized and proposed to be resolved through the introduction of new technical and/or legal tools, was referred to by F. Antonio de Sio and G. Mecacci as „resolutionism“, with two options for addressing this issue: technical and legal [4].

Currently, there is no generally accepted definition of the „responsibility gap“ in the context of AI usage. However, given the need to form a legal framework for the distribution of responsibility for harm caused by AI, the term "responsibility gap" may be used to describe a legal phenomenon characterized by difficulties in identifying the perpetrator of harm and holding specific individuals accountable. This concept should receive a clear doctrinal definition, and its causes should be classified to facilitate the search for ways to address the „responsibility gap“ through legal means [4]. Thus, the „responsibility gap“ is a legal situation in which it is impossible to clearly identify the entity responsible for a specific offense or harmful consequences arising from actions or omissions, particularly in the fields of new technologies, international law, or complex managerial decisions.

In the context of AI usage, the „responsibility gap“ may refer to a situation where it is unclear who should be held responsible for harm: the algorithm developer, the system owner, the user, or the system itself (which is currently legally impossible).

It is known that the legal elements of a general tort include: 1) the presence of harm; 2) the unlawful nature of the person’s behavior; 3) a causal link between the actions of the perpetrator and the harm; 4) the fault of the person who caused the harm.

When the use of AI technologies leads to a situation where the error cannot be attributed to a specific individual, it becomes impossible to establish certain elements of the legal composition of a tort: the unlawful nature of the behavior of the person(s) when none of the participants in the system or AI application lifecycle has violated the law or instructions; the causal link between the actions of the perpetrator and the harm; fault. In the case of harm caused by an AI system or application, the only certain fact is the occurrence of harm.

Accordingly, the main problems of holding someone accountable for harm caused by AI are identifying the perpetrator and the absence of fault when they could not have influenced the adverse consequences of using AI in any other way than by refusing to use it. Protective obligations arising from harm caused by the use of an AI system or application belong to the group of tort obligations, characterized by the specific means of causing harm. Today, the following types of special torts are known: a) harm caused by activities that create a heightened danger to others; b) harm caused by defects in products, works, or services.

What types of special torts can be applied to protective obligations arising from harm caused by AI?

1. Responsibility of the Owner of a Hazardous Source. One of the most well-known applications of AI that exhibits such features today is the highly autonomous vehicle. It is obvious that soon other AI applications will emerge, including fully autonomous assistant robots with a wide range of functions. In some AI applications, such as in an unmanned vehicle, the driver does not have a steering wheel or pedals at all. Such designs imply the responsibility of the owner without fault in cases of losing control over the object, but not responsibility for the unavoidable errors of others, such as the errors of the developer or inherent flaws in the model. Therefore, the presumption of fault seems theoretically unfounded. Moreover, the composition of this special tort does not exclude the necessity of establishing a causal link and the unlawfulness of the owner's actions. Accordingly, placing responsibility for someone else's actions (or inaction) on the owner within this framework is impossible on its own: there is a lack of legal tools to fill at least two missing elements of the composition.

2. Responsibility for Damage Caused by Defects in Goods. Harm caused by design defects or other flaws in a product, as well as by insufficient or misleading information about the product, should be compensated by the seller or manufacturer of the product regardless of their fault and whether the victim had a contractual relationship with them (Article 1209 as amended by Law No. 3390-VI of May 19, 2011). In this case, the problematic element of the tort composition is the presence of a causal link between the defect (error) in the AI system or application and the damage, because: a) the concept of a defect (error) is not legally defined in Ukrainian legislation; b) the properties of the system or application can change under the influence of the user. Accordingly, for this construction, it is problematic to establish two elements of the tort composition.

The problem of responsibility arises from the inability to establish the necessary elements of the legal composition of a tort committed using AI. This is an extremely undesirable situation, so it is necessary to find ways to eliminate it. To place responsibility on a specific person (or persons), it is necessary to develop legal tools to fill the missing elements of the tort composition committed using AI.

As mentioned earlier, the „responsibility gap“ is one of the legal consequences of technologically blurred accountability. However, „gaps in accountability“ can be caused by various technological reasons. The technological "accountability gap" occurs when harm is caused by the use of AI in at least two situations: the inherent error in the AI model is objectively unavoidable (for example, object recognition errors despite sufficient training of an unmanned aerial vehicle); and the inherent error in the AI model is excluded through expert analysis, but the search for the „author“ of the error is significantly complicated due to the complexity of the AI system or application in which the failure occurred (the „black box“ problem) [5]. Even more complicating this issue is the category of „AI hallucination“, where an AI chatbot generates invented, incorrect, or unfounded information in response to queries. In this situation, the program itself unintentionally creates erroneous content, which can have significant consequences in certain areas of human activity.

From a legal perspective, an inherent error in the AI model means the inability to establish three elements of the legal composition of a civil law violation: a) the causal link between the harm and the actions of the person using the system or AI application; b) the fault of that person; c) unlawfulness. This phenomenon seems to be the closest to what is already referred to as a „responsibility gap“ [8].

When technical expertise has ruled out the inherent error in the AI model but is still unable to determine whose actions caused the error, it seems to be a case of an apparent „accountability gap“. Although, with the current level of technology, there is a subjective impossibility of identifying the „author“ of the error, in the future, such a possibility may arise, and then the causal link can be established (along with other elements of the composition). In such a situation, the apparent „responsibility gap“ will be removed, essentially by technical means. A. Malgina believes that, given today's level of technology, the apparent „responsibility gap“ can only be overcome by legal means, just as in the first situation. Apparently, legal means for eliminating true and apparent „responsibility gaps“ should be conceptually similar [9].

In our opinion, A. Malgina's position on the apparent „responsibility gap“ raises several critical points. First, it is based on the assumption that future technological development will inevitably allow the establishment of a causal link and, accordingly, the identification of the responsible party. However, such a prediction is purely hypothetical and does not take into account possible new challenges, particularly the increasing complexity of AI models, which could make their behavior even less transparent.

Second, the author essentially reduces the problem to a matter of time, arguing that technical means will eventually resolve the responsibility gap. This overlooks situations where, even with advanced technological development, responsibility will still remain blurry due to the layered nature of AI development and usage.

Third, the assertion that the apparent „responsibility gap“ can today only be overcome by legal means is not undisputed. Legal mechanisms can only partially compensate for gaps in establishing responsibility, but they do not eliminate the uncertainty regarding the party responsible for the error. Moreover, equating the approaches to resolving true and apparent responsibility gaps is problematic because the nature of these phenomena is different: a true gap arises from the objective impossibility of identifying the culprit, while an apparent gap may be related to a lack of knowledge or technology at a particular time. This problem becomes especially acute in cases of „AI hallucination“, as we mentioned earlier. This occurs when the system generates false or non-existent facts without clear causal links. In such situations, responsibility cannot be attributed either to the developers or the users, since the algorithm itself operates unpredictably, and the mistakes have no obvious „author“. This further complicates the establishment of responsibility and contradicts Malgina's assumption that technological development will automatically resolve the problem.

Thus, her position is overly optimistic regarding the capabilities of technological progress and insufficiently accounts for the complexity of the legal and ethical aspects of AI responsibility. The concept of a „responsibility gap“ should be distinguished from „dilution of responsibility“. The latter refers to a situation where it becomes difficult to identify the cause of harm due to the so-called "many hands" problem, where the operation of an AI system controlling an AI application is mediated by the actions of multiple parties: the manufacturer, owner, dispatcher, operator, maintenance personnel, cloud infrastructure owner, and other participants in the AI application’s lifecycle. In such a case, the identification of the responsible party is determined by the quality and depth of the technical expertise, which must identify the individuals whose actions led to the error causing the adverse consequences of using the AI application. In this case, it is possible to establish the elements of a civil wrong.

Therefore, analysts believe that „responsibility gaps“ for harm caused by AI use can be divided into the following types: a true responsibility gap – the objective impossibility of identifying the cause of harm due to the occurrence of adverse consequences from an inherent error in the AI model that operates within the AI system (independent of the controlling subject); an apparent responsibility gap – the subjective impossibility of identifying the cause of harm due to the occurrence of adverse consequences from an AI system error when the conclusions of technical expertise fail to establish the fault of a specific person (or people) due to unclear error etiology (the „black box“ problem), which is not an inherent error of the specific AI model; and the „dilution of responsibility“ – the subjective impossibility of identifying the cause of harm due to the occurrence of adverse consequences from using an AI application, when the operation of the AI system is mediated by the actions of many participants in the lifecycle of the AI application.

In December 2023, the European Union adopted the Artificial Intelligence Act, which introduced clear requirements and obligations for developers and deployers of AI systems concerning their specific use. This law establishes a unified structure for all EU countries, based on the definition of AI and risk assessment. For example, high-risk AI systems, such as medical software or AI systems used for recruitment or security purposes, must comply with strict requirements, including risk mitigation systems, high-quality data sets, clear user information, and human oversight [10].

Particularly, AI systems that allow governments or companies to „assess social indicators“ are considered to present an obvious threat to basic human rights and are therefore banned. Such especially harmful uses of artificial intelligence include: exploiting vulnerabilities of individuals, manipulation, and the use of subconscious techniques; social scoring for governmental and private purposes; individual predictive policing based exclusively on profiling people; indiscriminate scraping of the internet or surveillance cameras to obtain facial images for creating or expanding databases; emotion recognition in workplaces and educational institutions, except for medical reasons or security purposes; biometric categorization of individuals to determine their race, political views, union membership, religious or philosophical beliefs, or sexual orientation. Labeling or filtering data sets and categorizing data in law enforcement still remain permissible; however, real-time remote biometric identification in public spaces by law enforcement is subject to certain exceptions.

The classification of risks is based on the intended purpose of the AI system, in accordance with the current EU legislation on product safety. Therefore, classification depends on the function of the specific AI system and its particular goals, methods, and uses [10].

The AI Act also establishes two advisory bodies to provide expert input: a Scientific Group and an Advisory Forum. These bodies will provide information from stakeholders and interdisciplinary scientific communities, informing decision-making and ensuring a balanced approach to the development of artificial intelligence [10].

As mentioned earlier, it is also possible that AI itself could pose an indirect potential threat, for example, when used to protect critical infrastructure. One of the most promising applications of AI in the energy sector is the prediction of potential threats and risk assessment for critical infrastructure. AI enables detailed analysis of past incidents, as well as the current state of systems, allowing for the creation of accurate predictions regarding future attacks and improving the defense strategies for energy facilities. Such systems could become a crucial tool in combating cyber threats, enabling energy companies to respond to potential risks in a timely manner (especially for energy institutions) [11, c 182].

One of the key advantages of AI in this case is the ability to dynamically update predictions in real-time. When conditions change, such as an increase in hacker group activities or shifts in external factors, AI can quickly adapt its predictions, ensuring that defense strategies are constantly updated. In today’s aggressive environment, the ability to promptly adjust forecasts and strategic decisions will be a significant advantage for energy companies [11, c 183].

However, despite the numerous advantages, the implementation of AI-powered video surveillance systems is associated with certain challenges. One of the main issues is privacy. Since these systems collect and process vast amounts of data, including video footage and personal information, there is a need for strict data protection measures and adherence to privacy regulations. Maintaining the right balance between security and privacy is crucial to ensuring public trust and the acceptance of these technologies [12].

Thus, AI has become an integral part of our lives, helping humanity in many areas. However, there is a need for a government program to stimulate the development of AI and its environment, which should be careful and balanced. It is already clear today that uncontrolled development of these technologies poses a great threat to humanity. These systems are actively used by the armed forces of various countries, and their autonomy brings this issue to the forefront at the level of international law, human rights, humanitarian law, and national security. However, there remain several technical, legal, and ethical challenges.

While the legal aspect can still be regulated, including through some classic precedents of Anglo-Saxon law, other challenges are more complex. Regarding the first (legal), we suggest considering the opinion of Judge Cardozo in the decision of the New York Court of Appeals in the case McPherson v. Buick Motor Co. (1916) regarding consumer protection from harm caused directly by dangerous goods, such as mis-labeled poisons, and expanding the applicability of this precedent to cases of harm caused by a product that becomes hazardous due to the manufacturer's negligence. [13, c. 429], This corresponds to the situation of „AI hallucination“, where erroneous actions may pose a danger. Similarly, the standard requirement to avoid negligence towards others, as formulated in the case Donoghue V. Stevenson (1932), applies to all cases regardless of the specific circumstances of harm being caused [13, c. 179].

Conclusions.

1. The issue of legal liability for harm caused by the use of artificial intelligence systems is related to the „responsibility gap“, which arises due to the inability to clearly identify the responsible party. This complicates the application of classical legal approaches to accountability, particularly due to the absence of a clear cause-and-effect relationship and the difficulty in establishing fault.

2. A feature of artificial intelligence technologies is their ability to self-learn, which complicates predicting their behavior and the responsibility of manufacturers, operators, or users. There is also the risk of „AI hallucination“, where the system generates false or fabricated information, potentially leading to significant legal consequences without a clearly identified perpetrator.

3. The lack of a clear definition of „artificial intelligence systems“ and mechanisms for their accountability in Ukraine's legal system creates a normative vacuum. This complicates legal enforcement in cases of harm caused by AI, necessitating the development of new legislation or the adaptation of existing legal norms to the challenges of technological progress.

4. International law continues to debate potential approaches to overcoming the „responsibility gap“. Both technical and legal methods are discussed, but a unified solution has not yet been reached. The European Union has already adopted legislation on AI, establishing different levels of regulation depending on the risks associated with the use of these technologies.

5. Addressing the issue of AI system liability requires a comprehensive approach, which includes improving legal regulation, creating mechanisms for monitoring the development and use of AI, and introducing effective technical means for tracking and analyzing the actions of these systems. This will help avoid legal uncertainty and ensure a balance between technological progress and legal guarantees of safety.

6. The „responsibility gap“ is a legal situation in which it is impossible to clearly determine the party responsible for a specific violation or harmful consequences resulting from actions or omissions, especially in the context of emerging technologies, international law, or complex management decisions. In the context of AI, the „responsibility gap“ could mean a situation where it is unclear who should be held accountable for the harm: the algorithm's developer, the system owner, the user, or the system itself (which is currently legally impossible).

REFERENCES

1. Draft Framework Convention on Artificial Intelligence, Human Rights, Democracy and The Rule of Law. Committee on Artificial Intelligence (CAI). Strasbourg, 18 December 2023. URL : https://rm.coe.int/cai-2023-28-draft-framework-convention/1680ade043 (accessed on 30.01.2025).

2. Melnikova E., Surov I. Legal. Status of Artificial Intelligence from Quantum-Theoretic Perspective. *BRICS Law Journal.* 2023. Vol. X. Is. 4. P. 22.

3. Matthias A. The responsibility gap: Ascribing responsibility for the actions of learning automata. *Ethics and Information Technology.* 2004. Vol. 6, № 3. P. 175. DOI 10.1007/s10676-004-3422-1

4. Santoni de Sio F., Mecacci G. Four Responsibility Gaps with Artificial Intelligence: Why they Matter and How to Address them. *Philosophy & Technology*. 2021. Vol. 34. P. 1057–1084 DOI 10.1007/s13347-021-00450-x ; URL : https://link.springer.com/article/10.1007/s13347-021-00450-x (accessed on 30.01.2025).

5. Sparrow R. Killer robots. *Journal of Applied Philosophy*. 2007. Vol. 24, № 1. P. 62–77. DOI 10.1111/j.1468-5930.2007.00346.x

6. Simpson T. W., Müller V. C. Just war and robots' killings. The Philosophical Quarterly. 2016. Vol. 66, Is. 263. P. 302–322. DOI 10.1093/pq/pqv075

7. Burri T. International Law and Artificial Intelligence. *German Yearbook of International Law*. 2017. Berlin : Duncker & Humblot, 2019. Vol. 60. P. 101.

8. Königs P. Artificial intelligence and responsibility gaps: what is the problem? *Ethics and Information Technology*. 2022. Vol. 24, № 3. DOI 10.1007/s10676-022-09643-0; Santoni de Sio F., Mecacci G. Op. cit.

9. Malgina A. IT technologies, artificial intelligence and law. URL : https://www.eurointegration.com (accessed on 30.01.2025).

10. Otsokolich V. The European Law on Artificial Intelligence has entered into force. 08.08.2024 / Ligazakon. URL : https://biz.ligazakon.net/analitycs/229699_nabuv-chinnost-vropeyskiy-zakon-pro-shtuchniy-ntelekt-pro-osnovn-vimogi-ta-zobovyazannya-pri-vikoristann-shtuchnogo-ntelektu (accessed on 30.01.2025).

11. Dorogy Ya. Yu., Tsurkan V. V., Doroga-Ivanyuk O. O. Using artificial intelligence in protecting critical infrastructure of energy sector institutions. *Energy security in the era of digital transformation* : VI scientific and practical conference of the Institute of Modeling Problems in Energy named after G. E. Pukhov of the National Academy of Sciences of Ukraine (Kyiv, December 13, 2024). IPME named after G.E. Pukhov of the NAS of Ukraine. Kyiv, 2024. P. 180–183.

12. Improving critical infrastructure protection with AI-powered video surveillance / TVT Digital. 15.09.2023. URL : https://tvtdigital.com.ua/pokrashchennia-zakhystu-krytychno-vazhlyvoi-infrastruktury-za-dopomohoiu-videosposterezhennia-zi-shtuchnym-intelektom/ (accessed on 30.01.2025).

13. Kononenko V. P. Judicial precedent in international and national law : monograph. Odessa : Phoenix, 2013. 512 p.

С. Г. Денисюк, В. П. Кононенко. ПРОБЛЕМА ЮРИДИЧНОЇ ВІДПОВІДАЛЬНОСТІ ЗА ШКІДЛИВІ НАСЛІДКИ ВИКОРИСТАННЯ СИСТЕМ ШТУЧНОГО ІНТЕЛЕКТУ

У статті досліджується проблема юридичної відповідальності за шкоду, заподіяну використанням систем штучного інтелекту (ШІ). Розглядається феномен «розриву відповідальності» (responsibility gap) та його вплив на правове регулювання. Аналізуються концептуальні підходи до визначення суб'єкта відповідальності в умовах автономного функціонування ШІ та особливостей його навчання.

Розкриваються складнощі правозастосування, зумовлені імовірнісним характером роботи ШІ, його здатністю до самонавчання та проблемою «чорної скриньки». Окрему увагу приділено питанням технологічного «галюцинування» ШІ (AI hallucination), коли *система генерує помилкові або неіснуючі дані, ускладнюючи встановлення причинно-наслідкових зв'язків та відповідального суб'єкта.*

У статті розглядаються три основні форми «розриву відповідальності»: істинний розрив, уявний розрив та «розмивання відповідальності», спричинене багаторівневою взаємодією різних суб'єктів. Аналізуються можливі юридичні механізми усунення цих проблем, зокрема запровадження спеціальних режимів відповідальності для розробників, власників і користувачів ШІ.

Окремо проаналізовано міжнародний досвід регулювання ШІ, зокрема положення нового Європейського закону про ШІ, що встановлює ризик-орієнтований підхід до відповідальності. Робиться висновок про необхідність адаптації існуючих правових концепцій та розробки нових регуляторних моделей, здатних враховувати особливості автономних систем.

Ключові слова: *штучний інтелект, юридична відповідальність, розрив відповідальності, цивільно-правова відповідальність, технологічне галюцинування, проблеми правозастосування.*

Стаття надійшла до редколегії 4 лютого 2025 року