Access to Justice in Eastern Europe
ISSN 2663-0575 (Print)
ISSN 2663-0583 (Online)
http://ajee-journal.com

RESEARCH ARTICLE

Research Article

FROM JOINT TO DIFFERENTIATED LIABILITY: REFORMING UKRAINIAN MEDICAL LAW IN LIGHT OF THE EU AI ACT AND THE ESTONIAN EXPERIENCE

Volodymyr Kapustnyk* and Volodymyr Kurylo

ABSTRACT

Background: *The growing use of high-risk artificial intelligence (AI) systems in healthcare challenges traditional models of medical liability, particularly where clinical decisions emerge from interactions among healthcare professionals, healthcare institutions, software providers, and algorithmic systems. In such circumstances, establishing causation and allocating responsibility becomes significantly more complex because of algorithmic opacity, distributed decision-making, and the involvement of multiple actors with different degrees of control over AI-related risks.*

Method: *This study employs doctrinal and comparative legal methods to examine the transformation of liability models in the context of AI-assisted medical decision-making. The analysis is based on Ukrainian civil and medical law, Regulation (EU) 2024/1689 'the EU Artificial Intelligence Act' (EU AI Act), standards of access to justice under Article 6 of the European Convention on Human Rights, and the Estonian model of digital healthcare governance and accountability.*

DOI:
https://doi.org/10.33327/AJEE-18-9.4-a0002009

Date of submission: 01 Jun 2026
Date of acceptance: 24 Jul 2026
Online First Publication: 30 Sep 2026

Disclaimer:
The authors declare that their opinions and views expressed in this manuscript are free of the influence of any organisations.

Copyright:
© 2026 Volodymyr Kapustnyk and Volodymyr Kurylo

Results and Conclusions: *The study demonstrates that traditional models of joint liability are increasingly inadequate for disputes involving high-risk medical AI systems because they fail to distinguish between actors exercising different degrees of control over algorithmic risk. It further demonstrates that the EU AI Act provides both a normative and conceptual foundation for a differentiated liability framework based on functional responsibility, human oversight, and risk governance. The article pays particular attention to the procedural significance of explainability, logging, and traceability as mechanisms that support causation assessment, access to evidence, and effective judicial review. The Estonian experience illustrates how digital accountability infrastructure, supported by clear institutional responsibilities and legal regulation, can strengthen oversight of AI-assisted medical decision-making. The article identifies key legislative gaps in Ukrainian medical law on AI-assisted healthcare. It proposes practical reform directions, including a differentiated liability model based on control over algorithmic risk. It concludes that this approach provides a more coherent and legally predictable framework for allocating responsibility in AI-assisted healthcare than traditional models of collective liability and aligns with emerging European approaches to AI governance and liability.*

1 INTRODUCTION

The increasing use of artificial intelligence (AI) systems in healthcare poses significant challenges to traditional models of legal liability. When harm to a patient arises in AI-assisted medical decision-making, the relevant outcome often depends on the interaction of multiple actors, including AI developers, software providers, healthcare institutions, and healthcare professionals. Under such circumstances, establishing causation and allocating legal responsibility become considerably more complex than in traditional medical malpractice disputes, particularly where algorithmic processes are opaque or difficult to verify.[1]

These challenges are becoming increasingly relevant for Ukraine as the healthcare sector undergoes rapid digital transformation and gradually incorporates AI-assisted technologies into clinical practice. Although Ukrainian legislation currently lacks a specialised framework governing liability for harm caused by medical AI systems, disputes involving algorithmically supported decision-making are likely to become more frequent. Existing civil and medical liability mechanisms were largely designed for

1 On the challenges that algorithmic opacity creates for legal accountability, evidential assessment, and the allocation of responsibility in AI-assisted decision-making, see Katie Atkinson, Trevor Bench-Capon and Danushka Bollegala, 'Explanation in AI and Law: Past, Present and Future' (2020) 289 Artificial Intelligence 103387 <https://doi.org/10.1016/j.artint.2020.103387> accessed 18 July 2026; Karen McGregor Richmond and others, 'Explainable AI and Law: An Evidential Survey' (2024) 3(1) Digital Society 1, doi:10.1007/s44206-023-00081-z <https://doi.org/10.1007/s44206-023-00081-z> accessed 18 July 2026.

situations in which medical decisions are made exclusively by human actors and therefore may prove inadequate in cases involving high-risk AI systems.

At the European level, the adoption of Regulation (EU) 2024/1689 (the EU AI Act) marks an important shift towards a risk-based and function-oriented approach to AI governance.[2] Rather than treating liability as a uniform concept, the EU regulatory framework differentiates obligations according to the actor's role, degree of control over algorithmic risk, and capacity to prevent harm.[3] This approach provides an important conceptual foundation for reconsidering traditional models of liability in healthcare.

The article argues that the conventional model of joint liability is increasingly ill-suited to disputes involving high-risk medical AI systems. Instead, a differentiated liability model based on control over algorithmic risk offers a more coherent framework for allocating responsibility among developers, healthcare institutions, and healthcare professionals.

To explore this proposition, the article analyses the EU AI Act's regulatory approach and Estonia's experience of digital healthcare governance. Estonia was selected as the primary comparative jurisdiction because it represents one of Europe's most advanced digital health ecosystems and provides a particularly relevant example for Ukraine as a post-socialist legal system that has undergone extensive digital transformation.[4] The study further examines the implications of explainability, logging, traceability, and human oversight for judicial review and liability allocation.[5]

2 For the legal framework establishing a risk-based approach to AI regulation and governance, see Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 Laying Down Harmonised Rules on Artificial Intelligence and amending Regulations (EC) No 300/2008, (EU) No 167/2013, (EU) No 168/2013, (EU) 2018/858, (EU) 2018/1139 and (EU) 2019/2144 and Directives 2014/90/EU, (EU) 2016/797 and (EU) 2020/1828 (AI Act) [2024] OJ L 2024/1689 <http://data.europa.eu/eli/reg/2024/1689/oj> accessed 18 July 2026.

3 On the EU's risk-based regulatory model and the differentiated allocation of obligations among actors involved in the AI lifecycle, see Henry Fraser and José-Miguel Bello y Villarino, 'Acceptable Risks in Europe's Proposed AI Act: Reasonableness and Other Principles for Deciding How Much Risk Management is Enough' (2024) 15(2) European Journal of Risk Regulation 431, doi:10.1017/err.2023.57 <https://doi.org/10.1017/err.2023.57> accessed 18 July 2026; Kasia Söderlund and Stefan Larsson, 'Enforcement Design Patterns in EU Law: An Analysis of the AI Act' (2024) 3 Digital Society 41 <https://doi.org/10.1007/s44206-024-00129-8> accessed 18 July 2026.

4 On Estonia's development as one of Europe's most advanced digital health ecosystems and its transition towards integrated data-driven healthcare, see Lili Milani and others, 'The Estonian Biobank's Journey from Biobanking to Personalized Medicine' (2025) 16 Nature Communications 3270 <https://doi.org/10.1038/s41467-025-58465-3> accessed 18 July 2026.

5 On transparency, explainability, and the right to explanation as elements of AI accountability and legal oversight, see Gintare Makauskaite-Samuole, 'Transparency in the Labyrinths of the EU AI Act: Smart or Disbalanced?' (2025) 8(2) Access to Justice in Eastern Europe 38 <https://doi.org/10.33327/AJEE-18-8.2-a000105> accessed 18 July 2026; Alycia Noë, Sarah Bouhouita-Guermech and Ma'n H Zawati, 'The Right to Explanation in AI: In a Lonely Place' (2025) 27 Journal of Medical Internet Research e64482 <https://doi.org/10.2196/64482> accessed 18 July 2026; Richmond and others (n 1); Ida Varošanec, 'On the Path to the Future: Mapping the Notion of Transparency in the EU Regulatory Framework for AI' (2022) 36(2) International Review of Law, Computers & Technology 95 <https://doi.org/10.1080/13600869.2022.2060471> accessed 18 July 2026.

© 2026 Volodymyr Kapustnyk and Volodymyr Kurylo. This is an open-access article distributed under the terms of the Creative Commons Attribution License (CC BY 4.0), which permits unrestricted use, distribution, and reproduction in any medium, provided the original author and source are credited.

This article assesses the feasibility of shifting Ukrainian medical law from a model of joint liability to one of differentiated liability in disputes involving high-risk AI systems. It proposes legal and institutional mechanisms to support such a transition.

2 METHODOLOGY

This study uses doctrinal and comparative legal approaches to examine how legal liability is transforming in the context of using high-risk AI systems in healthcare.

The research analyses Ukrainian civil and medical law, the provisions of the EU AI Act, and standards of access to justice and fair trial guarantees developed in European Court of Human Rights case law applying Article 6 of the European Convention on Human Rights.[6]

This study uses a comparative-functional method to assess how different legal models allocate liability in cases involving AI-assisted medical decision-making. This study focuses on the Estonian experience in digital healthcare. Estonia was selected as the primary comparative jurisdiction because it represents one of Europe's most advanced digital health ecosystems and provides a relevant point of comparison for Ukraine as a post-socialist legal system that has undergone extensive digital transformation.[7] In particular, the Estonian model offers practical examples of how logging, traceability, digital evidentiary mechanisms, and human oversight can be integrated into healthcare governance and judicial accountability frameworks.[8]

The study also conducts a functional analysis of how responsibility is allocated among actors using medical AI, including system developers, healthcare institutions, software providers, and healthcare professionals. It pays particular attention to the relationship between legal responsibility and the degree of control exercised over algorithmic risk.[9]

6 Regulation (EU) 2024/1689 (AI Act) (n 2); Council of Europe, *European Convention on Human Rights: as amended by Protocols Nos 11, 14 and 15; supplemented by Protocols Nos 1, 4, 6, 7, 12, 13 and 16* (ECtHR 2013) art 6 <https://www.echr.coe.int/documents/d/echr/convention_eng> accessed 18 July 2026.

7 On Estonia's development as one of Europe's most advanced digital health ecosystems and its transition towards integrated data-driven healthcare, see Milani and others (n 4).

8 On traceability, transparency, explainability, and oversight mechanisms within contemporary AI governance frameworks, see Makauskaite-Samuole (n 5); Richmond and others (n 1); Kasia Söderlund, 'High-Risk AI Transparency? On Qualified Transparency Mandates for Oversight Bodies under the EU AI Act' (2025) 2025 Technology and Regulation 97 <https://doi.org/10.71265/6bedar76> accessed 18 July 2026.

9 On the relationship between legal liability, causation, and control over algorithmic risk in AI-assisted decision-making, see Daiju Ueda and others., 'Legal Liability of Physicians and New Governance in the AI Era' (2026) 44 Japanese Journal of Radiology 1316 <https://doi.org/10.1007/s11604-026-01997-5> accessed 18 July 2026; Sylwia Wojtczak and Sylwia Księżak, 'Causation in Civil Law and the Problems of Transparency in AI' (2021) 29(4) European Review of Private Law 561 <https://doi.org/10.54648/erpl2021030> accessed 18 July 2026.

In addition, the research adopts a problem-oriented approach to identify shortcomings in the existing Ukrainian legal framework for addressing disputes involving AI-assisted medical decision-making. This approach assesses the extent to which the differentiated liability model emerging from European AI regulation may contribute to future reforms of Ukrainian medical law.

The study pays particular methodological attention to the procedural dimension of disputes involving medical AI. In this context, the study examines evidentiary asymmetry, access to technical information, explainability, the burden of proof, and the possibility of effectively challenging AI-assisted decisions through judicial proceedings.[10]

A methodological limitation is the lack of established Ukrainian case law on civil liability for harm caused by high-risk medical AI systems. Accordingly, the research relies on comparative legal analysis, emerging regulatory approaches, and contemporary scholarship on AI accountability.

3 THE CRISIS OF TRADITIONAL LIABILITY MODELS IN MEDICAL AI DISPUTES

3.1. The Transformation of Medical Decision-Making in AI-Assisted Systems

The growing use of artificial intelligence in healthcare is transforming the traditional model of medical decision-making, under which physicians exercised primary responsibility for diagnosis, risk assessment, and treatment selection. Contemporary AI-assisted systems increasingly support clinical decision-making through predictive analytics, medical image interpretation, risk stratification, and automated clinical data analysis.[11] As a result, medical decisions are no longer produced exclusively by human actors but emerge through interactions between healthcare professionals, algorithmic systems, and digital infrastructure.

10 On evidentiary asymmetry, access to technical information, digital evidence, and procedural guarantees in technology-related disputes, see Council of Europe, *European Convention on Human Rights* (n 6) art 6; European Committee on Legal Co-operation, Guidelines on Electronic Evidence in Civil and Administrative Proceedings (adopted on 30 January 2019) <https://www.coe.int/en/web/cdcj/digital-evidence/-/asset_publisher/7dbCE86mCocc/content/-the-administration-and-you-a-handbook> accessed 18 July 2026; Richmond and others (n 1).

11 On the growing use of AI-assisted technologies in clinical practice, including diagnostic support, medical image analysis, and predictive decision-making systems, see World Health Organization, *Ethics and Governance of Artificial Intelligence for Health: Guidance on Large Multi-Modal Models* (WHO 2024); Geeta Joshi and others, 'FDA-Approved Artificial Intelligence and Machine Learning (AI/ML)-Enabled Medical Devices: An Updated Landscape' (2024) 13(3) Electronics 498 <https://doi.org/10.3390/electronics13030498> accessed 18 July 2026; Sanju Kaladharan, Dhanya Manayath and Rejikumar Gopalakrishnan, 'Regulatory Challenges in AI/ML-Enabled Medical Devices: A Scoping Review and Conceptual Framework' (2024) 18(4) Journal of Medical Devices 040801 <https://doi.org/10.1115/1.4066280> accessed 18 July 2026.

© 2026 Volodymyr Kapustnyk and Volodymyr Kurylo. This is an open-access article distributed under the terms of the Creative Commons Attribution License (CC BY 4.0), which permits unrestricted use, distribution, and reproduction in any medium, provided the original author and source are credited.

This transformation has important legal implications. Under the EU AI Act, most medical AI applications are classified as high-risk AI systems because algorithmic errors may directly affect patients' health and safety.[12] High-risk medical AI systems include, among others, clinical decision support tools, diagnostic software, and AI-enabled medical devices subject to conformity assessment under European medical device regulations.[13]

Clinical decision support systems (CDSS) integrated into electronic health records are particularly significant. Such systems analyse patient data in real time and generate recommendations concerning diagnosis, treatment, and risk management.[14] In practice, AI-generated recommendations may substantially influence clinical decisions, even where the physician formally retains final decision-making authority.

The increasing involvement of AI systems fundamentally challenges traditional models of medical liability. In conventional malpractice disputes, courts generally focus on the conduct of healthcare professionals or healthcare institutions. In contrast, AI-assisted medical decision-making involves a broader network of actors, including developers, software providers, healthcare institutions, digital infrastructure operators, and healthcare professionals. Harm may result from algorithmic defects, biased training data, software failures, inadequate system integration, or improper human use of AI-generated recommendations.

These developments are particularly significant for Ukraine. Existing Ukrainian civil and medical liability mechanisms were developed on the assumption that medical decisions originate primarily from human actors. Consequently, current legal frameworks offer limited guidance on allocating responsibility when harmful outcomes arise from interactions among multiple actors in AI-assisted medical decision-making.

Under such circumstances, traditional concepts of joint liability may provide compensation mechanisms but do not necessarily identify which actor exercised effective control over the relevant algorithmic risk. This creates difficulties in establishing causation, allocating

12 On the classification of medical AI applications as high-risk systems and the corresponding regulatory requirements under EU law, see Regulation (EU) 2024/1689 (AI Act) (n 2).

13 For discussions of AI-enabled medical devices, clinical decision support systems, and regulatory challenges associated with their deployment in healthcare, see Joshi and others (n 11); Kaladharan, Manayath and Gopalakrishnan (n 11).

14 On the risks associated with AI-assisted medical decision-making, including hidden model limitations, algorithmic errors, and the implications of such failures for legal liability, see Michael H Bernstein and others, 'Randomized Study of the Impact of AI on Perceived Legal Liability for Radiologists' (2025) 2(6) NEJM AI <https://doi.org/10.1056/AIoa2400785> accessed 18 July 2026; Qiao Jin and others, 'Hidden Flaws Behind Expert-Level Accuracy of Multimodal GPT-4 Vision in Medicine' (2024) 7 npj Digital Medicine 190 <https://doi.org/10.1038/s41746-024-01185-7> accessed 18 July 2026; David O Shumway and Hayes J Hartman, 'Medical Malpractice Liability in Large Language Model Artificial Intelligence: Legal Review and Policy Recommendations' (2024) 124(7) Journal of Osteopathic Medicine 287 <https://doi.org/10.1515/jom-2023-0229> accessed 18 July 2026.

responsibility, and ensuring legal certainty for both patients and participants in the AI ecosystem.[15] Accordingly, the growing use of medical AI creates a need to reconsider traditional liability models and to explore differentiated approaches based on the degree of control exercised over algorithmic risk.

3.2. The Black Box Effect and the Problem of Causation

One of the most significant challenges of using high-risk AI systems in healthcare is the so-called black box effect: the reasoning behind an algorithmic output is wholly or partially inaccessible to users, patients, or even system developers.[16] In disputes involving medical AI, this phenomenon substantially complicates the establishment of causation, which remains a central requirement for civil liability.[17]

Under traditional models of medical malpractice, courts typically assess healthcare professionals' conduct and determine whether harm resulted from professional negligence, diagnostic error, or a breach of applicable medical standards. In AI-assisted medical decision-making, however, harmful outcomes may arise from a combination of factors, including algorithmic defects, biased training data, software failures, inadequate system integration, or inappropriate reliance on AI-generated recommendations.[18] As a result, causation becomes distributed across multiple actors and technological processes rather than being attributable to a single identifiable decision-maker.

This development exposes an important limitation of traditional joint liability. Although collective liability may facilitate compensation where causal uncertainty exists, it does not necessarily identify which actor effectively controlled the risk that ultimately materialised. In the context of medical AI, the central legal question is often not whether several actors participated in the decision-making process, but which actor could have prevented the specific failure that caused harm.[19] Thus, causation and control become closely interconnected.

15 On the challenges of causation, responsibility allocation, and tort liability arising from AI-assisted decision-making, see Jan De Bruyne and Wannes Ooms, 'Tort Liability and Artificial Intelligence: Some Challenges and (Regulatory) Responses' in Nathalie A Smuha (ed), *The Cambridge Handbook of the Law, Ethics and Policy of Artificial Intelligence* (CUP 2025) 158 <http://doi.org/10.1017/9781009367783.011> accessed 18 July 2026; Wojtczak and Księżak (n 9).

16 On the concept of the black box effect, explainability, and the difficulties associated with understanding algorithmic reasoning in AI-assisted decision-making, see Atkinson, Bench-Capon, and Bollegala (n 1); Richmond and others (n 1).

17 On the relationship between transparency, causation, and civil liability in AI-related disputes, see Wojtczak and Księżak (n 9).

18 For discussions of hidden model limitations, algorithmic errors, biased outputs, and the implications of such failures for healthcare decision-making, see De Bruyne and Ooms (n 15); Jin and others (n 14).

19 On the allocation of liability according to control over risk and the ability to prevent harm, see De Bruyne and Ooms (n 15); Wojtczak and Księżak (n 9).

© 2026 Volodymyr Kapustnyk and Volodymyr Kurylo. This is an open-access article distributed under the terms of the Creative Commons Attribution License (CC BY 4.0), which permits unrestricted use, distribution, and reproduction in any medium, provided the original author and source are credited.

From this perspective, the black box effect is not merely a technical problem but a legal and evidentiary challenge. Where courts cannot meaningfully reconstruct how an AI system operated, they may struggle to determine whether harm resulted from defects in the system itself, failures in its implementation, or errors by healthcare professionals. Such uncertainty may undermine both legal predictability and the effectiveness of judicial protection.

Contemporary European AI regulation increasingly addresses this problem through requirements concerning explainability, traceability, and logging. The EU AI Act requires providers of high-risk AI systems to maintain technical documentation, ensure traceability of system operations, and implement logging mechanisms that record relevant algorithmic activities.[20] These obligations serve not only regulatory and safety purposes but also important evidentiary functions by facilitating the reconstruction of algorithmic decision-making processes.

In this context, explainability acquires particular legal significance. Access to information about how an AI system functions is often a prerequisite for establishing causation, allocating liability, and effectively challenging harmful outcomes. Consequently, the black box effect raises concerns not only regarding liability but also regarding access to justice and the practical ability of courts to review AI-assisted medical decisions.[21]

For Ukraine, these challenges are especially important because existing liability mechanisms were developed without consideration of algorithmically mediated decision-making. As the use of medical AI expands, the lack of adequate mechanisms to reconstruct algorithmic processes may significantly hinder judicial assessment of causation. This reinforces the need for a differentiated liability framework supported by robust requirements concerning logging, traceability, and access to relevant technical information.

3.3. Procedural Asymmetry and Access to Justice

The use of high-risk AI systems in healthcare creates not only substantive legal challenges but also significant procedural concerns. One of the most important of these is evidentiary and informational asymmetry between the parties to a dispute. Patients and their representatives often lack access to the technical information needed to assess how an AI system functions. At the same time, healthcare institutions, software providers, or developers may control the relevant data, logs, and technical documentation.[22] As a result,

20 Regulation (EU) 2024/1689 (AI Act) (n 2).

21 On the evidential significance of explainability and access to information for judicial review of AI-assisted decisions, see Noë, Bouhouita-Guermech and Zawati (n 5); Richmond and others (n 1).

22 On evidentiary asymmetry and unequal access to information in disputes involving AI-assisted decision-making, see Niamh Kinchin, '"Voiceless": The Procedural Gap in Algorithmic Justice' (2024) 32 International Journal of Law and Information Technology eaae024 <https://doi.org/10.1093/ijlit/eaae024> accessed 18 July 2026; Richmond and others (n 1).

the effective protection of rights increasingly depends on access to information concerning the operation of algorithmic systems.

In traditional medical disputes, courts primarily rely on medical records, expert testimony, and clinical protocols. In AI-assisted medical decision-making, however, much of the relevant evidence may exist within digital infrastructure inaccessible to patients and external experts.[23] Consequently, disputes involving medical AI raise questions not only of liability allocation but also of procedural fairness and access to evidence.

From this perspective, explainability acquires a procedural function. The issue is not merely whether an algorithm can be technically explained but whether parties to a dispute can obtain sufficient information to challenge the validity of an AI-assisted decision, identify the source of an error, and establish a causal connection between system operation and harm. Without such access, judicial review may become largely formal.[24]

These concerns are closely connected with the guarantees of a fair trial protected under Article 6 of the European Convention on Human Rights. The principle of equality of arms requires that each party be afforded a reasonable opportunity to present its case under conditions that do not place it at a substantial disadvantage compared with the opposing party.[25] In the context of medical AI, this principle may be affected where one party controls the technical information necessary to assess the operation of an algorithm. In contrast, the opposing party has no practical means of obtaining or evaluating such information.

Disputes involving medical AI should not be viewed solely through the lens of substantive liability. They also raise questions about access to evidence, procedural transparency, and courts' ability to review AI-assisted decisions effectively. In this respect, the logging, traceability, and auditability mechanisms required for high-risk AI systems serve not only technical and regulatory functions but also important procedural ones by facilitating access to relevant evidence.[26]

The Estonian experience illustrates how digital accountability mechanisms can support procedural fairness. Estonia's digital health infrastructure incorporates extensive logging and traceability mechanisms that allow reconstruction of healthcare interactions and data

23 On the procedural implications of digital evidence and access to technologically relevant information, see European Committee on Legal Co-operation (n 10).

24 On the evidential significance of explainability and access to information for meaningful review of AI-assisted decisions, see Noë, Bouhouita-Guermech and Zawati (n 5); Richmond and others (n 1).

25 On the principle of equality of arms and procedural fairness, see *Brandstetter v Austria* Apps nos 11170/84, 12876/87 and 13468/87 (ECtHR, 28 August 1991) <https://hudoc.echr.coe.int/eng?i=001-57683> accessed 18 July 2026; *Dombo Beheer BV v The Netherlands* App no 14448/88 (ECtHR, 27 October 1993) <https://hudoc.echr.coe.int/eng?i=001-57850> accessed 18 July 2026.

26 On the procedural significance of logging, traceability, transparency, and auditability mechanisms in high-risk AI systems, see Regulation (EU) 2024/1689 (AI Act) (n 2); Makauskaite-Samuole (n 5); Söderlund (n 8).

© 2026 Volodymyr Kapustnyk and Volodymyr Kurylo. This is an open-access article distributed under the terms of the Creative Commons Attribution License (CC BY 4.0), which permits unrestricted use, distribution, and reproduction in any medium, provided the original author and source are credited.

access events. Such mechanisms enhance transparency and provide courts with the evidentiary basis necessary to determine how a particular decision was made and which actors participated in the process.

For Ukraine, the procedural dimension of medical AI disputes may prove as important as the substantive allocation of liability. Even the most sophisticated, differentiated liability model cannot function effectively if courts lack access to the information required to identify who controlled the relevant algorithmic risk. Consequently, access to algorithmically relevant evidence should be regarded as a necessary precondition for implementing differentiated liability in healthcare.

3.4. The Emergence of the Principle of Human Oversight in Contemporary Judicial Practice

Although Ukrainian courts have not yet developed case law concerning civil liability for harm caused by medical AI systems, recent judicial practice demonstrates the gradual emergence of a broader principle of human oversight in the professional use of artificial intelligence.[27]

Several recent decisions of the Supreme Court and appellate courts concerning the use of generative AI in legal proceedings have emphasised that AI systems may serve only as auxiliary tools and cannot replace professional judgement or legal responsibility. In particular, Ukrainian courts have repeatedly stressed that users remain responsible for verifying AI-generated information and that relying on unverified outputs may breach professional duties or procedural obligations.[28]

These decisions do not directly concern medical AI. Nevertheless, they matter because they reveal an emerging judicial approach to allocating responsibility in AI-assisted decision-making. Rather than treating AI systems as autonomous decision-makers, Ukrainian courts continue to link responsibility to the individual who controls the technology and makes the final professional decision.[29]

27 For recent examples of Ukrainian judicial practice addressing the professional use of generative AI and the continuing responsibility of human users, see Case no 925/496/24 (Commercial Cassation Court, Supreme Court of Ukraine, 8 July 2025) <https://reyestr.court.gov.ua/Review/128775966> accessed 18 July 2026; Case no 240/14153/24 (Administrative Cassation Court, Supreme Court of Ukraine, 15 January 2026) <https://reyestr.court.gov.ua/Review/133336040> accessed 18 July 2026; Case no 620/12085/25 (Sixth Administrative Court of Appeal, 26 January 2026) <https://reyestr.court.gov.ua/Review/133574154> accessed 18 July 2026.

28 Case no 925/496/24 (n 27); Case no 240/14153/24 (n 27).

29 On the continuing attribution of responsibility to the human user exercising control over AI-assisted decision-making, see Case no 240/14153/24 (n 27); Case no 620/12085/25 (n 27).

This approach closely resembles the concept of meaningful human oversight embodied in the EU AI Act.[30] Under this principle, high-risk AI systems should be designed and deployed in a manner that enables qualified human users to understand, supervise, and, where necessary, override algorithmic outputs. Human oversight serves not merely as a technical safeguard but also as a mechanism to preserve accountability in increasingly automated environments.

This principle is particularly relevant in healthcare. Clinical decision support systems and other medical AI applications may significantly influence diagnosis, treatment selection, and risk assessment. However, the increasing sophistication of AI systems does not eliminate healthcare practitioners' professional responsibility to evaluate clinical information and exercise independent medical judgement.

For this reason, human oversight should be regarded not only as a regulatory requirement but also as an emerging legal principle that can guide future liability allocation in medical AI disputes.[31] Within a differentiated liability framework, responsibility should remain connected to the actor who possessed the authority, information, and practical ability to supervise the relevant AI-assisted decision-making process.

Beyond judicial practice, Ukraine has also begun developing a broader policy framework for governing artificial intelligence. The Concept for the Development of Artificial Intelligence in Ukraine (2020) initiated the formation of a national AI policy, while the White Paper on Artificial Intelligence Regulation (2024) outlined a gradual approach towards regulatory harmonisation with the EU AI Act. This direction has since been reinforced by the draft National Strategy for the Development of Artificial Intelligence until 2030, sector-specific healthcare initiatives, including the National Health Strategy 2030, and methodological guidance on assessing AI-enabled medical technologies through updated health technology assessment procedures. Together with the Voluntary Code of Conduct on the Ethical and Responsible Use of Artificial Intelligence, these documents demonstrate that Ukraine is progressively moving towards a comprehensive governance framework combining legal regulation, ethical standards, and sector-specific implementation mechanisms. Although these instruments do not yet establish a specialised civil liability regime, they provide an important policy foundation for the future development of differentiated liability in AI-assisted healthcare.[32]

30 Regulation (EU) 2024/1689 (AI Act) (n 2); Andreas Holzinger, Kurt Zatloukal and Heimo Müller, 'Is Human Oversight to AI Systems Still Possible?' (2025) 85 New Biotechnology 59 <https://doi.org/10.1016/j.nbt.2024.12.003> accessed 18 July 2026; Liming Zhu and others, 'Designing Meaningful Human Oversight in AI' (2026) 6 AI and Ethics 286 <https://doi.org/10.1007/s43681-026-01147-7> accessed 18 July 2026.

31 ibid

32 On the development of Ukraine's artificial intelligence governance framework, see Order of the Cabinet of Ministers of Ukraine no 1556-r of 2 December 2020 'Approving the Concept of Artificial Intelligence Development in Ukraine' <https://zakon.rada.gov.ua/laws/show/1556-2020-%D1%80> accessed 18 July 2026; Ministry of Digital Transformation of Ukraine, *White Paper on Artificial*

© 2026 Volodymyr Kapustnyk and Volodymyr Kurylo. This is an open-access article distributed under the terms of the Creative Commons Attribution License (CC BY 4.0), which permits unrestricted use, distribution, and reproduction in any medium, provided the original author and source are credited.

4 THE EU AI ACT AND THE EMERGENCE OF A DIFFERENTIATED LIABILITY MODEL IN MEDICAL AI

4.1. The Risk-Based Approach of the EU AI Act

The adoption of the European Union Artificial Intelligence Act (EU AI Act) marks a significant shift in regulating high-risk technologies, including AI systems used in healthcare. Rather than imposing uniform obligations on all participants in developing and deploying AI systems, the AI Act adopts a risk-based approach that calibrates legal duties to an AI system's potential impact on fundamental rights, safety, and human health.[33]

Medical AI systems occupy a central position within this framework and are generally classified as high-risk AI systems.[34] This classification reflects the recognition that algorithmic errors in healthcare may directly affect diagnosis, treatment decisions, and patient safety. As a result, the AI Act imposes extensive obligations on actors who can influence the safety and reliability of such systems.

Intelligence Regulation in Ukraine: Vision of the Ministry of Digital Transformation of Ukraine: Version for Consultation (Expert Committee on the Development of Artificial Intelligence, June 2024) <https://storage.thedigital.gov.ua/files/c/fc/36c4cae89deedfbf3781ec6bceddffcc.pdf> accessed 18 July 2026; Ministry of Digital Transformation of Ukraine, *Draft National Strategy for the Development of Artificial Intelligence until 2030* (*Digital State UA*, 12 November 2025) <https://digitalstate.gov.ua/uk/news/govtech/ukrayina-prezentuvala-draft-stratehiyi-rozvytku-shi-do-2030-roku-fokus-na-praktychne-zastosuvannia-infrastrukturu-ta-vlasni-modeli> accessed 18 July 2026; Order of the Cabinet of Ministers of Ukraine no 34-r of 17 January 2025 'On Approval of the Healthcare System Development Strategy for the Period until 2030 and Approval of the Operational Action Plan for Its Implementation in 2025–2027' <https://zakon.rada.gov.ua/laws/show/34-2025-%D1%80> accessed 18 July 2026; Ministry of Digital Transformation of Ukraine, *Voluntary Code of Conduct for the Ethical and Responsible Use of Artificial Intelligence* (25 December 2024) <https://storage.thedigital.gov.ua/files/0/e0/e9540a11682f3bc1d0472755b09fbe04.pdf> accessed 18 July 2026; Order of the Ministry of Health of Ukraine no 1771 of 21 November 2025 'On Approval of the Guideline on Health Technology Assessment of Medical Devices' <https://moz.gov.ua/uk/decrees/nakaz-moz-ukrayini-vid-21-11-2025-1771-pro-zatverdzhennya-nastanovi-z-derzhavnoyi-ocinki-medichnih-tehnologij-shodo-medichnih-virobiv> accessed 18 July 2026.

33 On the risk-based regulatory approach established by the EU AI Act and its classification of AI systems according to their potential impact on fundamental rights, safety, and health, see Regulation (EU) 2024/1689 (AI Act) (n 2); Şaban İbrahim Göksal, Maria Claudia Solarte Vasquez and Archil Chochia, 'The EU AI Act's Alignment within the European Union's Regulatory Framework on Artificial Intelligence' (2024) 24(2) International and Comparative Law Review 25 <https://doi.org/10.2478/iclr-2024-0017> accessed 18 July 2026.

34 On the classification of medical AI applications as high-risk systems under European AI regulation, see Regulation (EU) 2024/1689 (AI Act) (n 2); Alejandro Bellogín and others, 'The EU AI Act and the Wager on Trustworthy AI' (2024) 67(12) Communications of the ACM 58 3665322 <https://doi.org/10.1145/3665322> accessed 18 July 2026.

A particularly important feature of the AI Act is that it distributes regulatory obligations among different participants in the AI ecosystem according to their respective functions.[35] Providers are responsible for system design, risk management, data governance, technical documentation, and compliance mechanisms. Deployers, including healthcare institutions, are responsible for appropriate implementation and use of AI systems, ongoing monitoring, and maintaining effective human oversight.

From a legal liability perspective, this allocation of obligations matters because it links regulatory responsibility directly to control over algorithmic risk. The EU AI Act assigns legal obligations to actors who can prevent specific categories of risk throughout the AI lifecycle. Providers are responsible for system design, data governance, conformity assessment, and technical documentation because they exercise control over the technological sources of risk. Deployers, including healthcare institutions, are responsible for implementation, operational monitoring, and meaningful human oversight because they control the clinical environment in which AI systems are used.[36] Although the EU AI Act does not establish a comprehensive civil liability regime, its allocation of regulatory obligations reflects a broader normative principle: responsibility should follow the actor's capacity to control and prevent harm. The proposed differentiated liability framework develops this principle in civil liability by linking legal responsibility to where effective control over the algorithmic risk ultimately materialised.[37]

The broader European liability framework further reinforces this approach. In particular, Directive (EU) 2024/2853 on liability for defective products facilitates compensation in situations involving defective AI-enabled products and software. Although the Directive does not establish a specific AI liability regime, it complements the risk-based logic of the EU AI Act by strengthening mechanisms to identify responsible actors and improve access to compensation where technological defects contribute to harmful outcomes.[38]

The requirements concerning human oversight, logging, traceability, and technical documentation are particularly relevant in this respect.[39] These obligations not only promote the safe operation of high-risk AI systems but also facilitate the identification of

35 On the functional allocation of obligations among providers, deployers, importers, distributors, and other actors involved in the AI lifecycle, see Regulation (EU) 2024/1689 (AI Act) (n 2); Söderlund and Larsson (n 3).

36 On the allocation of obligations under the EU AI Act and the relationship between regulatory functions and enforcement mechanisms, see *ibid*.

37 On tort liability for AI systems and differentiated allocation of responsibility, see *Regulation (EU) 2024/1689 (AI Act)* (n 2); De Bruyne and Ooms (n 15).

38 Directive (EU) 2024/2853 of the European Parliament and of the Council of 23 October 2024 on liability for defective products and repealing Council Directive 85/374/EEC [2024] OJ L 2024/2853 <http://data.europa.eu/eli/dir/2024/2853/oj> accessed 18 July 2026.

39 On transparency, traceability, logging, technical documentation, and oversight obligations applicable to high-risk AI systems, see *Regulation (EU) 2024/1689 (AI Act)* (n 2); Makauskaite-Samuole (n 5); Söderlund (n 8).

© 2026 Volodymyr Kapustnyk and Volodymyr Kurylo. This is an open-access article distributed under the terms of the Creative Commons Attribution License (CC BY 4.0), which permits unrestricted use, distribution, and reproduction in any medium, provided the original author and source are credited.

the actor who exercised control over a particular stage of the decision-making process. Consequently, the AI Act contributes to an accountability framework in which responsibility can be allocated according to the actor's capacity to prevent harm rather than merely according to formal participation in a decision-making chain.

For Ukraine, the AI Act's significance extends beyond regulatory harmonisation with European Union law. The Act offers a conceptual model[40] for addressing one of the central challenges of AI-assisted medical decision-making: how to allocate responsibility among multiple actors participating in the creation, deployment, and use of high-risk AI systems. In this sense, the AI Act's risk-based approach provides an important foundation for the transition from traditional joint liability to a differentiated liability model based on control over algorithmic risk.

4.2. The Estonian Model of Digital Accountability and Human Oversight

Among European jurisdictions, Estonia provides a particularly relevant comparative example for examining the future regulation of medical AI in Ukraine. Estonia was selected not only because of its advanced digital infrastructure but also because it shows how legal accountability can be integrated into a highly digitalised healthcare environment.[41] As a post-socialist legal system that has undergone extensive technological transformation, Estonia offers a useful point of comparison for Ukraine's ongoing digitalisation of healthcare services.[42]

A distinctive feature of the Estonian approach is the combination of extensive technological integration with the preservation of human responsibility for final clinical decisions.[43] Although artificial intelligence systems are actively incorporated into healthcare processes, Estonian policy has consistently rejected the idea of autonomous legal responsibility for AI systems.[44] Instead, AI is treated as a decision support tool, while legal responsibility remains attached to human actors exercising control over medical decision-making.[45]

40 Karolina Kiejnich-Kruk, 'The AI Act: Challenges for Justice and Democracy in the Deployment of AI-Based Systems' (2026) 31(1) *Białostockie Studia Prawnicze* 115 <https://doi.org/10.15290/bsp.2026.31.01.07> accessed 18 July 2026.

41 Kaija Kasekamp and others, '*Estonia: Health System Review 2023*' (2023) 25(5) Health Systems in Transition 1 <https://eurohealthobservatory.who.int/publications/i/estonia-health-system-review-2023> accessed 18 July 2026.

42 On Estonia's development as one of Europe's most advanced digital health ecosystems and its transition towards integrated data-driven healthcare and personalised medicine, see Milani and others (n 4).

43 Kasekamp and others (n 41).

44 On contemporary approaches to AI governance that preserve human responsibility and reject autonomous legal personhood for AI systems, see Regulation (EU) 2024/1689 (AI Act) (n 2); World Health Organization (n 11).

45 Law of the *Republic of Estonia of* 9 May 2001 *on the Organization of Health Services 'Tervishoiuteenuste korraldamise seadus (TTKS)'* (amended 3 July 2026) <https://www.riigiteataja.ee/en/akt/

This approach is particularly important for developing differentiated liability. Rather than treating the technology itself as a potential bearer of responsibility, the Estonian model allocates accountability based on each participant's role within the digital healthcare ecosystem. Physicians remain responsible for clinical judgement and treatment decisions, while technology providers bear responsibility for system design, technical reliability, and data quality. In practice, liability follows the location of effective control over the relevant risk.[46]

Estonia's extensive digital accountability infrastructure reinforces the practical significance of this model.[47] Healthcare interactions, access to medical records, and system operations are recorded through traceability and logging mechanisms that make it possible to reconstruct the sequence of events leading to a particular decision.[48] Such mechanisms are especially important in disputes involving AI-assisted medical decision-making because they provide courts with evidence concerning who accessed information, how recommendations were generated, and whether appropriate human oversight was exercised.

From a liability-allocation perspective, the most important lesson of the Estonian experience is not the specific technology employed but the existence of an evidentiary infrastructure capable of supporting judicial review. Logging, traceability, and digital accountability mechanisms transform abstract principles of responsibility into practically enforceable legal standards.[49] Without such infrastructure, it may be difficult to identify which actor controlled the relevant algorithmic risk and should, therefore, bear responsibility for harmful outcomes.

For Ukraine, the Estonian model shows that regulating medical AI successfully requires more than adopting legal norms. Effective differentiated liability depends on creating institutional and technological mechanisms that support transparency, accountability, and evidentiary access. In this respect, Estonia illustrates how digital governance can facilitate the practical implementation of human oversight and control-over-risk principles in healthcare. The relevance of the Estonian experience lies not in transplanting specific technological solutions but in the broader lesson that differentiated liability can function effectively only where an adequate digital accountability infrastructure supports legal responsibility.

502022016002?leiaKehtiv> accessed 18 July 2026; Law of the *Republic of Estonia of 26 September 2001 on the Obligations Act 'Võlaõigusseadus (VÕS)'* (amended 30 June 2026) <https://www.riigiteataja.ee/en/akt/528032016012?leiaKehtiv> accessed 18 July 2026.

46 Ueda and others (n 9); De Bruyne and Ooms (n 15).

47 Kasekamp and others (n 41).

48 Richmond and others (n 1); Söderlund (n 8).

49 Makauskaite-Samuole (n 5); Richmond and others (n 1).

© 2026 Volodymyr Kapustnyk and Volodymyr Kurylo. This is an open-access article distributed under the terms of the Creative Commons Attribution License (CC BY 4.0), which permits unrestricted use, distribution, and reproduction in any medium, provided the original author and source are credited.

4.3. The Significance of the European Approach for Ukraine

The significance of the European approach for Ukraine extends beyond the formal process of legislative approximation to European Union law. More importantly, it provides a conceptual framework for addressing legal challenges that existing Ukrainian civil and medical liability mechanisms do not adequately regulate.

Current Ukrainian legislation lacks specific provisions governing liability for harm caused through AI-assisted medical decision-making.[50] Existing legal frameworks were developed on the assumption that medical decisions are made primarily by healthcare professionals and healthcare institutions. Consequently, Ukrainian law offers limited guidance regarding situations in which harmful outcomes result from the interaction of physicians, healthcare providers, software developers, and algorithmic systems.

This regulatory gap becomes increasingly important as digital technologies are integrated into healthcare practice. Electronic health records, digital diagnostic tools, medical imaging software, and AI-assisted decision support systems are already influencing clinical processes. As a result, disputes concerning algorithmically assisted medical decisions are likely to become more common, while existing liability doctrines may prove insufficient to address complex questions of causation and responsibility.[51]

From this perspective, the European model's principal contribution lies not in creating entirely new forms of liability but in developing mechanisms to allocate responsibility according to control over risk. The EU AI Act demonstrates how legal obligations may be linked to specific functions performed by different actors within an AI ecosystem.[52] This approach provides a useful foundation for future reforms of Ukrainian medical law.

Several aspects of the European framework appear particularly relevant for Ukraine. First, the principle of human oversight provides an important mechanism for preserving professional accountability in increasingly automated clinical environments.[53] Second, requirements concerning logging, traceability, and technical documentation create evidentiary tools capable of supporting judicial assessment of causation. Third, the functional differentiation of obligations among providers, deployers, and other participants offers a possible model for future liability allocation in disputes involving medical AI.

50 Although Ukrainian legislation regulates civil liability and the provision of healthcare services, it does not currently establish a specialised liability framework for harm caused by AI-assisted medical decision-making. See also Ueda and others (n 9).

51 On the challenges that AI-assisted decision-making creates for traditional doctrines of causation and liability, see De Bruyne and Ooms (n 15); Wojtczak and Księżak (n 9).

52 See Regulation (EU) 2024/1689 (AI Act) (n 2); Fraser and Bello y Villarino (n 3); Söderlund and Larsson (n 3).

53 On human oversight, traceability, logging, technical documentation, and the functional allocation of obligations among participants in the AI ecosystem, see Regulation (EU) 2024/1689 (AI Act) (n 2); Holzinger, Zatloukal and Müller (n 30); Söderlund (n 8); Zhu and others (n 30).

At the same time, the European experience suggests that legal reform alone is insufficient. Effective implementation of differentiated liability requires institutional and technological mechanisms that ensure transparency, accountability, and access to algorithmically relevant information. In this respect, the Estonian experience demonstrates how digital accountability infrastructure may complement legal regulation and facilitate practical enforcement.

The European approach matters for Ukraine not merely because it represents a future regulatory obligation associated with European integration, but because it offers practical solutions to legal problems already emerging in the digital transformation of healthcare. It therefore provides an important foundation for developing a modern liability framework that balances patient protection, technological innovation, and legal certainty.

5 A DIFFERENTIATED LIABILITY FRAMEWORK FOR UKRAINE

5.1. The Inadequacy of Traditional Joint Liability in Medical AI Disputes

Contemporary scholarship increasingly recognises that traditional civil liability doctrines are not fully adapted to disputes involving AI-assisted decision-making. Existing research shows that algorithmic opacity, the distributed nature of AI development and deployment, and the separation between technological design and clinical use complicate identifying the actor who should bear legal responsibility for harm. Scholars have argued that conventional concepts of joint liability may provide effective compensation but often fail to allocate responsibility according to each participant's actual capacity to control, prevent, or mitigate algorithmic risk. These developments have stimulated growing academic support for liability models that distinguish between the different functions performed by providers, deployers, and healthcare professionals. Against this background, this article develops the differentiated liability framework within the context of Ukrainian medical law.[54]

The proposed differentiated liability model is also supported by the regulatory architecture established under the EU AI Act. Rather than imposing uniform obligations on all participants, the Regulation assigns legal responsibilities based on each actor's functional role and capacity to manage specific risks. Providers remain responsible for the design, conformity assessment, and post-market monitoring of AI systems. At the same time, deployers assume obligations related to lawful implementation, human oversight, and operational use within healthcare institutions. This functional allocation of regulatory duties provides a normative basis for assigning civil liability according to the sphere of

54 On the limitations of traditional liability doctrines in AI-assisted healthcare and the emerging shift towards function-based allocation of responsibility, see De Bruyne and Ooms (n 15); Shumway and Hartman (n 14); Ueda and others (n 9); Wojtczak and Księżak (n 9).

© 2026 Volodymyr Kapustnyk and Volodymyr Kurylo. This is an open-access article distributed under the terms of the Creative Commons Attribution License (CC BY 4.0), which permits unrestricted use, distribution, and reproduction in any medium, provided the original author and source are credited.

effective control over the risk that materialised, thereby reinforcing the rationale for differentiated liability within Ukrainian medical law.[55]

Traditional concepts of joint liability were developed to ensure effective compensation in situations when harm results from the conduct of multiple actors and the precise contribution of each participant cannot be determined. In conventional healthcare relationships, this approach has often protected patients when several healthcare professionals or institutions participated in delivering medical care.

The increasing use of AI-assisted medical decision-making challenges the assumptions underlying these traditional liability models.[56] Unlike conventional medical disputes, responsibility for AI-assisted outcomes may involve healthcare professionals, healthcare institutions, software developers, AI providers, and other participants in the digital healthcare ecosystem. As a result, harmful outcomes may emerge from a complex interaction of technological and human factors rather than from the conduct of a single identifiable actor.[57]

Although joint liability may facilitate compensation in situations characterised by causal uncertainty, it presents several important limitations in the context of medical AI. Most significantly, it does not distinguish between actors who merely participated in a technological process and actors who exercised effective control over the risk that ultimately materialised.[58] Consequently, responsibility may be allocated without adequate consideration of each participant's ability to prevent harm.

This limitation is particularly significant for Ukraine. Existing civil liability mechanisms were developed primarily for disputes involving human decision-makers and offer limited guidance on allocating responsibility in technologically mediated decision-making processes. Ukrainian legislation currently lacks a specialised framework to distinguish between algorithmic defects, system deployment failures, deficiencies in human oversight, and professional medical errors.

As a result, applying traditional joint liability may create legal uncertainty for all participants in AI-assisted healthcare. Healthcare professionals may face liability for failures originating in technological systems beyond their expertise or control. At the same time, technology providers may avoid adequate scrutiny where causal links cannot be clearly established. Such outcomes undermine both fairness and legal predictability.

55 On the allocation of obligations under the EU AI Act and their implications for differentiated responsibility, see Regulation (EU) 2024/1689 (AI Act) (n 2); De Bruyne and Ooms (n 15); Ueda and others (n 9).

56 On the impact of AI-assisted decision-making on traditional concepts of legal liability and professional responsibility, see Shumway and Hartman (n 14); Ueda and others (n 9).

57 On the distributed nature of causation and responsibility in AI-assisted decision-making, see De Bruyne and Ooms (n 15); Wojtczak and Księżak (n 9).

58 On the importance of linking responsibility to control over risk and the ability to prevent harm, see De Bruyne and Ooms (n 15); Ueda and others (n 9).

From a policy perspective, excessive reliance on joint liability may also weaken incentives for risk management. Where responsibility is distributed collectively rather than according to effective control over risk, actors may have reduced incentives to implement safeguards, improve system transparency, or maintain adequate oversight mechanisms.

For these reasons, the growing use of medical AI requires a transition towards a differentiated liability model.[59] Rather than focusing exclusively on participation in a decision-making process, such a model would allocate responsibility according to the actor's function, access to relevant information, capacity to influence system behaviour, and ability to prevent the materialisation of algorithmic risk.

5.2. The Principle of Allocating Liability Through Control Over Risk

A central premise of the proposed differentiated liability model is that legal responsibility should be linked not merely to participation in a medical process but to the degree of control exercised over algorithmic risk.[60] In the context of AI-assisted medical decision-making, the decisive question is not who participated in the operation of the system, but who possessed the practical ability to prevent, mitigate, or manage the risk that ultimately materialised.

This approach reflects a broader tendency within contemporary European AI governance. Although the EU AI Act does not establish a comprehensive liability regime, it distributes legal obligations among different actors according to their functions in ensuring the safety and reliability of high-risk AI systems. The underlying logic is that responsibility should follow control.[61] Actors who possess greater authority over system design, deployment, monitoring, or oversight should bear correspondingly greater responsibility for failures occurring within those domains.

Within such a framework, providers exercise primary control over technological risk. They determine the algorithm's architecture, the quality and representativeness of training data, system design choices, software updates, technical documentation, and compliance mechanisms. Consequently, where harm results from algorithmic defects, inadequate datasets, software malfunctions, or failures of system design, responsibility should primarily rest with the provider because these risks originate within areas under its effective control.[62]

59 For discussions supporting differentiated approaches to responsibility allocation in AI-assisted decision-making, see ibid.

60 On the relationship between legal responsibility, risk governance, and control over algorithmic risk, see ibid.

61 On the functional allocation of obligations according to the actor's capacity to manage and control risks associated with AI systems, see Regulation (EU) 2024/1689 (AI Act) (n 2); Fraser and Bello y Villarino (n 3).

62 On the responsibilities of providers relating to system design, data governance, technical documentation, conformity assessment, and risk management, see Regulation (EU) 2024/1689 (AI Act) (n 2); Göksal, Solarte Vasquez and Chochia (n 33).

© 2026 Volodymyr Kapustnyk and Volodymyr Kurylo. This is an open-access article distributed under the terms of the Creative Commons Attribution License (CC BY 4.0), which permits unrestricted use, distribution, and reproduction in any medium, provided the original author and source are credited.

Deployers, including healthcare institutions, occupy a different position within the risk structure. Although they do not control the system's internal architecture, they exercise organisational control over its implementation and use. Their responsibilities include integrating AI into clinical workflows, complying with operating instructions, organising human oversight, monitoring system performance, and responding to dangerous or anomalous system behaviour.

When harm results from improper implementation, inadequate supervision, or failure to respond to evident system deficiencies, responsibility should fall primarily on the deployer.[63]

A separate layer of responsibility remains attached to healthcare professionals. Using AI-assisted systems does not eliminate the professional duty to evaluate clinical circumstances and exercise independent medical judgement. Physicians retain responsibility for decisions falling within their sphere of professional competence, particularly where they disregard obvious clinical indicators, fail to assess AI-generated recommendations critically, or reduce human oversight to a purely formal exercise.[64]

The proposed model does not allocate responsibility according to institutional status alone. Instead, it allocates responsibility based on where effective control over the relevant risk lies. This distinction matters in medical AI because different categories of risk arise at different stages of the technological process and are controlled by different actors.

Importantly, differentiated liability does not exclude concurrent responsibility. In complex cases, harm may result from a combination of algorithmic defects, deployment failures, and professional error. However, even in such situations, courts should not impose liability by automatically applying joint liability. Instead, courts should assess which actor exercised effective control at the critical stage when the relevant risk materialised and allocate responsibility accordingly.

From the perspective of Ukrainian law, the principle of control over risk offers a more coherent and technologically appropriate framework than traditional collective liability. It improves legal certainty, aligns responsibility with actual capacities to prevent harm, and creates stronger incentives for all participants in the AI ecosystem to maintain adequate safety, transparency, and oversight mechanisms.

Accordingly, control over risk should be the central criterion for future liability allocation in disputes involving AI-assisted medical decision-making. This approach aligns with both the structure of contemporary European AI governance and the practical realities of increasingly digitalised healthcare systems.

63 On the obligations of deployers, including implementation, monitoring, human oversight, and compliance with operational requirements, see Regulation (EU) 2024/1689 (AI Act) (n 2); Söderlund and Larsson (n 3).

64 On the continuing professional responsibility of healthcare practitioners despite the use of AI-assisted systems and on the importance of meaningful human oversight, see Holzinger, Zatloukal and Müller (n 30); Ueda and others (n 9); Zhu and others (n 30).

5.3. Legal Gaps in Ukrainian Medical Law Concerning AI-Assisted Medical Decision-Making

Despite the gradual integration of digital technologies into healthcare, Ukrainian legislation currently lacks a specialised legal framework governing liability for harm caused by the use of artificial intelligence systems in medical decision-making. Existing civil and medical liability mechanisms were developed on the assumption that healthcare professionals and institutions make clinical decisions. Consequently, they are only partially suitable for addressing situations in which algorithmic systems significantly influence diagnostic or therapeutic outcomes.

The Civil Code of Ukraine establishes the general principles of tort liability based on the existence of damage, unlawful conduct, causation, and fault.[65] At the same time, the Fundamentals of Ukrainian Legislation on Health Care define the professional duties of healthcare professionals and the general grounds for liability arising from the improper provision of medical care.[66] However, neither of these legislative acts takes into account the specific features of AI-assisted medical decision-making, algorithmic decision support, or the distributed nature of contemporary digital healthcare processes.

In this context, several key legal gaps emerge.

First, Ukrainian legislation does not distinguish between professional medical error and algorithmic error. Traditional models of medical liability assume that diagnostic and therapeutic decisions originate from healthcare professionals. In AI-assisted healthcare environments, however, harm may result from algorithmic defects, biased training data, technical malfunctions, or system integration failures. Existing legislation does not provide clear criteria for determining whether such harm should be attributed to a physician, a healthcare institution, a technology developer, or several actors simultaneously.

Second, no legal mechanism allocates responsibility among participants in the AI ecosystem. The current regulatory framework does not differentiate between the legal status of developers, providers, operators, healthcare institutions, and healthcare professionals using AI systems. As a result, courts may struggle to determine which actor controlled the risk that ultimately caused the harm.

Third, Ukrainian law does not provide specific procedural mechanisms for accessing algorithmically relevant information.[67] Disputes involving medical AI may require the

65 Civil Code of Ukraine no 435-IV of 16 January 2003 (amended 25 May 2026) <https://zakon.rada.gov.ua/laws/show/435-15> accessed 18 July 2026.

66 Law of Ukraine no 2801-XII of 19 November 1992 'Fundamentals of Ukrainian Legislation on Health Care' (amended 11 February 2026) <https://zakon.rada.gov.ua/laws/show/2801-12#top> accessed 18 July 2026.

67 On evidentiary asymmetry, access to technical information, and the procedural challenges arising in AI-related disputes, see European Committee on Legal Co-operation (n 10); Richmond and others (n 1).

© 2026 Volodymyr Kapustnyk and Volodymyr Kurylo. This is an open-access article distributed under the terms of the Creative Commons Attribution License (CC BY 4.0), which permits unrestricted use, distribution, and reproduction in any medium, provided the original author and source are credited.

examination of event logs, technical documentation, software version records, algorithmic operating parameters, and other forms of digital evidence. Existing procedural legislation was not designed for such disputes and provides only limited opportunities to overcome evidentiary asymmetry between patients and entities controlling technological information.

Fourth, the current legal framework does not define the scope of human oversight in using AI systems in clinical practice.[68] Although healthcare professionals remain responsible for treatment outcomes, Ukrainian law does not establish criteria for determining when reliance on algorithmic recommendations is justified and when it may constitute professional negligence.

These legal gaps are likely to become increasingly significant as AI-assisted technologies continue to expand within the Ukrainian healthcare system. Without specialised regulation, legal uncertainty will increase for patients, healthcare professionals, healthcare institutions, and technology developers alike.

Accordingly, developing a differentiated liability framework is necessary not only to harmonise with European legal approaches but also to address specific deficiencies in the existing Ukrainian system of medical and legal regulation. Such an approach would provide clearer criteria for allocating responsibility, enhance the predictability of judicial practice, and strengthen the protection of patients' rights in the context of the ongoing digital transformation of healthcare.

5.4. A Proposed Model of Differentiated Liability for Ukraine

The analysis conducted in this study suggests that the future regulation of medical AI in Ukraine should move beyond traditional approaches based on collective or undifferentiated liability. Instead, legal responsibility should be allocated according to the degree of control over algorithmic risk and an actor's ability to prevent harm.[69]

The proposed model is based on the principle that liability should follow control.[70] Different participants in AI-assisted medical decision-making exercise control over different stages of the technological and clinical process and should therefore bear responsibility only within their respective spheres of influence.

68 On meaningful human oversight as a legal and governance requirement for AI-assisted decision-making, see Regulation (EU) 2024/1689 (AI Act) (n 2); Holzinger, Zatloukal and Müller (n 30); Zhu and others (n 30).

69 On the allocation of legal responsibility according to control over risk and the capacity to prevent harm, see De Bruyne and Ooms (n 15); Ueda and others (n 9).

70 On the functional allocation of obligations among actors participating in the AI lifecycle, see Regulation (EU) 2024/1689 (AI Act) (n 2); Söderlund and Larsson (n 3).

At the technological level, AI system providers should bear primary responsibility.[71] Providers control the architecture of algorithms, the quality of training data, software development, system updates, cybersecurity measures, and compliance with technical requirements. Accordingly, where harm results from an algorithmic defect, non-representative data, software malfunction, or deficiencies in system design, liability should primarily rest with the actor controlling those risks.

A separate layer of responsibility should apply to deployers, including healthcare institutions implementing AI technologies in clinical practice.[72] Such entities exercise organisational control over the use of AI systems and are responsible for their proper integration into healthcare processes. Their obligations include staff training, organising meaningful human oversight, monitoring system performance, and responding to identified risks. Consequently, when harm results from improper implementation, inadequate supervision, or the failure to address known system deficiencies, liability should be attributed primarily to the deployer.

Professional liability should remain attached to healthcare professionals. Although AI systems may substantially influence clinical decision-making, physicians continue to exercise professional medical judgement and remain responsible for final decisions about diagnosis and treatment. Where a healthcare professional relies uncritically on algorithmic recommendations, disregards obvious clinical indicators, or fails to exercise adequate professional oversight, liability should arise based on traditional principles of professional negligence.[73]

The proposed framework also recognises mixed-causation cases. In practice, harm may result from a combination of algorithmic defects, organisational deployment failures, and professional error. In such situations, courts should not automatically apply joint-liability mechanisms. Instead, they should determine which actor exercised effective control over the stage of the process at which the relevant algorithmic risk materialised and allocate liability in accordance with each participant's actual contribution to the harm.

Implementing such a model would require appropriate procedural mechanisms. Courts should have access to event logs, technical documentation, audit trails, and other forms of algorithmically relevant evidence. Where such information remains exclusively

71 On the responsibilities of providers relating to system design, data governance, technical documentation, risk management, conformity assessment, and compliance with safety requirements, see Regulation (EU) 2024/1689 (AI Act) (n 2); Göksal, Solarte Vasquez and Chochia (n 33).

72 On the obligations of deployers, including implementation, monitoring, staff training, human oversight, and compliance with operational requirements, see Regulation (EU) 2024/1689 (AI Act) (n 2); Söderlund and Larsson (n 3).

73 On the continuing professional responsibility of healthcare practitioners and the importance of meaningful human oversight in AI-assisted decision-making, see Holzinger, Zatloukal and Müller (n 30); Ueda and others (n 9); Zhu and others (n 30).

© 2026 Volodymyr Kapustnyk and Volodymyr Kurylo. This is an open-access article distributed under the terms of the Creative Commons Attribution License (CC BY 4.0), which permits unrestricted use, distribution, and reproduction in any medium, provided the original author and source are credited.

under the control of providers or deployers, courts may consider introducing specific procedural mechanisms to facilitate access to digital evidence or, where justified, partially shifting the burden of proof.

For Ukraine, the proposed model offers several advantages. It enhances legal certainty, aligns liability with actors' actual capacity to prevent harm, encourages compliance with standards of safe AI use, and contributes to the development of an effective system of AI governance in healthcare.

Accordingly, a differentiated liability framework based on the principle of control over algorithmic risk may serve as a conceptual foundation for the future transformation of Ukrainian medical law in the era of AI-assisted medical decision-making.

5.5. Human Oversight as a Legal Duty in the Field of Medical AI

A differentiated liability framework in medical AI cannot function effectively without a clear definition of human oversight. Although human oversight is commonly presented as a technical safeguard designed to reduce the risks associated with high-risk AI systems, its significance extends beyond regulatory compliance. In the context of legal liability, human oversight should be understood as a distinct legal duty that connects technological decision support systems with human accountability.[74]

This principle stems from the fact that AI-assisted medical decision-making remains fundamentally different from fully autonomous decision-making. Even when sophisticated clinical decision support systems influence diagnosis, treatment selection, or risk assessment, medical decisions remain within a professional environment governed by legal and ethical duties. Accordingly, responsibility cannot be transferred entirely to technological systems.[75]

At the same time, meaningful human oversight requires more than the formal presence of a healthcare professional within a decision-making process. Oversight becomes ineffective where users lack sufficient information to understand system outputs, cannot assess the reliability of recommendations, or are deprived of practical opportunities to intervene. In such circumstances, attributing responsibility solely to healthcare professionals would undermine the principle that liability should correspond to actual control over risk.[76]

74 On meaningful human oversight as a mechanism linking AI governance with legal accountability, see Regulation (EU) 2024/1689 (AI Act) (n 2); Holzinger, Zatloukal and Müller (n 30); Zhu and others (n 30).

75 On the continuing responsibility of human decision-makers in AI-assisted environments, see Regulation (EU) 2024/1689 (AI Act) (n 2); Ueda and others (n 9).

76 On the relationship between supervision, risk control, and responsibility allocation, see De Bruyne and Ooms (n 15); Zhu and others (n 30).

For this reason, human oversight should be analysed as a relational concept linking responsibility to the actor's capacity to supervise algorithmic decision-making. The scope of this duty depends on several factors, including the user's professional role, access to relevant information, the level of system explainability, and the practical ability to influence outcomes generated by the AI system.

This approach matters in healthcare because of the well-documented phenomenon of automation bias.[77] Healthcare professionals may develop excessive reliance on algorithmic recommendations, especially where AI systems demonstrate high levels of accuracy or operate within complex clinical environments. However, automation bias does not eliminate professional responsibility. Rather, it reinforces the need to define when reliance on AI-generated outputs remains reasonable and when independent clinical assessment is required.

Recent Ukrainian judicial practice concerning the professional use of AI, although not directly related to healthcare, illustrates an emerging understanding of human oversight as a legal obligation rather than a purely technical recommendation.[78] Ukrainian courts increasingly emphasise that individuals who rely on AI-generated outputs retain responsibility for verifying information and for decisions made based on such outputs. This tendency supports the broader proposition that accountability should remain connected to the human actor exercising supervisory authority over AI-assisted processes.

Within the proposed differentiated liability model, human oversight constitutes a separate layer of legal responsibility. It should neither serve as a mechanism for transferring all responsibility to healthcare professionals nor be reduced to a symbolic requirement that legitimises algorithmic decision-making. Instead, it functions as a criterion for determining whether the actor responsible for supervising an AI-assisted process exercised the level of control reasonably expected under the circumstances.

Accordingly, human oversight should be regarded as a central component of AI accountability in healthcare. It preserves the link between professional judgement and legal responsibility while ensuring liability remains tied to real opportunities for supervision, intervention, and harm prevention.

77 On automation bias and excessive reliance on algorithmic recommendations in professional decision-making, see Florian Kücking and others, 'Automation Bias in AI-Decision Support: Results from an Empirical Study' in Rainer Röhrig and others (eds), *German Medical Data Sciences 2024: Health - Thinking, Researching and Acting Together* (IOS Press 2024) 298 <https://doi.org/10.3233/shti240871> accessed 18 July 2026; Perica Jovchevski, Stefan Buijsman and Mark Neerincx, 'What Is Wrong with Automation Bias?' (2026) 39 Philosophy & Technology 84 <https://doi.org/10.1007/s13347-026-01090-9> accessed 18 July 2026.

78 Case no 925/496/24 (n 27); Case no 240/14153/24 (n 27); Case no 620/12085/25 (n 27).

© 2026 Volodymyr Kapustnyk and Volodymyr Kurylo. This is an open-access article distributed under the terms of the Creative Commons Attribution License (CC BY 4.0), which permits unrestricted use, distribution, and reproduction in any medium, provided the original author and source are credited.

5.6. Logging, Explainability, and Digital Evidence in Medical AI Disputes

The practical implementation of differentiated liability in medical AI disputes depends on mechanisms that can identify how algorithmic risk materialised and which actor controlled the relevant stage of the decision-making process. Logging, explainability, and traceability should therefore be regarded not merely as technical features of AI systems but as essential components of an accountability infrastructure.[79] Without reliable information concerning system operation, courts may be unable to distinguish between failures originating in system design, deployment, human oversight, or clinical decision-making. Consequently, differentiated liability requires sufficient technical and evidentiary mechanisms to reconstruct the pathway through which harm occurred.

From a legal perspective, logging, explainability, and traceability transform the principle of control over risk into a practically enforceable standard. Event logs, technical documentation, audit trails, and other forms of algorithmically relevant evidence enable courts to determine which actor controlled the relevant stage of the decision-making process and whether appropriate oversight was exercised. For Ukraine, developing such digital evidentiary infrastructure may become a necessary precondition for effectively implementing differentiated liability in healthcare and for meaningfully assessing causation in disputes involving AI-assisted medical decision-making.

6 CONCLUSIONS

The growing use of high-risk artificial intelligence systems in healthcare challenges traditional approaches to medical liability. AI-assisted medical decision-making no longer rests solely on healthcare professionals; it emerges from the interaction of multiple actors, including algorithm developers, technology providers, healthcare institutions, and medical practitioners. Under such circumstances, traditional models of joint liability increasingly prove inadequate for ensuring a fair and predictable allocation of responsibility. The comparative and doctrinal analysis in this study shows that this transformation cannot be addressed by merely extending traditional concepts of joint liability; instead, it requires a functional allocation of legal responsibility that reflects the governance structure of high-risk AI systems.

This study shows that the EU AI Act is significant not only as a regulatory instrument governing high-risk AI systems but also as a normative and conceptual foundation for developing a differentiated liability model. By functionally allocating obligations among

79 On the evidentiary significance of logging, explainability, traceability, and digital accountability mechanisms in AI-assisted decision-making, see Makauskaite-Samuole (n 5); Richmond and others (n 1); Söderlund (n 8).

providers, deployers, and other participants in the AI ecosystem, the EU AI Act provides a legal basis for transitioning from undifferentiated collective liability to a differentiated liability framework grounded in control over algorithmic risk.

The article argues that differentiated liability better suits disputes involving medical AI than traditional models of collective liability. Legal responsibility should be determined by the degree of control exercised over the relevant risk, access to technically significant information, the ability to influence system operation, and the capacity to prevent harm. Accordingly, control over risk should serve as the central criterion for future liability allocation in disputes arising from AI-assisted medical decision-making.

The study further demonstrates that an effective differentiated liability framework depends on meaningful human oversight supported by an adequate digital evidentiary infrastructure. Explainability, logging, traceability, and access to algorithmically relevant evidence serve important evidentiary functions by helping establish causation and identify the actor responsible at a particular stage of AI-assisted decision-making.

The Estonian experience in digital healthcare shows that an effective liability system depends not only on substantive liability rules but also on integrating digital governance, institutional accountability, and evidentiary infrastructure supported by transparent technological safeguards and an appropriate legal framework. This comparative experience offers valuable guidance for the future development of Ukrainian medical law. At the same time, contemporary Ukrainian judicial practice on the professional use of artificial intelligence indicates the gradual emergence of an approach in which meaningful human oversight is recognised as an independent legal duty linking the use of AI technologies to human responsibility. Taken together, these developments suggest that effective legal regulation of AI-assisted healthcare requires the parallel development of legal accountability and digital governance mechanisms to ensure effective judicial protection.

For Ukraine, the findings of this study demonstrate the need to reconsider traditional liability models developed for exclusively human decision-making environments. Although current legislation does not yet provide a specialised liability regime for medical AI, future legislative reform should establish a differentiated allocation of responsibility among providers, deployers, healthcare institutions, and healthcare professionals according to their respective degree of control over algorithmic risk. Such reform should define each participant's legal responsibilities in the AI-assisted healthcare ecosystem, establish evidentiary rules governing the preservation and disclosure of algorithmically relevant evidence, including logging and traceability, strengthen requirements for meaningful human oversight, and ensure effective judicial access to technically relevant information.

Accordingly, the future development of Ukrainian medical law should transition from formal collective liability to a differentiated liability framework in which legal responsibility

© 2026 Volodymyr Kapustnyk and Volodymyr Kurylo. This is an open-access article distributed under the terms of the Creative Commons Attribution License (CC BY 4.0), which permits unrestricted use, distribution, and reproduction in any medium, provided the original author and source are credited.

is allocated according to the degree of control exercised over algorithmic risk. Such a framework would enhance legal certainty, improve responsibility allocation among participants in AI-assisted healthcare, and strengthen the effective protection of patients' rights through an appropriate combination of digital accountability, meaningful human oversight, and access to algorithmically relevant evidence.

REFERENCES

1. Atkinson K, Bench-Capon T and Bollegala D, 'Explanation in AI and Law: Past, Present and Future' (2020) 289 Artificial Intelligence 103387 <https://doi.org/10.1016/j.artint.2020.103387> accessed 18 July 2026
2. Bellogín A and others, 'The EU AI Act and the Wager on Trustworthy AI' (2024) 67(12) Communications of the ACM 58 <https://doi.org/10.1145/3665322> accessed 18 July 2026
3. Bernstein MH and others, 'Randomized Study of the Impact of AI on Perceived Legal Liability for Radiologists' (2025) 2(6) NEJM AI <https://doi.org/10.1056/AIoa2400785> accessed 18 July 2026
4. De Bruyne J and Ooms W, 'Tort Liability and Artificial Intelligence: Some Challenges and (Regulatory) Responses' in Smuha NA (ed), *The Cambridge Handbook of the Law, Ethics and Policy of Artificial Intelligence* (CUP 2025) 158 <http://doi.org/10.1017/9781009367783.011> accessed 18 July 2026
5. Fraser H and Bello y Villarino JM, 'Acceptable Risks in Europe's Proposed AI Act: Reasonableness and Other Principles for Deciding How Much Risk Management is Enough' (2024) 15(2) European Journal of Risk Regulation 431 <https://doi.org/10.1017/err.2023.57> accessed 18 July 2026
6. Göksal Şİ, Solarte Vasquez MC and Chochia A, 'The EU AI Act's Alignment within the European Union's Regulatory Framework on Artificial Intelligence' (2024) 24(2) International and Comparative Law Review 25 <https://doi.org/10.2478/iclr-2024-0017> accessed 18 July 2026
7. Holzinger A, Zatloukal K and Müller H, 'Is Human Oversight to AI Systems Still Possible?' (2025) 85 New Biotechnology 59 <https://doi.org/10.1016/j.nbt.2024.12.003> accessed 18 July 2026
8. Jin Q and others, 'Hidden Flaws Behind Expert-Level Accuracy of Multimodal GPT-4 Vision in Medicine' (2024) 7 npj Digital Medicine 190 <https://doi.org/10.1038/s41746-024-01185-7> accessed 18 July 2026
9. Joshi G and others, 'FDA-Approved Artificial Intelligence and Machine Learning (AI/ML)-Enabled Medical Devices: An Updated Landscape' (2024) 13(3) Electronics 498 <https://doi.org/10.3390/electronics13030498> accessed 18 July 2026

10. Jovchevski P, Buijsman S and Neerincx M, 'What Is Wrong with Automation Bias?' (2026) 39 Philosophy & Technology 84 <https://doi.org/10.1007/s13347-026-01090-9> accessed 18 July 2026

11. Kaladharan S, Manayath D and Gopalakrishnan R, 'Regulatory Challenges in AI/ML-Enabled Medical Devices: A Scoping Review and Conceptual Framework' (2024) 18(4) Journal of Medical Devices 040801 <https://doi.org/10.1115/1.4066280> accessed 18 July 2026

12. Kasekamp K and others, '*Estonia: Health System Review 2023*' (2023) 25(5) Health Systems in Transition 1 <https://eurohealthobservatory.who.int/publications/i/estonia-health-system-review-2023> accessed 18 July 2026

13. Kiejnich-Kruk K, 'The AI Act: Challenges for Justice and Democracy in the Deployment of AI-Based Systems' (2026) 31(1) *Białostockie Studia Prawnicze* 115 <https://doi.org/10.15290/bsp.2026.31.01.07> accessed 18 July 2026

14. Kinchin N, '"Voiceless": The Procedural Gap in Algorithmic Justice' (2024) 32 International Journal of Law and Information Technology eaae024 <https://doi.org/10.1093/ijlit/eaae024> accessed 18 July 2026

15. Kücking F and others, 'Automation Bias in AI-Decision Support: Results from an Empirical Study' in Röhrig R and others (eds), *German Medical Data Sciences 2024: Health - Thinking, Researching and Acting Together* (IOS Press 2024) 298 <https://doi.org/10.3233/shti240871> accessed 18 July 2026

16. Makauskaite-Samuole G, 'Transparency in the Labyrinths of the EU AI Act: Smart or Disbalanced?' (2025) 8(2) Access to Justice in Eastern Europe 38 <https://doi.org/10.33327/AJEE-18-8.2-a000105> accessed 18 July 2026

17. Milani L and others, 'The Estonian Biobank's Journey from Biobanking to Personalized Medicine' (2025) 16 Nature Communications 3270 <https://doi.org/10.1038/s41467-025-58465-3> accessed 18 July 2026

18. Noë A, Bouhouita-Guermech S and Zawati MH, 'The Right to Explanation in AI: In a Lonely Place' (2025) 27 Journal of Medical Internet Research e64482 <https://doi.org/10.2196/64482> accessed 18 July 2026

19. Richmond KM and others, 'Explainable AI and Law: An Evidential Survey' (2024) 3(1) Digital Society 1 <https://doi.org/10.1007/s44206-023-00081-z> accessed 18 July 2026

20. Shumway DO and Hartman HJ, 'Medical Malpractice Liability in Large Language Model Artificial Intelligence: Legal Review and Policy Recommendations' (2024) 124(7) Journal of Osteopathic Medicine 287 <https://doi.org/10.1515/jom-2023-0229> accessed 18 July 2026

21. Söderlund K, 'High-Risk AI Transparency? On Qualified Transparency Mandates for Oversight Bodies under the EU AI Act' (2025) 2025 Technology and Regulation 97 <https://doi.org/10.71265/6bedar76> accessed 18 July 2026

© 2026 Volodymyr Kapustnyk and Volodymyr Kurylo. This is an open-access article distributed under the terms of the Creative Commons Attribution License (CC BY 4.0), which permits unrestricted use, distribution, and reproduction in any medium, provided the original author and source are credited.

22. Söderlund K and Larsson S, 'Enforcement Design Patterns in EU Law: An Analysis of the AI Act' (2024) 3 Digital Society 41 <https://doi.org/10.1007/s44206-024-00129-8> accessed 18 July 2026

23. Ueda D and others, 'Legal Liability of Physicians and New Governance in the AI Era' (2026) 44 Japanese Journal of Radiology 1316 <https://doi.org/10.1007/s11604-026-01997-5> accessed 18 July 2026

24. Varošanec I, 'On the Path to the Future: Mapping the Notion of Transparency in the EU Regulatory Framework for AI' (2022) 36(2) International Review of Law, Computers & Technology 95 <https://doi.org/10.1080/13600869.2022.2060471> accessed 18 July 2026

25. Wojtczak S and Księżak S, 'Causation in Civil Law and the Problems of Transparency in AI' (2021) 29(4) European Review of Private Law 561 <https://doi.org/10.54648/erpl2021030> accessed 18 July 2026

26. Zhu L and others, 'Designing Meaningful Human Oversight in AI' (2026) 6 AI and Ethics 286 <https://doi.org/10.1007/s43681-026-01147-7> accessed 18 July 2026

AUTHORS' INFORMATION

Volodymyr Kapustnyk*
Dr. Sc. (Law), Associate Professor, Professor of the Department of Forensic Medicine, Medical Law named after Honoured Professor M.S. Bokarius, Kharkiv National Medical University, Kharkiv, Ukraine
vv.kapustnyk@knmu.edu.ua
https://orcid.org/0000-0003-0733-4233
Corresponding author, responsible for Conceptualisation, Methodology, Formal Analysis, Investigation, Legal Analysis, Writing – Original Draft Preparation, Writing – Review & Editing.

Volodymyr Kurylo
PhD in Law, Judge, Novobavarskyi District Court of Kharkiv, Ukraine
kurylo-volodymyr@ukr.net
https://orcid.org/0009-0002-8032-6387
Co-author, responsible for Methodology, Formal Analysis, Legal Analysis, Writing – Review & Editing, Supervision.

Competing interests: No competing interests were disclosed.

Disclaimer: The authors declare that their opinions and views expressed in this manuscript are free of the influence of any organisations.

FUNDING AND APC STATEMENT

The authors received no specific grant or external funding for the research and publication of this article. Consequently, the publisher partially waived the APC (50%) in accordance with the AJEE Charges Policy for authors from Lower-Middle-Income countries (as per World Bank classification). The authors and/or their institutions covered the remaining balance.

RIGHTS AND PERMISSIONS

Copyright: © 2026 Volodymyr Kapustnyk and Volodymyr Kurylo. This is an open-access article distributed under the terms of the Creative Commons Attribution License (CC BY 4.0), which permits unrestricted use, distribution, and reproduction in any medium, provided the original author and source are credited.

EDITORS

Managing Editor – Mag. Bohdana Zahrebelna. **English Editor** – Robert Reddin.
Ukrainian Editor – Liliia Hartman.

ABOUT THIS ARTICLE

Cite this article
Kapustnyk V and Kurylo V, 'From Joint to Differentiated Liability: Reforming Ukrainian Medical Law in Light of the EU AI Act and the Estonian Experience' (2026) 9(4) Access to Justice in Eastern Europe 1-34 <https://doi.org/10.33327/AJEE-18-9.4-a0002009> Published Online 30 Sep 2026

DOI: https://doi.org/10.33327/AJEE-18-9.4-a0002009

Summary: 1. Introduction. – 2. Methodology. – 3. The Crisis of Traditional Liability Models in Medical AI Disputes. – *3.1. The Transformation of Medical Decision-Making in AI-Assisted Systems.* – *3.2. The Black Box Effect and the Problem of Causation.* – *3.3. Procedural Asymmetry and Access to Justice.* – *3.4. The Emergence of the Principle of Human Oversight in Contemporary Judicial Practice.* – 4. The EU AI Act and the Emergence of a Differentiated Liability Model in Medical AI. – *4.1. The Risk-Based Approach of the EU AI Act.* – *4.2. The Estonian Model of Digital Accountability and Human Oversight.* – *4.3. The Significance of the European Approach for Ukraine.* – 5. A Differentiated Liability Framework for Ukraine. – *5.1. The Inadequacy of Traditional*

Joint Liability in Medical AI Disputes. – 5.2. The Principle of Allocating Liability Through Control Over Risk. – 5.3. Legal Gaps in Ukrainian Medical Law Concerning AI-Assisted Medical Decision-Making. – 5.4. A Proposed Model of Differentiated Liability for Ukraine. – 5.5. Human Oversight as a Legal Duty in the Field of Medical AI. – 5.6. Logging, Explainability, and Digital Evidence in Medical AI Disputes. – 6. Conclusions.

Keywords**:** *Artificial intelligence; Medical AI; Medical liability; Joint liability; Differentiated liability; Human oversight; Explainability; Traceability; Logging; Access to justice; Article 6 ECHR; Algorithmic accountability; Digital evidence; Medical law.*

DETAILS FOR PUBLICATION

Date of submission: 01 Jun 2026
Date of acceptance: 24 Jul 2026
Online First Publication: 30 Sep 2026
Publication: Nov 2026
Was the manuscript fast-tracked? - No
Number of reviewer reports submitted in the first round: 4 reports
Number of revision rounds: 3 rounds with major revisions

Technical tools used in the editorial process

Plagiarism checks - Turnitin from iThenticate
https://www.turnitin.com/products/ithenticate/
Scholastica for Peer Review
https://scholasticahq.com/law-reviews
Paperpal for Academic Editing & Proofreading
https://paperpal.com/

AI DISCLOSURE STATEMENT

The authors prepared the manuscript. They only used AI tools for spelling, grammar, and stylistic refinement. No generative AI was used to produce original content, research ideas, or analysis.

АНОТАЦІЯ УКРАЇНСЬКОЮ МОВОЮ

Дослідницька стаття

ВІД СОЛІДАРНОЇ ДО ДИФЕРЕНЦІЙОВАНОЇ ВІДПОВІДАЛЬНОСТІ: РЕФОРМУВАННЯ МЕДИЧНОГО ПРАВА УКРАЇНИ З УРАХУВАННЯМ АКТА ЄС ПРО ШТУЧНИЙ ІНТЕЛЕКТ ТА ДОСВІДУ ЕСТОНІЇ

Володимир Капустник* та Володимир Курило

АНОТАЦІЯ

Передумови. *Зростання масштабів застосування високоризикових систем штучного інтелекту (ШІ) у сфері охорони здоров'я створює нові виклики традиційним моделям юридичної відповідальності у медицині, зокрема у випадках, коли клінічні рішення формуються внаслідок взаємодії медичних працівників, закладів охорони здоров'я, постачальників програмного забезпечення та алгоритмічних систем. За таких умов встановлення причинно-наслідкового зв'язку та розподіл юридичної відповідальності істотно ускладнюється через непрозорість алгоритмічних процесів, розподілений характер ухвалення рішень та залучення багатьох суб'єктів із різним ступенем контролю над ризиками, пов'язаними із ШІ.*

Методи. *У дослідженні застосовано доктринальний та порівняльно-правовий методи для аналізу трансформації моделей юридичної відповідальності в контексті ухвалення медичних рішень із застосуванням ШІ. Дослідження ґрунтується на нормах цивільного та медичного законодавства України, положеннях Регламенту (ЄС) 2024/1689 «Акт про штучний інтелект» (Акт ЄС про ШІ), стандартах забезпечення права на доступ до правосуддя відповідно до статті 6 Конвенції про захист прав людини і основоположних свобод, а також на естонській моделі цифрового врядування та підзвітності у сфері охорони здоров'я.*

Результати та висновки. *Доведено, що традиційні моделі солідарної відповідальності стають дедалі менш придатними для вирішення спорів щодо застосування високоризикових медичних систем ШІ, оскільки вони не розмежовують суб'єктів за критерієм здійснення фактичного контролю над алгоритмічним ризиком. Обґрунтовано, що Акт ЄС про ШІ забезпечує нормативне й концептуальне підґрунтя для запровадження диференційованої моделі відповідальності, заснованої на засадах функціональної відповідальності, людського нагляду та ризик-орієнтованого управління. Особливу увагу приділено процесуальному значенню пояснюваності (explainability), логування (протоколювання подій) та простежуваності як механізмів, які сприяють встановленню причинного зв'язку, забезпеченню доступу до доказів і здійсненню дієвого судового контролю. Досвід Естонії демонструє, як інфраструктура цифрової підзвітності, підкріплена чітким розподілом інституційних обов'язків та належним нормативно-правовим регулюванням, може сприяти посиленню нагляду за*

© 2026 Volodymyr Kapustnyk and Volodymyr Kurylo. This is an open-access article distributed under the terms of the Creative Commons Attribution License (CC BY 4.0), which permits unrestricted use, distribution, and reproduction in any medium, provided the original author and source are credited.

процесом ухвалення медичних рішень із застосуванням ШІ. Виявлено ключові законодавчі прогалини медичного права України у сфері застосування ШІ та запропоновано практичні напрями реформування, включно з моделлю диференційованої відповідальності за критерієм контролю над алгоритмічним ризиком. Зроблено висновок, що такий підхід формує більш послідовну та юридично передбачувану основу для розподілу відповідальності в охороні здоров'я, ніж класичні конструкції колективної відповідальності, та гармонізується з актуальними європейськими підходами до регулювання ШІ та юридичної відповідальності.

Ключові слова: *штучний інтелект, ШІ в медичній сфері, медична відповідальність, солідарна відповідальність, диференційована відповідальність, людський нагляд, пояснюваність, простежуваність, логування (протоколювання), доступ до правосуддя, стаття 6 ЄКПЛ, алгоритмічна підзвітність, цифрові докази, медичне право.*