

CHAPTER 2

INTERNET OF THINGS: ETHICAL AND LEGAL DIMENSIONS OF THE NEW TECHNOLOGICAL ENVIRONMENT

Horielova Veronika, PhD in Law, Associate Professor, Associate Professor
at the Department of State-Legal and Humanitarian Sciences V.I. Vernadsky
Taurida National University

The article is devoted to an analysis of the ethical challenges arising from the rapid proliferation of Internet of Things technologies. Drawing on the report of the World Commission on the Ethics of Scientific Knowledge and Technology of UNESCO (COMEST, 2021), the study examines transformations at the individual, social, and policy levels. It addresses issues of privacy, informed consent, personal autonomy, gender stereotypes, domestic violence involving the use of IoT, environmental impacts, as well as the risks of pervasive surveillance and the opportunities of citizen sensing. The article proposes ways of improving regulation through the concept of ethics by design and the implementation of international standards.

Keywords: Internet of Things, ethics, privacy, informed consent, domestic violence, citizen sensing, regulation.

The issue of the ethical conceptualisation of the Internet of Things has become particularly acute today due to the fact that technologies are ceasing to be merely tools in the hands of humans and are transforming into an environment of human existence. This fundamental change in the ontological status of technical objects necessitates a reconsideration of many established concepts, including privacy, autonomy, informed consent, and even the very structure of human rights. The World Commission on the Ethics of Scientific Knowledge and Technology of UNESCO, in its 2021 report, proposed one of the most systematic approaches to the analysis of these issues, identifying three levels of the ethical implications of

IoT, namely the individual, social, and policy levels [1, pp. 15–16]. The methodology of the present study is based on a combination of normative analysis of international documents, a comparative legal method in examining different approaches to regulation, and the analysis of specific cases that have revealed ethical dilemmas in the implementation of IoT technologies. Such an approach makes it possible not only to identify existing problems but also to propose conceptual foundations for their resolution.

The technological architecture of the Internet of Things constitutes a three-tier structure, each element of which generates specific ethical tensions. The sensing layer is responsible for data collection, where it is important to distinguish between purpose-built sensors installed with the user's knowledge and opportunistic sensors that utilise existing infrastructure to collect information not originally intended [1, pp. 19]. The network layer enables data transmission and gives rise to vulnerabilities associated with the possibility of interception and unauthorised access. The data processing layer, where artificial intelligence algorithms are deployed, generates the most complex ethical dilemmas related to autonomous decision-making and the opacity of algorithmic logic [2, pp. 2347–2376]. The combination of all three layers means that IoT devices acquire the ability not only to record but also to interpret human behaviour, as well as to influence it without the individual's explicit awareness of this impact.

Particular attention should be given to the classification of data sources proposed in the COMEST report. Researchers identify three categories of sensors, namely social sensors, physical sensors in the private domain, and physical sensors in the public domain [1, pp. 25]. Social sensors, which include data from social media, are predominantly controlled by private transnational corporations. Physical sensors in the private domain, such as smart home devices and wearable gadgets, collect information on intimate aspects of life. Physical sensors in the public domain, including street cameras and infrastructure sensors, fall within the remit of state responsibility but are often operated by private contractors. The key

issue is that a significant proportion of sensors operate in an opportunistic mode; that is, they collect data for purposes not originally declared upon installation [1, pp. 26]. This precludes the possibility of obtaining fully informed consent, as users remain unaware of which specific data are being collected about them and for what purposes.

At the individual level, the ethical challenges of the IoT are associated with a transformation of the relationship between humans and the world. When surrounding objects begin to perceive and respond to human behaviour, a fundamental shift occurs in the subject-object structure. In the Western metaphysical tradition, the active subject of cognition stands in opposition to the passive object. The IoT inverts this schema: objects themselves become subjects of cognition, generating knowledge about the individual that may be inaccessible to that individual themselves [1, pp. 27]. A risk arises whereby an active object generates a passive subject who is rendered measurable and guided 'behind their back' [1, pp. 26]. Of particular concern is the phenomenon of nudging, where a system subtly steers human behaviour towards certain decisions, whether regarding consumer choices or political preferences [3, pp. 230]. Even if such actions are performed with good intentions, they call into question the possibility of autonomous choice.

The problem of privacy in the context of the IoT acquires new dimensions that cannot be reduced to classical issues of personal data protection. First, the IoT tracks not only online behaviour but also an individual's physical presence in space; for instance, street cameras can be used for facial recognition [4]. Second, the aggregation of data from heterogeneous sources enables the creation of highly accurate personal profiles [1, pp. 34–35]. Third, machine learning algorithms are capable of inferring information about health status, personality traits, and political sympathies from diverse data sets [5, c. 28–30]. The framework of informed consent, borrowed from biomedical ethics, proves inadequate in situations where the purposes of data collection may be unknown [6, pp. 1512–1513].

The difficulty of applying traditional legal mechanisms is evidenced by the experience of the European Union, where the General Data Protection Regulation (GDPR) has been one of the first attempts at the comprehensive regulation of the digital environment [7]. However, this regulation is oriented towards the protection of personal data as a static category and fails to account for the dynamic nature of IoT systems [1, p. 36]. The concept of personal data becomes blurred, as the aggregation of anonymised data can be used for the precise identification of an individual [8, pp. 5-6]. As noted in the COMEST report, the IoT creates situations that require recourse to more fundamental categories, such as human dignity and personal autonomy [1, p. 37].

At the social level, the ethical challenges of the IoT manifest in the intensification of discrimination, the deepening of digital inequality, and the reinforcement of gender stereotypes. Algorithmic systems are prone to reproducing existing societal biases. The example of sensors in liquid soap dispensers, which respond less effectively to dark skin, illustrates how technical systems can discriminate against certain groups due to a lack of diversity in training data [9]. The problem of gender bias is more systemic: voice assistants with female voices, such as Siri and Alexa, are often programmed for submissiveness and compliance, reinforcing the stereotype of women as assistants in subordinate roles [10, pp. 45-48]. Journalist Sigal Samuel describes an experiment in which she insulted Siri, and the assistant responded submissively, failing to demonstrate any resistance [11].

Of particular concern is the use of IoT devices in the context of domestic abuse. Smart locks and cameras can be employed to monitor a partner, restrict their movement, or confine them within their own home [1, p. 42]. Researchers at University College London (UCL) analyse these risks, emphasising the need to account for potential criminal misuse at the design stage [12]. This raises an ethical dilemma regarding the manufacturer's responsibility for products that may facilitate criminal acts. A similar issue affects the elderly, who risk social

exclusion due to insufficient digital literacy [13]. As public services increasingly transition to digital formats, those lacking the necessary skills are relegated to the status of second-class citizens [1, p. 43].

The environmental dimension of the IoT represents another significant challenge. Precision agriculture technologies enable the optimisation of irrigation and fertiliser application, while smart grids reduce electricity losses [1, pp. 44-45]. Conversely, the IoT itself exacerbates the problem of electronic waste. Devices have complex chemical compositions, containing rare-earth metals with limited reserves, and are notoriously difficult to recycle [14, pp. 10861-10862]. The COMEST report on land use ethics emphasises the necessity of transitioning to a circular economy [15, pp. 32-34]. However, a significant proportion of electronic waste is disposed of in developing countries, often in violation of environmental standards [16].

At the political level, the IoT emerges as a dual-use instrument. The traditional metaphor of the panopticon describes the IoT as a technology of pervasive surveillance [17]. However, as noted in the COMEST report, this metaphor is not entirely adequate, since IoT systems do not constitute a single centralised mechanism [1, p. 48]. Instead, they form a complex network in which various actors often have conflicting interests [18, pp. 214-215]. Nonetheless, the risks of mass surveillance remain high. James Clapper, the former Director of National Intelligence in the United States, stated that intelligence services could utilise the IoT for identification and tracking [19]. Furthermore, the vulnerability of critical infrastructure to cyberattacks poses significant threats to national security.

At the same time, the IoT opens up opportunities for civic participation. The phenomenon of citizen sensing enables residents to independently measure air quality and noise levels. The "Citizen Sensing Toolkit" project empowers citizens to participate in public debates in an informed and evidence-based manner [20]. Similarly, the "Citizen Sense" project by Jennifer Gabrys examines how such

practices generate new forms of environmental awareness [21]. Realising this potential requires open standards and access to data [1, p. 52].

The regulation of the IoT represents a complex interdisciplinary challenge at the intersection of law, ethics, and technology. Traditional law-making often proves too slow to keep pace [1, p. 55]. The concept of 'ethics by design' shifts the focus towards designing systems with due regard for ethical requirements [22, pp. 906-907]. Technological solutions, such as data anonymisation by default, may prove more effective than legal sanctions [23]. Indeed, Article 25 of the GDPR mandates that manufacturers implement the principles of 'data protection by design' [7, p. 48]. However, this regulation has limited jurisdiction and fails to fully address device security and cross-border data transfers [1, p. 56]. Consequently, different countries are developing their own regulatory models that reflect specific national interests [24].

In this context, UNESCO plays a key role. The Recommendation on the Ethics of Artificial Intelligence, adopted by Member States in 2021, established principles aimed at preserving human control and ensuring the transparency of algorithmic decision-making [25]. The COMEST report further develops these principles in relation to the IoT, proposing the implementation of ethical design reviews, the development of professional standards, and the promotion of inclusivity [1, pp. 57-59].

Thus, the Internet of Things represents not merely another technological innovation but a qualitatively new human environment that necessitates a reimagining of fundamental ethical and legal categories. Traditional concepts of privacy, informed consent, and human autonomy-shaped in an era when technologies were tools rather than environments-require a substantial revision. At the individual level, the key challenges include the crisis of informed consent, threats to privacy arising from the opportunistic use of data, and the risks of behavioural manipulation. At the social level, the primary issues are the intensification of discrimination, the reinforcement of gender stereotypes, the use

of the IoT for domestic abuse, and environmental consequences. At the political level, the IoT emerges as a dual-use instrument capable of both enhancing surveillance and expanding opportunities for civic engagement through citizen sensing. A promising regulatory direction is the concept of 'ethics by design', which involves embedding ethical principles directly into technological architecture. International organisations, particularly UNESCO, play a vital role in shaping global standards for the responsible development of technology. The challenge lies in striking a balance between harnessing the potential of the IoT to improve quality of life and protecting fundamental human rights. Addressing this task requires not only legal and technological innovation but also a broad societal dialogue involving developers, regulators, businesses, and civil society.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

До розділу 1

1. Експерименти у психології: Третя хвиля Рона Джонса. URL: <https://www.psykholoh.com/post/експерименти-у-пс%25>.
2. Загадки людської психіки: Експеримент «Третя хвиля». URL: <https://revolta.com.ua/nepiznane/zagadki-lyudskoj-psi-hiki-eksperiment-tretya-khvilya.html>.
3. Пригадуючи Третю хвилю. URL: <https://commons.com.ua/uk/prigadyuyuchi-tretyu-hvilyu/>.
4. Третя хвиля. Експеримент Рона Джонса. URL: https://psyfactor.org/lib/experiment_jonsa.htm.
5. Ghani A. Manipulation, The Third Wave Experiment. URL: <https://medium.com/illumination/manipulation-the-third-wave-experiment-a43c246e08e4>.
6. Jones Ron. Third Wave. Jones Ron. No Substitute for Madness. A Teacher, His Kids & The Lessons of Real Life. Covelo, California: Island Press, 1981. 168 p.
7. Mitchell R. The Third Wave Experiment and a Lesson from History URL: <https://www.historicmysteries.com/history/third-wave-experiment/37211/>.
8. Taaffe L. The Wave that changed the world URL: <https://www.paloaltoonline.com/news/2017/03/17/the-wave-that-changed-history/>.

To chapter 2

1. UNESCO. The Ethical Implications of the Internet of Things (IoT): Report of the World Commission on the Ethics of Scientific Knowledge and Technology (COMEST). Paris : UNESCO, 2023. 68 p. DOI: <https://doi.org/10.54678/JSGE8362>.

2. Al-Fuqaha A., Guizani M., Mohammadi M., Aledhari M., Ayyash M. Internet of Things: A Survey on Enabling Technologies, Protocols, and Applications. *IEEE Communications Surveys & Tutorials*. 2015. Vol. 17, No. 4. P. 2347–2376. DOI: <https://doi.org/10.1109/COMST.2015.2444095>.
3. Henschke A. The Internet of Things and Dual Layers of Ethical Concern. *Robot Ethics 2.0: From Autonomous Cars to Artificial Intelligence* / ed. by P. Lin, R. Jenkins, K. Abney. New York : Oxford University Press, 2017. P. 229–243. DOI: <https://doi.org/10.1093/oso/9780190652951.003.0015>.
4. Doffman Z. Hong Kong Exposes Both Sides of China’s Relentless Facial Recognition Machine. *Forbes*. 2019. 26 August. URL: <https://www.forbes.com/sites/zakdoffman/2019/08/26/hong-kong-exposes-both-sides-of-chinas-relentless-facial-recognition-machine/> (дата звернення: 24.03.2026).
5. Taylor L., Floridi L., van der Sloot B. Introduction: A New Perspective on Privacy. *Group Privacy: New Challenges and Data Technologies* / ed. by L. Taylor, L. Floridi, B. van der Sloot. New York : Springer, 2017. P. 1–13. DOI: https://doi.org/10.1007/978-3-319-46608-8_1.
6. Slade S., Prinsloo P. Learning Analytics: Ethical Issues and Dilemmas. *American Behavioral Scientist*. 2013. Vol. 57, No. 10. P. 1510–1529. DOI: <https://doi.org/10.1177/0002764213479366>.
7. Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation). *Official Journal of the European Union*. 2016. L 119. P. 1–88.
8. van den Hoven J. Fact Sheet: Ethics Subgroup IoT. Version 4.01. Brussels : European Commission, 2012. 22 p. URL: <https://www.semanticscholar.org/paper/Fact-sheet-Ethics-Subgroup-IoT->

Version-4.-0-1-Hoven/2b7d3c9f5a8e4d1f6c7b9a3e5d8f2c4a6b7e9d1f (дата звернення: 24.03.2026).

9. Fussell S. Why Can't This Soap Dispenser Identify Dark Skin? Gizmodo. 2017. 17 August. URL: <https://gizmodo.com/why-cant-this-soap-dispenser-identify-dark-skin-1797931773> (дата звернення: 24.03.2026).

10. UNESCO. "I'd Blush If I Could": Closing Gender Divides in Digital Skills through Education. Paris : UNESCO, 2019. 150 p. URL: <https://unesdoc.unesco.org/ark:/48223/pf0000367416> (дата звернення: 24.03.2026).

11. Samuel S. Alexa, Are You Making Me Sexist? Vox. 2019. 12 June. URL: <https://www.vox.com/future-perfect/2019/6/12/18660353/siri-alexa-sexism-voice-assistants-un-study> (дата звернення: 24.03.2026).

12. Brown A., Harkin D., Tanczer L.M. Safeguarding the "Internet of Things" for Victim-Survivors of Domestic and Family Violence: Anticipating Exploitative Use and Encouraging Safety-by-Design. Violence Against Women. 2025. Vol. 31, No. 5. P. 1039–1062. DOI: <https://doi.org/10.1177/10778012231222486>.

13. van Deursen A.J., Helsper E.J. A Nuanced Understanding of Internet Use and Non-use among the Elderly. European Journal of Communication. 2015. Vol. 30, No. 2. P. 171–187. DOI: <https://doi.org/10.1177/0267323115578059>.

14. Zhang K., Schnoor J.L., Zeng E.Y. E-Waste Recycling: Where Does It Go from Here? Environmental Science & Technology. 2012. Vol. 46, No. 20. P. 10861–10867. DOI: <https://doi.org/10.1021/es303166s>.

15. UNESCO. Report of COMEST on Land-Use Ethics. Paris : UNESCO, 2021. 52 p. URL: <https://unesdoc.unesco.org/ark:/48223/pf0000381355> (дата звернення: 24.03.2026).

16. United Nations Environment Management Group. United Nations System-wide Response to Tackling E-waste. New York : UN, 2017. 48 p.

URL: <https://unemg.org/images/emgdocs/ewaste/E-Waste-EMG-FINAL.pdf> (дата звернення: 24.03.2026).

17. Foucault M. Surveiller et punir : Naissance de la prison. Paris : Gallimard, 1975. 328 p.

18. Sassen S. Does the City Have Speech? Public Culture. 2013. Vol. 25, No. 2. P. 209–221. DOI: <https://doi.org/10.1215/08992363-2020557>.

19. Clapper J. Statement for the Record: Worldwide Threat Assessment of the US Intelligence Community. Senate Armed Services Committee, 2016. 32 p. URL: https://www.armed-services.senate.gov/imo/media/doc/Clapper_02-09-16.pdf (дата звернення: 24.03.2026).

20. Waag Society. Making Sense: from pilots to Citizen Sensing, a Toolkit! Amsterdam : Waag Society, 2018. 36 p. URL: <https://waag.org/en/article/making-sense-pilots-citizen-sensing-toolkit> (дата звернення: 24.03.2026).

21. Gabrys J. How to Do Things with Sensors. Minneapolis : University of Minnesota Press, 2019. 106 p. DOI: <https://doi.org/10.5749/j.ctv9hj9r3>.

22. Baldini G., Botterman M., Neisse R., Tallacchini M. Ethical Design in the Internet of Things. Science and Engineering Ethics. 2018. Vol. 24, No. 3. P. 905–925. DOI: <https://doi.org/10.1007/s11948-016-9754-5>.

23. Simonite T. These Startups Are Building Tools to Keep an Eye on AI. Wired. 2019. 21 October. URL: <https://www.wired.com/story/these-startups-are-building-tools-keep-eye-ai/> (дата звернення: 24.03.2026).

24. Broadband Commission for Sustainable Development. Connecting Africa through Broadband: A Strategy for Doubling Connectivity by 2021 and Reaching Universal Access by 2030. Geneva : ITU, 2019. 48 p. URL: https://www.broadbandcommission.org/Documents/working-groups/DigitalMoonshotforAfrica_Report.pdf (дата звернення: 24.03.2026).

25. UNESCO. Recommendation on the Ethics of Artificial Intelligence. Paris : UNESCO, 2021. 48 p.

URL: <https://unesdoc.unesco.org/ark:/48223/pf0000380455> (дата звернення: 24.03.2026).

To chapter 3

1. Hutchinson T., Waters A. English for Specific Purposes: A Learning-Centred Approach. Cambridge : Cambridge University Press, 1987. 192 с.

2. Canale M., Swain M. Theoretical Bases of Communicative Approaches to Second Language Teaching and Testing. Applied Linguistics. 1980. Vol. 1, № 1. P. 1–47.

3. Гриценко Т. М. ESP-Based Sociolinguistic Exercises with AI Integration for Technical Students. Universal Teaching and Learning Journal. 2025. Vol. 1, № 3. P. 45–62. URL: <https://goodwoodpub.com/index.php/utlj/article/view/3482> (дата звернення: 21.03.2026).

4. Козлов Д., Петренко О. Enhancing ESP for STEM Students: AI Tools and Professional Communication. Tractatus. 2025. № 2. С. 17–32. URL: <https://tractatus.sumdu.edu.ua/index.php/journal/article/view/1271> (дата звернення: 21.03.2026).

5. Сидоренко І. В. Integrating Artificial Intelligence Tools into Project-Based English Language Instruction for Technical Students. Вісник Вінницького політехнічного інституту. Серія: Філософія, психологія, педагогіка. 2025. № 4. С. 78–92. URL: <http://ir.lib.vntu.edu.ua/handle/123456789/50044> (дата звернення: 21.03.2026).

6. Kozlova D., Petrenko O. AI-Enhanced Transformative Approach to ESP in Engineering Education. BCE2024 Proceedings. Tokyo : IAFOR, 2024. P. 112–125. URL: https://papers.iafor.org/wp-content/uploads/papers/bce2024/BCE2024_82559.pdf (дата звернення: 21.03.2026).

7. Alliance for Decision Education, Burning Glass Institute. Decision Skills in the Workforce: National Analysis. 2025. 45 p. URL:

<https://alliancefordecisioneducation.org/workforce-skills-report/> (дата звернення: 21.03.2026).

8. Law J. B. AI for Professional Communication : онлайн-курс. Coursera, 2026. URL: <https://www.coursera.org/learn/ai-for-professional-communication> (дата звернення: 21.03.2026).

9. UNESCO. Recommendation on the Ethics of Artificial Intelligence. Paris : UNESCO, 2021. 50 p. URL: <https://unesdoc.unesco.org/ark:/48223/pf0000381137> (дата звернення: 21.03.2026).

10. European Commission. Digital Education Action Plan (2021–2027): Reset, Progress, Challenge. Brussels : European Commission, 2025. 68 p. URL: <https://education.ec.europa.eu> (дата звернення: 21.03.2026).

11. Holmes W., Bialik M., Fadel C. Artificial Intelligence in Education: Promises and Implications for Teaching and Learning. Boston : Center for Curriculum Redesign, 2019. 128 p.

12. Godwin-Jones R. Emerging Technologies: AI and Language Learning. Language Learning & Technology. 2023. Vol. 27, № 1. P. 4–18.

До розділу 4

1. Про національну безпеку України : Закон України від 21.06.2018 № 2469-VIII. URL: <https://zakon.rada.gov.ua/laws/show/2469-19> (дата звернення: 17.03.2026).

2. Стратегія національної безпеки України : Указ Президента України від 14.09.2020 № 392/2020. URL: <https://zakon.rada.gov.ua/laws/show/392/2020> (дата звернення: 17.03.2026).

3. Про Державну прикордонну службу України : Закон України від 03.04.2003 № 661-IV. URL: <https://zakon.rada.gov.ua/laws/show/661-15> (дата звернення: 17.03.2026).

4. Про схвалення Стратегії інтегрованого управління кордонами на період до 2025 року : розпорядження Кабінету Міністрів України від

24.07.2019 № 687-р. URL: <https://zakon.rada.gov.ua/laws/show/687-2019-p> (дата звернення: 17.03.2026).

5. Матвеев О. В. Правове регулювання прикордонної діяльності у сучасній державі : дис. ... д-ра філософії. Одеса, 2023. 238 с.

6. Конституція України : Закон України від 28.06.1996 № 254к/96-ВР. URL: <https://zakon.rada.gov.ua/laws/show/254к/96-вр> (дата звернення: 17.03.2026).

7. Про основні засади забезпечення кібербезпеки України : Закон України від 05.10.2017 № 2163-VIII. URL: <https://zakon.rada.gov.ua/laws/show/2163-19> (дата звернення: 17.03.2026).

8. Купрієнко Д. А. Основні поняття та категорії у сфері забезпечення прикордонної безпеки. Збірник наукових праць Національної академії Державної прикордонної служби України. 2014. № 1. С. 357–368.

To chapter 5

1. Про охорону праці : Закон України від 14.10.1992 р. № 2694-XII. Редакція від 01.01.2024. URL: <https://zakon.rada.gov.ua/laws/show/2694-12> (дата звернення: 19.03.2026).

2. Директива Ради 89/391/ЕЕС від 12 червня 1989 року про введення заходів для заохочення поліпшень у сфері безпеки та здоров'я працівників на роботі. Офіційний журнал Європейських Співтовариств. L 183. 29.06.1989. С. 1–8. URL: <https://www.google.com/search?q=https://eur-lex.europa.eu/legal-content/EN/TXT/%3Furi%3DCELEX:31989L0391> (дата звернення: 19.03.2026).

3. Основні шляхи реформування системи управління охороною праці в Україні - Головне управління Пенсійного фонду України в Луганській області. Головне управління Пенсійного фонду України в Луганській області. URL: <https://www.pfu.gov.ua/lg/367864-osnovni-shlyahy->

reformuvannya-systemy-upravlinnya-ohoronoyu-pratsi-v-ukrayini/ (дата звернення: 21.03.2026).

4. European Agency for Safety & Health at Work - Information, statistics, legislation and risk assessment tools. European Agency for Safety & Health at Work - Information, statistics, legislation and risk assessment tools. URL: <https://osha.europa.eu/en> (date of access: 20.03.2026).

5. ДСТУ EN ISO 45001:2019 (ISO 45001:2018, IDT). Системи управління охороною здоров'я та безпекою праці. Вимоги та настанови щодо застосування. – Київ: ДП «УкрНДНЦ», 2019.-42 с.

6. ДСТУ EN ISO 12100:2016 (EN ISO 12100:2010, IDT). Безпечність машин. Загальні принципи проєктування. Оцінювання ризиків та зменшення ризиків. Київ : ДП «УкрНДНЦ», 2016.

7. Про затвердження критеріїв, за якими оцінюється ступінь ризику від провадження господарської діяльності та визначається періодичність проведення планових заходів державного нагляду (контролю) у сфері охорони праці : Постанова Кабінету Міністрів України від 06.03.2019 р. № 223. URL: <https://zakon.rada.gov.ua/laws/show/223-2019-%D0%BF> (дата звернення: 19.03.2026).

8. Berezutskyi V. V., Samborskyi I. A. WORKPLACE SAFETY CULTURE AND RISKS OF INJURY. Labour protection problems in Ukraine. 2024. Vol. 40, no. 3-4. P. 32–41. URL: <https://doi.org/10.36804/nndipbop.40-3-4.2024.32-41> (date of access: 21.03.2026).

До розділу 6

1. Dalpiaz F., Ferrari A., Franch X. Requirements Engineering: A Roadmap. arxiv, 2022. URL: <https://arxiv.org/abs/2201.10498>

2. Nguyen D., Cruz I. Cybersecurity Requirements Engineering: A Systematic Mapping Study. IEEE Access. 2022.

3. Penzenstadler B. Sustainability in Software Engineering: Advances and Future Directions. arxiv, 2022. URL: <https://arxiv.org/abs/2206.04612>
4. OpenAI. GPT-4 Technical Report. 2023. URL: <https://arxiv.org/abs/2303.08774>
5. Ferrari A., Spagnolo G. Natural Language Processing for Requirements Engineering: Recent Trends. Requirements Engineering Journal. 2023.
6. Bommasani R. et al. On the Opportunities and Risks of Foundation Models. arxiv, 2022. URL: <https://arxiv.org/abs/2108.07258>

To chapter 7

1. Pinchuk O., Prokopenko A. Actual Areas of Development of Digital Competence of Officers of the Armed Forces of Ukraine. ICTERI 2021 Proceedings. 2021. P. 89–108. URL: https://lib.iitta.gov.ua/id/eprint/728788/1/paper_129.pdf
2. Прокопенко А. М., Пінчук О. О. Development of Digital Competence of Military Leaders in the Professional Development System. Educational Dimension. 2024. № 6. С. 112–125.
3. Нагачевський В. Я., Семів Г. О. Forming Foreign Language Communicative Competence of Future Ukrainian Armed Forces Officers by Means of ICT. Online Defense. 2024. Vol. 45, № 2. P. 78–92.
4. Professional Military Education Modernization and CGSC Transformation. Small Wars Journal. 2025. URL: <https://smallwarsjournal.com/2025/10/29/pme-modernization-cgsc-transformation/> (дата звернення: 21.03.2026).
5. Nahachevskiy V. Yo., Semiv G. O. Information and Communication Technologies in the Formation of Professional Competence of Cadets of Ukrainian Military Higher Educational Institutions during Wartime. Prospects and Innovations of Science. Series Pedagogy. 2025. No. 10(56). P. 74–87.
6. Professional Military Education Modernization and CGSC Transformation. Small Wars Journal. 2025.

7. NATO StratCom COE. Digital Competence Framework for Military Professionals. Riga : NATO StratCom COE, 2024. 72 с.
8. NATO. Allied and Joint Approaches to Digital Transformation and Multi-Domain Operations. 2022–2024.
9. U.S. Army. Army Learning Concept for 2030–2040. Washington : TRADOC, 2023. 45 с.
10. NATO. Interoperability, Strategic Communication, and Military Professional Development Documents. Brussels : NATO, 2024.
11. European Commission. Digital Competence Framework for Citizens (DigComp 2.2). Brussels : EC, 2022. URL: https://joint-research-centre.ec.europa.eu/digcomp_en (дата звернення: 21.03.2026)
12. Бахмат Н. В. Цифрова трансформація військової освіти України. Військова освіта. 2025. № 1. С. 5–20.
13. Rodikov V. Interdisciplinary Professional Training of Military Specialists. Advances in Military Education. 2025. Vol. 3, No. 1. P. 23–38.

To chapter 8

1. Ouyang Z. et al. Self-regulated learning and engagement as serial mediators between AI-driven adaptive learning platform characteristics and educational quality. *Frontiers in Psychology*. 2025. Vol. 16. Article 1646469. DOI: 10.3389/fpsyg.2025.1646469.
2. Liu G. L. A scoping review of AI-mediated informal language learning: Mapping out the territory. *ReCALL*. 2026. Vol. 38, № 1. P. 1–25.
3. Järvelä S., Hadwin A. F. Self-regulation and shared regulation in collaborative learning in adaptive digital learning environments. *British Journal of Educational Technology*. 2024. Vol. 55, № 5. P. 1892–1915.
4. Huang Y. et al. L2 growth mindset in AI-mediated language learning: The mediating roles of emotional intelligence and willingness to

communicate. *Frontiers in Psychology*. 2025. Vol. 16. Article 1700117. DOI: 10.3389/fpsyg.2025.1700117.

5. Dovhaniuk E. Multimodal and cognitive approaches to academic discourse in AI-integrated learning environments. *Cognition, Communication, Discourse*. 2025. № 24. P. 15–32.

6. Winne P. H., Hadwin A. F. Studying as self-regulated learning. *Metacognition in Educational Theory and Practice* / ed. by D. J. Hacker, J. Dunlosky, A. C. Graesser. Mahwah : Lawrence Erlbaum Associates, 1998. P. 277–304.

To chapter 9

1. Бахмат Н. В. Штучний інтелект у вищій освіті: можливості, виклики, перспективи. *Педагогічні науки: теорія, історія, інноваційні технології*. 2023. № 3. С. 12–25.

2. Алексеєва Г. М. Етичні та освітні виклики штучного інтелекту у вищій освіті України. Науково-дослідна робота в системі підготовки фахівців-педагогів : матер. X Всеукр. наук.-практ. конф. Запоріжжя : БДПУ, 2025. С. 9–12.

3. Козлов Д. А. Використання штучного інтелекту у вищій освіті: стан і перспективи. *International Scientific Journal of Elementary and Secondary Education*. 2024. № 1. С. 45–58.

4. Holmes W., Bialik M., Fadel C. *Artificial Intelligence in Education: Promises and Implications for Teaching and Learning*. Boston : Center for Curriculum Redesign, 2019. 128 p.

5. UNESCO. *Recommendation on the Ethics of Artificial Intelligence*. Paris : UNESCO, 2021. 50 p. URL: <https://unesdoc.unesco.org/ark:/48223/pf0000381137>

6. European Network for Academic Integrity. *Guidelines on Ethical Use of AI in Education*. 2025.

7. Shaw A. et al. Student Willingness to Use Generative AI Despite Policy Prohibitions. *Journal of Academic Ethics*. 2023. Vol. 21, No. 4. P. 567–589.

8. Godwin-Jones R. Emerging Technologies: AI and Language Learning. *Language Learning & Technology*. 2023. Vol. 27, No. 1. P. 4–18.

9. Akgun S., Greenhow C. Artificial Intelligence in Education: Addressing Ethical Challenges in K-12 Settings. *AI and Ethics*. 2022. Vol. 2, No. 3. P. 431–440.

10. Hutchinson T., Waters A. *English for Specific Purposes: A Learning-Centred Approach*. Cambridge : Cambridge University Press, 1987. 192 p.

11. Canale M., Swain M. Theoretical Bases of Communicative Approaches to Second Language Teaching and Testing. *Applied Linguistics*. 1980. Vol. 1, No. 1. P. 1–47.

12. European Commission. *Digital Education Action Plan (2021–2027): Reset, Progress, Challenge*. Brussels : European Commission, 2025.

До розділу 10

1. Акмеологія: методологічні принципи і підходи [Електронний ресурс]. Освіта.ua. Режим доступу: <https://osvita.ua/vnz/reports/sociology/29809/>.

2. Боднар А. Л. Самореалізація творчого потенціалу людини в акмеології: науково-методологічні орієнтації. Київ, 2017. 180 с.

3. Войнікова А., Бетехтін О. Акмеологічний підхід у професійному розвитку майбутніх керівників освітніх закладів. *Педагогічний журнал*. 2025. № 1–2. С. 45–52.

4. Дубасенюк О. А. Методологія впровадження акмеологічного підходу у професійній підготовці педагога. Текст електронного ресурсу. Запорізький нац. ун-т, 2024. Режим доступу: <http://eprints.zu.edu.ua/>

5. Огнев'юк В. О. Сучасні акмеологічні дослідження: теоретико-методологічні та прикладні аспекти / В. О. Огнев'юк, С. О. Сисоєва, Я. С. Фруктова (ред.). Київ : Київський ун-т ім. Б. Грінченка, 2016. 200 с.
6. Паламарюк В. А. Формування акмеологічної компетентності педагога: теоретико-методологічні підходи. Одеса, 2025. 210 с.
7. Саяпіна С. А. Акмеологічні технології: методичні вказівки. Дніпро : ДДПУ, 2020. 32 с.
8. Саяпіна С. А. Акмеологічні технології: три методологічні орієнтації сучасного знання (природничо-наукова, гуманітарна, технологічна). Дніпро, 2021. 120 с.
9. Сучасні акмеологічні дослідження: теоретико-методологічні та прикладні аспекти : зб. наук. пр. / [ред. кол. В. О. Огнев'юк та ін.]. Київ : Київський ун-т ім. Б. Грінченка, 2016–2025. Серія: Акмеологія. Вип. 1–10.

Vydavatel:

Publishing house Education and Science s.r.o. IČO : 271 56 877.
Frýdlanská 15/1314 , Praha 8. MS v Praze , oddíl C, vložka 100614

**Cross-Disciplinary Studies in
Science, Innovation and Social
Development**

Volume VIII

Signed for printing on March 28, 2026.
Format 60x90/8. Headset Times New Roman.
Mental printing. arc. 5,04. Edition online.