Proceedings of the 19th International Scientific and Practical Conference «Scientific Horizon in the Context of Social Crises»

(August 16-18, 2026). Tokyo, Japan

No 305

PHILOSOPHY AND COGNITION

European Approaches to the Legal Regulation of Artificial Intelligence in Health Care: Prospects for Adaptation in Ukraine

Grygorenko Artem[1], Mikhaliev Kyrylo[2]

[1]Doctor of Philosophy in Law, Researcher (Law) at the Scientific Department of Educational and Information Technologies;
State Institution of Science "Center of innovative healthcare technologies" State Administrative Department (SIS "CIHT" SAD), Ukraine

[2]Doctor of Philosophy in Medicine, Senior Researcher, Head of the Scientific Department of Educational and Information Technologies;
State Institution of Science "Center of innovative healthcare technologies" State Administrative Department (SIS "CIHT" SAD), Ukraine

The digital transformation of health care relies increasingly on artificial intelligence (AI) technologies — from the automated interpretation of medical images to the prediction of disease course and the personalization of treatment protocols. The integration of algorithms into clinical practice, however, inevitably brings legal challenges that call for a response. The European Union has developed the most advanced model to date, one that combines the protection of fundamental human rights with support for technological innovation. For Ukraine, which is actively rolling out its electronic health care system (eHealth), the study of these approaches is not merely a theoretical task but an applied one, since the absence of comprehensive AI regulation creates risks for patients and legal uncertainty for physicians and developers [1-4].

The current European architecture for the legal regulation of AI rests on several interrelated instruments. The foundational document is the EU Artificial Intelligence Act [5], which introduces a *risk-based approach:* as a general rule, medical AI systems are classified as high-risk systems. This entails mandatory compliance with the applicable requirements throughout the entire product life cycle: risk management, high-quality data, human oversight and so on. Another important element is the protection of personal health

PHILOSOPHY AND COGNITION

data under the GDPR [6]. It lays down strict rules for processing sensitive information, requires data to be de-identified when algorithms are trained, and provides for substantial fines for non-compliance. The third element is the creation of the European Health Data Space (EHDS) [7], which enables the cross-border exchange of health data. The fourth element is the regulation of AI systems as medical devices under EU Regulation 2017/745 [8]. Where software is used to establish a diagnosis, determine treatment strategy or monitor a patient, it must undergo conformity assessment, clinical evaluation and certification. The model in question is therefore multi-layered and covers the stages from development to operation.

Ukraine has already made a certain amount of progress in the digitalization of health care, which provides a basis for introducing the mechanisms outlined above. An electronic health care system is being deployed, telemedicine and electronic prescriptions are developing, and the Concept for the Development of Artificial Intelligence has been approved [9]. At the same time, national legislation regulates only individual aspects (personal data protection [10] and the general principles of medical practice [11]), while containing no specific rules on the circulation of medical AI systems, their certification, clinical evaluation or the allocation of liability for algorithmic errors. A key obstacle is the absence of statutory definitions of fundamental concepts — for instance, what a "medical artificial intelligence system" is, the procedure for its state registration and other requirements, as well as mechanisms for apportioning liability. Alongside this, Ukraine's course towards European integration and the need to harmonize domestic legislation create the political and legal preconditions for the systematic implementation of these standards. It should be noted, however, that this process cannot amount to a mechanical copying of European instruments: it requires that the specific features of the Ukrainian health care system and the level of development of its digital infrastructure be taken into account. The following lines of work therefore appear appropriate:

1. ***Establishing the legal status of medical AI systems in legislation***, with clear classification criteria and defined procedures for conformity assessment, certification and state supervision. This would remove the legal uncertainty that arises when algorithms are applied in clinical practice.

PHILOSOPHY AND COGNITION

2. ***Introducing risk-based regulation*** — on the European model, not all AI systems require the same level of oversight. High-risk systems (diagnosis, choice of treatment) should be subject to enhanced requirements for safety, transparency and clinical validation, whereas simplified regulation is feasible for administrative tools.

3. ***Developing a mechanism for allocating legal liability*** — statutory definition of the liability of the software developer (for algorithmic defects), the medical device manufacturer (for the hardware), the health care facility (for implementation and staff training) and the physician (for the final clinical decision), which would make enforcement predictable.

4. ***Establishing a system of independent expert review*** — creating an institutional mechanism for reviewing algorithms at the development stage and throughout their operation against criteria of safety, clinical effectiveness, non-discrimination, cyber-resilience and ethical compliance. It would be advisable to draw on the experience of European conformity assessment bodies.

5. ***Providing a regulatory basis for transparency and patients' rights*** — establishing an obligation to inform the patient that AI is being used in the delivery of care, and guaranteeing the possibility of obtaining an intelligible explanation of the algorithm's role in a clinical decision. Such an approach meets the requirements for explainability of decision-making and secures the patient's right to informed consent.

6. ***Strengthening information security requirements*** — providing for the mandatory use of up-to-date cryptographic protection, multi-factor authentication and regular cybersecurity audits of the information systems of health care institutions in line with generally recognized standards.

7. ***Building institutional capacity*** — establishing a specialized advisory or coordinating body under the Ministry of Health (or the Ministry of Digital Transformation) that would provide methodological support for the introduction of AI, monitor its use, liaise with international organizations and prepare proposals for improving the legislative framework.

The paper draws on the results of research carried out as part of the research project of the Scientific Department of Healthcare Organization of the State Institution of Science "Center of innovative healthcare technologies" State Administrative Department, entitled «Medical and social justification, development and implementation of the «Center

of innovative healthcare technologies» model based on the trinity of science, education and practice in the work of a multidisciplinary healthcare institution and determining its role in the formation of a single medical space» (implementation period 2025-2029, state registration No. 0125U0000318).

References:

[6] Grygorenko A, Mikhaliev K. Pravovi aspekty intehratsii shtuchnoho intelektu v okhoronu zdorovia: mizhnarodnyi dosvid ta osnovni bariery. [Legal Aspects of Artificial Intelligence Integration into Healthcare: International Experience and Major Barriers]. Artificial Intelligence. 2026;31(2):14-22. doi: 10.15407/jai2026.02.014. (Ukrainian)

[7] Bidenko N, Stuchynska N, Palamarchuk Y, Matviienko M. Integrating Artificial Intelligence in Healthcare Practice: Challenges and Future Prospects. Wiadomości Lekarskie. 2025;78(5):1199-1205. doi: 10.36740/WLek/205397

[8] Servy H, Braithwaite B, Kiltz U. et al. Artificial intelligence in healthcare faces regulatory challenges: balancing innovation with human oversight. EULAR Rheumatology Open. 2026;2(1):283-288. doi: 10.1016/j.ero.2026.02.010

[9] WHO. Ethics and Governance of Artificial Intelligence for Health. https://www.who.int/publications/i/item/9789240029200 [Accessed 30 July 2026]

[10] Regulation (EU) 2024/1689 of the European Parliament and of the Council on artificial intelligence (Artificial Intelligence Act). https://eur-lex.europa.eu/eli/reg/2024/1689/oj/eng [Accessed 30 July 2026]

[11] Regulation (EU) 2016/679 of the European Parliament and of the Council on the protection of natural persons with regard to the processing of personal data (General Data Protection Regulation). Available from: https://eur-lex.europa.eu/eli/reg/2016/679/oj/eng [Accessed 30 July 2026]

[12] Regulation (EU) 2025/327 of the European Parliament and of the Council on the European Health Data Space. Available from: https://eur-lex.europa.eu/eli/reg/2025/327/oj/eng [Accessed 30 July 2026]

[13] Regulation (EU) 2017/745 of the European Parliament and of the Council on medical devices. Available from: https://eur-lex.europa.eu/eli/reg/2017/745/oj/eng [Accessed 30 July 2026]

[14] Kabinet Ministriv Ukrainy. Pro skhvalennia Kontseptsii rozvytku shtuchnoho intelektu v Ukraini. [On approval of the Concept for the development of artificial intelligence in Ukraine]. Order No. 1556-r; 2020. https://zakon.rada.gov.ua/laws/show/1556-2020-p [Accessed 30 July 2026] (Ukrainian)

[15] Verkhovna Rada of Ukraine. Osnovy zakonodavstva Ukrainy pro okhoronu zdorovia. [Fundamentals of the legislation of Ukraine on health care]. Law of Ukraine No. 2801-XII; 1992. https://zakon.rada.gov.ua/laws/show/2801-12#Text [Accessed 30 July 2026] (Ukrainian)

[16] Verkhovna Rada of Ukraine. Pro zakhyst personalnykh danykh. [On personal data protection]. Law of Ukraine No. 2297-VI; 2010. https://zakon.rada.gov.ua/laws/show/2297-17#Text [Accessed 30 July 2026] (Ukrainian)