PROCEEDINGS OF THE INTERNATIONAL INTERNSHIP AND CONFERENCE PROGRAMME

ESS CONFERENCE SERIES

SOCIAL SCIENCE AND HUMANITIES

01

VOLUME 1
ISSUE 1
2026

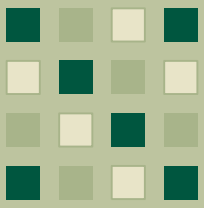
ESS Conference Series

Social Science and Humanities

Law, Digital Technologies and Sustainable Governance

13–22 JUNE 2026

VARNA, BULGARIA



VOLUME 1 / ISSUE 1 / 2026

DOI: 10.54658/esscssh.2026.1.1

ISSN:

ESS Press

EDITORIAL BOARD

OPEN ACCESS

Publisher:
ESS PRESS

info@ess.press

PUBLISHER'S NOTE:

The opinions expressed in the published articles are the sole responsibility of the authors and do not reflect the opinion of the editors or members of the editorial board.

CONTENTS

INTEGRATING ARTIFICIAL INTELLIGENCE INTO PARLIAMENTARY RESEARCH SERVICES: THE RESEARCH SERVICE OF THE VERKHOVNA RADA OF UKRAINE AS A CASE STUDY 8
Lesia Vaolevska; Ivan Myshchak

HUMAN DIGNITY AND THE LEGITIMACY OF PUBLIC AUTHORITY IN THE DIGITAL TRANSFORMATION OF THE STATE: A TWO-AXIS GOVERNANCE TEST FOR AUTOMATED ADMINISTRATION 29
Svitlana Bobrovnyk; Anatolii Shevchenko; Olha Varych

PROTECTION OF HUMAN RIGHTS BY THE NOTARIAT UNDER MARTIAL LAW: DIGITAL RESILIENCE, LEGAL CERTAINTY AND DIRECTIONS FOR REFORM 41
Anatolii Shevchenko; Myroslav Hryhorchuk; Ivanna Markelova

CLASSIFICATION OF NON-GOVERNMENTAL ORGANISATIONS IN MODERN LEGAL SCHOLARSHIP:
TOWARDS A MULTIDIMENSIONAL MODEL FOR DIGITAL GOVERNANCE 52
Danylo S. Perepolkin; Serhii M. Perepolkin

CYBERSECURITY AND PRIVACY RISKS OF AI ASSISTANTS IN ACADEMIC INSTITUTIONS: A RISK CLASSIFICATION AND GOVERNANCE FRAMEWORK 64
Oleksandr Muliarevych

PEDAGOGICAL FRAMEWORK FOR TRAINING SOCIAL WORKERS AS MEDIATORS IN CIVIL PROCEEDINGS:
A TRAUMA-INFORMED AND DIGITALLY RESPONSIBLE APPROACH 88
Kateryna Dmytrenko

DIGITAL TECHNOLOGIES IN THE FORMATION OF COMMUNICATIVE AND METHODOLOGICAL COMPETENCE OF FUTURE VOCAL TEACHERS:
A CONCEPTUAL FRAMEWORK FOR HIGHER ART EDUCATION 102
Yaroslav M. Yotka

CONTENTS

GREENING TOOLS IN TRANSPORT AND LOGISTICS OPERATIONS:
A POLICY-INSTRUMENT CLASSIFICATION AND GOVERNANCE ASSESSMENT 115
Maryna V. Halkevych; Tetiana A. Voichenko; Tetiana K. Metil

ARCHITECTURAL IMAGERY IN CHILDREN'S BOOKS CIRCULATING IN KAZAKHSTAN: CULTURAL MEMORY, PLACE IDENTITY, AND IMPLICATIONS FOR
CULTURAL SUSTAINABILITY 129
Nazerke Zhambylkyzy Toktassynova

THE UNREGULATED MIDDLE: GENERATIVE AI IN FOREIGN LANGUAGE TEACHER EDUCATION BETWEEN THE EU AI ACT AND UKRAINIAN LAW 141
Raisa Gladushyna

PUBLIC GOVERNANCE OF CYBERSECURITY IN HIGHER EDUCATION INSTITUTIONS: LEGAL AND INSTITUTIONAL FOUNDATIONS FOR SUSTAINABLE DIGITAL TRANSFORMATION IN UKRAINE 154
Herasym Dei

FOREWORD

The international internship and conference programme “Law, Digital Technologies and Sustainable Governance” is an interdisciplinary educational initiative aimed at deepening theoretical knowledge and practical understanding of the interaction between law, digital technologies and sustainable governance in accordance with European standards.

Digital transformation is changing the way public institutions exercise their authority, the way justice is administered, and the way universities prepare future professionals. These processes raise questions that no single discipline can answer alone: how to keep the human being at the centre of automated administration, how to protect rights and data in digital environments, and how to make innovation compatible with sustainable development. The programme in Varna created a platform for cross-sectoral dialogue, academic exchange and the development of partnerships between education, science, the state and civil society around precisely these questions.

The articles collected in this issue reflect the thematic breadth of the programme: from artificial intelligence in parliamentary work and the dignity of the person in the digital state, to the resilience of legal institutions under martial law, the governance of green transitions, and the digital transformation of education and culture.

We would like to thank the organizers, partners, speakers and all participants for their contribution to the development of a European culture of governance and for the practical steps they take to strengthen institutional reforms.

Adrian-Gabriel Corpădean
Babeș-Bolyai University, Cluj-Napoca, Romania

ABOUT THE CONFERENCE PROGRAMME

The international programme “Law, Digital Technologies and Sustainable Governance” was held in Varna, Bulgaria, on 13–22 June 2026, hosted by Varna Free University. The full programme ran from 22 March to 22 June 2026 and combined academic lectures, expert discussions, trainings and conference sessions focused on the legal, educational and governance dimensions of digital transformation.

KEY THEMATIC AREAS

The programme addressed, in particular: legal and ethical aspects of digitalisation; pedagogical and educational aspects of digital transformation; digital justice, e-court systems and artificial intelligence in judicial proceedings; risk management under conditions of instability; management and project governance; data protection and information security; open science, academic integrity and EU standards; innovative technologies and the digital transformation of organisations; and sustainable development, economics and ecology.

ORGANISERS

Centre SIPD, Kyiv, Ukraine
E-Science Space, Warsaw, Poland
ESS Press, Warsaw, Poland
Varna Free University, Varna, Bulgaria (host institution)

Vaolevska, L., & Myshchak, I. (2026). Integrating artificial intelligence into parliamentary research services: The Research Service of the Verkhovna Rada of Ukraine as a case study. ESS Conference Series Social Science and Humanities, 1(1). https://doi.org/10.54658/esscssh.2026.1.1.01

Integrating Artificial Intelligence Into Parliamentary Research Services: The Research Service Of The Verkhovna Rada Of Ukraine As A Case Study

Lesia Vaolevska
Research Service of the Verkhovna Rada of Ukraine
Kyiv, Ukraine
ORCID 0000-0002-3659-3851
lesia.vaolevska@ukr.net

Ivan Myshchak
Research Service of the Verkhovna Rada of Ukraine
Kyiv, Ukraine
ORCID 0000-0002-4466-9836
myshchak@ukr.net

Abstract.

This article examines how artificial intelligence (AI) can be incorporated into parliamentary research services while preserving professional responsibility, information security and democratic accountability. Using the Research Service of the Verkhovna Rada of Ukraine as the principal case, the study combines doctrinal and documentary analysis with a structured comparison of recent parliamentary practices in Germany, Canada, Switzerland, Spain, Indonesia and Bahrain. The comparative framework is derived from the Inter-Parliamentary Union (IPU) Guidelines for AI in Parliaments and the Maturity Framework for AI in Parliaments and focuses on governance, technical capability, organisational capability and democratic impact. The analysis shows that effective parliamentary AI adoption depends less on the acquisition of individual tools than on institutional rules, reliable data, human oversight, staff competence, controlled experimentation and auditable workflows. The Ukrainian case demonstrates an emerging governance model in which external AI systems are treated as auxiliary instruments for processing publicly available information, while professional verification, confidentiality requirements and restrictions on autonomous action remain central. Four vectors of incorporation are identified: internal regulation of AI use; development and dissemination of institutional guidance; comparative research on AI regulation and applications; and AI-literacy training for parliamentarians, advisers and parliamentary staff. The article concludes that sustainable AI adoption in parliamentary research services requires a staged, risk-based and human-centred approach in which technological efficiency remains subordinate to analytical integrity, parliamentary autonomy and public trust.

Keywords: *parliamentary research service; artificial intelligence; parliamentary administration; AI governance; digital parliament; human oversight*

1. Introduction

Over the past two decades, the concept of the e-parliament has expanded from websites, digital document flows and online broadcasting to data-driven and AI-assisted systems. The current phase of transformation is qualitatively different because generative AI and other machine-learning tools can support search, summarisation, classification, translation and

comparative analysis across large volumes of parliamentary information. For legislatures, however, the relevant question is not whether such tools are technically available, but under what institutional conditions they can be used without weakening confidentiality, professional judgement, accountability or trust in parliamentary work (United Nations et al., 2008; Inter-Parliamentary Union, 2024).

Ukraine is developing this agenda under the simultaneous pressures of war, European integration and rapid public-sector digitalisation. The national Strategy for the Digital Development of Innovation Activities up to 2030 prioritises the use of technology in governance, while the draft Artificial Intelligence Development Strategy up to 2030 places responsible and risk-managed AI adoption among the components of state modernisation. Within the Verkhovna Rada of Ukraine, these developments form part of the broader evolution of e-parliamentarism and of the institutional capacity needed to support legislative work.

Parliamentary research services occupy a particularly sensitive position in this transformation. Their outputs may inform legislative choices, comparative-law assessments, committee work and policy debates; consequently, speed gains from AI cannot be evaluated independently of source reliability, legal accuracy, data protection and professional accountability. The Research Service of the Verkhovna Rada of Ukraine therefore provides a useful case for examining AI not merely as an information technology, but as an object of institutional governance within a democratic legislature.

It is worth emphasising that AI incorporation into the Research Service's activities has not been the subject of any specific academic study. At the same time, certain aspects of this topic have been examined by academics. For instance, the authors have highlighted the information technology use in the preparation of the Research Service's proposals for the Verkhovna Rada of Ukraine's legislative work plan and in planning the parliament's legislative activities as a whole (Vaolevska, L. A. & Myshchak, I. M., 2025). However, even today, the argument that there are few academic studies examining AI implementation in the work of parliaments and parliamentary services (Koryzis, D., 2021) remains relevant.

It is worth mentioning studies, having briefly examined the potential for using AI to provide scientific and expert support for parliaments work. The article by Leston-Bandeira, C., a methodological approach is proposed for studying the impact and role of information and communication technologies (hereinafter 'ICT') on the parliamentary functions performance (Leston-Bandeira, C., 2007). Given that AI is the most advanced ICT tool, the questions raised in this study are, in our view, relevant and topical. The questions concerned the impact of new technological tools on various aspects of the parliamentary institution functioning: have there been changes in parliamentary practices; has the image of parliament improved; have new opportunities arisen for improving interaction and communication between parliamentarians and citizens? If we were to combine all these questions into one and summarise it concisely, it would sound like this: are new technological tools beneficial to the work of parliament?

An interesting perspective on the AI usage significance in parliament is its interpretation as a means of creating added value, with two corresponding levels being identified (Ziouvelou, X., 2022). The first refers to facilitating the parliamentary functions performance, whilst the second one refers to providing assistance to parliamentarians and parliamentary staff.

Researchers Ziouvelou, X., Giannakopoulos, G. and Giannakopoulos, V. emphasise the need for AI to possess certain essential characteristics, such as reliability—ensured by legality, ethical standards and technological resilience—and compliance with the recommendations of leading international experts.

Of particular interest are publications the authors of which systematically analyse the areas of AI application in parliament and develop specific proposals. For example, Lucke, J., Etscheid, J. and Fitsilis, F., with the involvement of experts and representatives of the Greek Parliament, analysed the relevance and priority of over 210 relevant areas and identified the top four which, in our view, directly concern the Parliament's research service (Lucke, J., 2022). In addition, 36 proposals have been put forward on AI use to improve the legislative process.

Based on the results of expert brainstorming sessions and surveys of the Greek Parliament members and staff, the following have been identified as the most important areas of AI application:

- intelligent examination of draft legislation to determine the impact of proposed changes on existing legislation;
- the conversion of the texts of legislative acts into machine-readable code;
- the implementation of the 'smart law' concept through the processing and interpretation of legal texts, as well as the identification of the consequences of their application using AI technologies;
- ensuring the legislative process transparency in parliament (Lucke, J., Etscheid, J., Fitsilis, F. 2022). The thesis/ assertion regarding the potential impact of implementing the 'smart law'concept on accelerating legal research within the framework of parliamentary research services is certainly worthy of particular study and discussion.

Hungarian researchers Szentgáli-Tóth, B. A. & Berkes, R. have demonstrated the importance of clear legal regulation governing AI integration into the day-to-day work of parliaments (Szentgáli-Tóth, B. A., Berkes, R., 2025). In our opinion, the article presents relevant arguments regarding the close link between parliamentary activity and national sovereignty and democratic processes, the special role of parliaments as key constitutional actors, the rapid spread of AI technology use in parliaments, and the lack of clear regulation of such activities. The authors put forward two alternative proposals to address the problem they have identified. These involve the drafting of an EU legal act to integrate AI into parliamentary activities, which would meet the criteria for preserving national sovereignty and parliamentary autonomy, whilst also promoting technological innovation within European Union institutions. Another option is to amend the EU Regulation on Artificial Intelligence (EU AI Act) to ensure that parliamentary applications based on AI technologies are classified as high-risk AI. According to Szentgáli-Tóth, B. A. & Berkes, R., this would establish stricter requirements for AI use in parliament.

According to Gonzalo, M. Á., Director of the Department of Documentation, Library and Archives of the Lower House of the Spanish Parliament, in his presentation at the international conference of the Libraries and Research Services for Parliaments Section of the International Federation of Library Associations and Institutions (IFLAPARL), AI is a tool, providing research service staff with access to in-depth analysis and research (Gonzalo, M. Á., 2024).

He believes that annotated bibliographies and comparative legal studies generated by AI not only help researchers to speed up national legislation analysis in various countries, but also contribute to improving the legislative process quality by providing accurate data in real time. At the same time, the expert emphasises the need for the responsible use of these cutting-edge technologies, for which the relevant ethical and legal frameworks must be refined. In our view, there is unlikely to be a linear, direct link between AI use and processes optimisation and qualitative improvement, as noted by Gonzalo, M. Á. It is people who are the decisive factor in bringing about these changes, as they are capable, in particular, of identifying and correcting AI hallucinations.

The rapid development of methods and approaches to AI technologies use in the parliamentary services work is illustrated by the article by Cifuentes-Silva, F., Astudillo, H., and Labra Gayo, J., which examines relevant practices using the example of the Chilean Parliamentary Library (Cifuentes-Silva, F., 2025). In our opinion, the use of Semantic Web technologies (What is the Semantic Web and Semantic Technology, 2026) for the publication of legislative acts and the presentation of information on the history of legislation is worth studying, analysing and considering in terms of possible ways of adopting them. However, AI use to predict the prospects of a bill being passed, taking into account the current political context, should probably be regarded as an experiment at this stage.

Against the background of global competition amongst states for leadership in the AI field, and in the absence of a unified conceptual approach to the legal regulation of its development and use, publications emphasising the need to anticipate the negative consequences of introducing AI into parliamentary activities and to minimise them deserve particular attention (Lucke, J., 2022).

Existing scholarship has examined digital parliaments, AI-supported legislation and individual AI applications in legislative institutions, but parliamentary research units remain under-analysed as a distinct organisational setting. This matters because research services combine legal and policy analysis, access to parliamentary information, comparative research and direct support for decision-makers. The resulting research gap is therefore institutional: there is limited comparative analysis of how AI governance principles are translated into day-to-day rules, workflows and professional safeguards within parliamentary research services.

Accordingly, the article asks two questions: (1) which governance and organisational conditions are associated with responsible AI incorporation into parliamentary research services; and (2) how does the emerging practice of the Research Service of the Verkhovna Rada of Ukraine compare with recent international parliamentary experience? The objective is to identify transferable governance principles rather than to rank national parliaments by technological maturity.

2. Materials And Methods

The study uses a qualitative comparative case-study design combining doctrinal analysis, document analysis and structured institutional comparison. The primary normative framework consists of the IPU Guidelines for AI in Parliaments (2024) and the IPU Maturity Framework for AI in Parliaments (2025). These instruments were selected because they

are parliament-specific and jointly provide an analytical structure covering governance, technical capability, organisational capability and democratic impact. The Ukrainian case is examined through publicly available documents of the Research Service, including its 2026 Regulation on the Implementation of Artificial Intelligence Technologies and its methodological recommendations on AI-assisted analytical and comparative-law work.

Germany, Canada, Switzerland, Spain, Indonesia and Bahrain were selected as comparative cases because recent 2025–2026 public documentation describes concrete parliamentary AI initiatives and because the cases represent different implementation pathways: centralised use-case management, staff-centred institutional adoption, AI-assisted parliamentary libraries, maturity assessment, phased data-and-AI infrastructure development, and formal AI-management certification. The comparison is purposive rather than statistically representative. Evidence was coded against the four IPU dimensions and used to identify recurring governance patterns and transferable practices. Claims about effectiveness are therefore qualitative and documentary; the study does not measure productivity gains, causal effects or user outcomes experimentally.

The analysis also distinguishes between evidence about the internal operation of the Research Service and the Service's external analytical outputs on AI regulation in other sectors. This distinction is necessary to avoid treating the subject matter of a parliamentary research product as evidence that the same technology is already deployed institutionally within the Research Service.

3. Results

AI implementation in the Research Service's activities is governed by the Regulations, setting out principles and ethical standards for external AI systems use; the methodology for their selection, adaptation and operational use; the provision of professional development for staff in the AI field; the management of legal risks and information security procedures; functional limits, prohibitions and responsibilities when working with AI technologies (Regulation on the Implementation of Artificial Intelligence, 2026). The management and staff of the Research Service regard AI as a means of speeding up the preparation of materials and improving the educational process. At the same time, all materials produced by the Research Service must be original in nature and reflect the professional approach of its staff, which forms the basis for the legitimacy of its activities. With this in mind, these Regulations stipulate that staff may use AI in their work exclusively as an auxiliary tool for processing publicly available information only.

The responsible approach taken by the drafters of the Regulations on the Proper Use of AI for Research and Information-Analytical Support of the Activities of the Verkhovna Rada of Ukraine was demonstrated, in particular, in the establishment of categorical prohibitions for Research Service staff, aimed at safeguarding the parliament's information sovereignty, preventing the Research Service discrediting, ensuring the parliamentary activities confidentiality and protecting personal data. These prohibitions include: breaching data security and confidentiality protocols; delegating exclusive intellectual functions and authorial powers; breaching the rules on fact-checking; seeking final advice and automating decisions

with legally significant consequences; breaching ethical standards and principles of impartiality; using AI systems that lack a transparent policy regarding the non-use of user data for training their models; grant autonomous AI agents the right to make changes to official databases or register documents without prior approval of each action by a staff member; use desktop computers when working with AI; use work email accounts to register for the use of various AI tools and services (Regulation on the Implementation of Artificial Intelligence, 2026).

Based on the analysis of specialist academic literature and a review of their own experience in AI use, the Research Service staff have drawn up recommendations regarding a procedure for applying AI technologies to produce a structured, summarised document (Recommendations of the Research Service of the Verkhovna Rada of Ukraine, 2026, No 7). It is suggested that the relevant measures be implemented in three stages:

- selecting a specialised tool based on the type of an analytical task;
- creating a query using a professional profile and a multi-level structure;
- carrying out expert verification and analytical filtering (Verify & Refine).

Each of these stages is described in detail; for example, a list of relevant specialised tools is provided; it is recommended to structure tasks for AI using specific questions, to set strict requirements regarding the format and style of the final document, to carry out atomisation and a 'factual audit', to cross-reference against official primary sources, and to counteract the model's 'compliant' behaviour (Sycophancy).

It is worth noting that the Research Service's recommendations contain fundamental caveats regarding collaboration with AI: analysts must carry out professional fact-checking of documents prepared by AI via official portals, as well as carefully review their content and provide their own professional judgement and legal assessment of the document. In our opinion, the value of these recommendations lies in their universality, as the proposed procedure is relevant not only to the preparation of parliamentary analytical materials but also to any materials of analytical nature.

It is also worth noting the recommendations on the appropriate use of AI technologies for conducting comparative legal research (Recommendations from the Research Service of the Verkhovna Rada of Ukraine, 2026, No 5), prepared by the Research Service staff, drawing on their own experience and that of European Union institutions. In our opinion, a key piece of advice is that experts should bear in mind the lack of direct online access to legislation databases containing the original documents in most standard LLM models. Consequently, AI systems may utilise outdated data and news articles from the internet. The proposed methods for verifying the legal accuracy of legal terminology translation are of particular relevance to academics and experts. These include parallel translation, which involves cross-checking the translation output using several translation systems; back-translation, for example from Spanish to English and then from English to Spanish, to verify that the original meaning of the term has been preserved; checking legal terms using legal dictionaries or encyclopaedias, official translations of legislative acts or international agreements; and verifying the interpretation of a legal provision by searching for similar provisions in the legislation of different countries.

In addition, the Research Service staff are studying international experience of AI moder-

nisation. As at 30 June 2026, the institution catalogue of analytical and information materials contained 14 items of information and analytical material (hereinafter referred to as 'Research Service materials'), which examined various aspects of AI legal regulation and use (Catalogue of Analytical and Information Materials of the Research Service of the Verkhovna Rada of Ukraine, 2026), the vast majority of which were drafted between 2025 and 2026. In quantitative terms, it is worth noting the analysis of the experience of nearly 50 countries and the European Union, the results of the study of whose legislation are set out in the aforementioned materials. Most frequently, the research subject was the experience of the EU and its 27 Member States, as well as the USA. Considerable attention was paid to South Korea, Singapore, India and China.

14 The overall value of the relevant materials stems from their examination of the legislation of countries in different geographical regions, which have varying levels of economic—and, in particular, technological—development, different legal traditions and cultures, and adopt different approaches to AI regulation. It is worth emphasising that comparative law materials predominate, given that the focus of enquiries from Ukrainian MPs is specifically on studying foreign experience; this is due to Ukraine being at the initial stage of introducing AI legal regulation and seeking the most appropriate and optimal conceptual approaches. Among the key qualitative characteristics of the Research Service's materials is an emphasis on both the positive and negative aspects of AI widespread use, as well as recommendations on preventing potential negative consequences through the introduction of appropriate legal regulation of this sphere of social relations.

AI materials examination prepared by the Research Service provides grounds for categorising them into four groups based on the research subject: AI is considered in the context of analysing a specific sphere of social relations as one of the tools for its modernisation; the legal regulation of AI technologies used in a specific sphere is analysed directly; the legal regulation of the development and general use of AI is examined; and AI organisational and institutional framework is considered.

In our opinion, based on the analysis of many national parliaments websites, the AI tools most frequently implemented to enhance the transparency and user-friendliness of parliamentary websites would be useful for modernising the website of the Verkhovna Rada of Ukraine. These include the automation of live streams of parliamentary sessions and parliamentary committee meetings, the use of transcription and translation tools, as well as improvements to the document search function. (Information reference on the peculiarities of the functioning of parliamentary websites: structure, content, methods of efficiency assessment, 2025).

Following the analysis of international and national experience in the judicial process digitalisation as well as in safeguarding the independence of judges and the judicial system, recommendations have been formulated regarding the advisability of enshrining, in accordance with the codes of procedure, the possibility of administering justice remotely in the event of state of war or state of emergency (Informational Reference on Current Trends in the Development and the State of Ensuring the Independence of Judges and the Judicial System in Ukraine (2024–2025), 2026). This refers to court hearings held outside the court premises, when participants use their own technical equipment and undergo mandatory

electronic identification in order to take part in such hearings.

The argument regarding the need to foster a new judicial culture—one based, in particular, on the ethical transparency of AI algorithms and adherence to the principle of 'human oversight'—is highly relevant. One of the challenges posed by the rapid digitalisation pace of the justice system in Ukraine is countering 'profiling of judges' and automated decision-making without human oversight, which necessitates strict adherence to the principles of the European Ethical Charter on the use of artificial intelligence in judicial systems and their environment in the technological modernisation of the justice system.

In our opinion, the findings of the study into the role of AI in the creation of new branches of the DPRK's Armed Forces are relevant to the legislative process of establishing specialised cyber forces in Ukraine (Parliamentary research on the institutional establishment and assessment of the capabilities of the DPRK's cyber forces, 2025). A factor contributing to the alarmingly rapid expansion of this state's military cyber capabilities has been identified as the increased use of AI technologies by the North Korean military and hackers in recent years. Cyberattacks on military and financial organisations, as well as critical infrastructure, are becoming more frequent and sophisticated. AI helps hackers conceal their poor command of foreign languages or lack of communication skills, enabling them to build long-term relationships with potential victims without arousing their suspicion. Moreover, North Korean military and hackers use AI to create more effective viruses and ransomware, as well as to gain employment within public and private financial institutions, cryptocurrency exchanges, the defence sector and other strategic industries by submitting documents containing AI-edited photographs.

The study subject is the legal regulation of AI itself, as used, for example, in the justice system, the media, robotics, urban infrastructure management and sports (Information note on the use of artificial intelligence in the media:potential and risks, 2025; Parliamentary research on the legislative trends in the implementation of artificial intelligence tools in the field of justice in the European Union, 2025; Analytical note on comparative legislation regarding regulatory and legal regulation of the field of robotics and robotisation, 2025; Analytical note (comparative legislation) on the implementation of the Smart City concept in the European Union, USA, Canada and South Korea, 2024).

To help mitigate the potential risks associated with AI use in the judicial system—relating to security, protection and fundamental human rights—and create the conditions for the development and use of reliable AI within Ukraine's judicial system and justice sector, analysts from the Research Service have formulated a number of proposals. It is suggested that European standards be implemented into Ukrainian law to ensure the safety and accountability of AI systems by providing legal certainty regarding AI regulation, which will promote investment and innovation in this field. Proposals have been put forward to draft and adopt new regulatory acts setting out safety requirements for AI systems within the judicial system and the justice sector, and to improve Ukraine's procedural legislation with a view to the safe and effective AI implementation and use by the courts. (Parliamentary research on the legislative trends in the implementation of artificial intelligence tools in the field of justice in the European Union, 2025).

The Research Service has analysed Ukrainian legislation governing AI use, particularly in

the media, and provided recommendations on its updating to take account of current trends in the development of cutting-edge technologies. This refers to the need for legislation to define specific grounds, conditions and procedures for AI use in the media, to establish additional safeguards for the rights of media service consumers, and to set out appropriate sanctions for offences committed using AI. In addition, the information and analytical materials emphasised the advisability of introducing a code of ethical conduct regarding AI use in the activities of the media and journalists, which would set out: principles for the responsible AI use by journalists in their day-to-day work; rules for labelling AI-generated media content; requirements for developers and suppliers of AI-based solutions; rules allowing consumers to opt out of AI-generated content; and measures to prevent uncontrolled AI use (Information note on the use of artificial intelligence in the media:potential and risks, 2025).

A fundamental conclusion regarding the legal regulation of the autonomous robotics and AI technologies sector in the EU, its Member States and other countries around the world is that it is comprehensive in nature and places legal responsibility on humans rather than robots (Analytical note on comparative legislation regarding regulatory and legal regulation of the field of robotics and robotisation, 2025). Furthermore, based on a review of international experience regarding the legal regulation of robotics and automation, the Research Service's report outlines the existing conceptual approaches, which will enable those with the right to initiate legislation to select the most suitable option for Ukraine.

Given the rapid pace of development of AI technologies and their growing impact on all areas of social life, particularly in sports, the recommendations set out in the Research Service's reports regarding the improvement of the legal framework governing sports in Ukraine are highly relevant. Taking into account the results of the analysis of EU law in this area, the following is recommended: amending Ukrainian legislation in the field of sports, in particular with regard to defining specific grounds, conditions and procedures for AI use, and establishing appropriate sanctions for offences committed using AI; the implementation of 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 personal data processing and on such data free movement, and repealing Directive 95/46/EC. Emphasis is also placed on the need for the National Olympic Committee of Ukraine and Ukraine's sports federations, organised by sport, to develop guidelines on the use of these technologies and to introduce codes of ethics governing AI use in sports. In our opinion, these recommendations implementation will help to protect athletes' rights and ensure fairness, integrity, accuracy and a level playing field for all parties involved in sport activities.

Based on the review of international experience in regulating AI (Parliamentary Study on the Legislative Regulation of the Use of Artificial Intelligence Technologies Across Countries Worldwide, 2026; Analytical note on comparative legislation regarding the regulation of artificial intelligence technologies in Ukraine, European countries and the United States, 2025; Analytical note on comparative legislation regarding the regulation of artificial intelligence technologies in Ukraine, European countries and the United States, 2025; Analytical note (comparative legislation) on legislation in the area of use of artificial intelligence technologies (current conditions and development prospects in the EU and in other countries), 2023; Information note on trends in the legal regulation of artificial intelligence technologies in

Ukraine and India, 2025), analysts at the Research Service suggest that, in the process of drafting the Ukrainian Law on AI, the European approach to regulating this sector should be followed. This position is based not only on Ukraine's status as a candidate country for EU membership, but also on the human-centred nature of the relevant legislation. The EU acquis in the AI field regulation is characterised, in particular, by the binding nature and uniformity of human-centred rules designed to ensure a high level of protection for health, safety, fundamental human rights, environment, etc; and by the enshrinement of the right to define the national specificities of legislative regulation of social relations in this field.

Furthermore, for Ukraine, in the context of the Russian Federation's large-scale armed invasion, the EU's experience of exempting AI systems intended exclusively for military, defence or national security purposes from the scope of legislation is particularly relevant, regardless of the type of organisation carrying out such activities. Establishing a transition period for parties involved in social relations relating to AI to adapt to the new legislative requirements also reflects the realities in Ukraine regarding the development of cutting-edge technologies and attempts to regulate their use.

In the 2023 report by the Research Service, based on the analysis of the legal and regulatory framework governing AI in many countries around the world, it is suggested that a specific approach be followed when introducing legal regulation of AI technologies in Ukraine:

- public discussion of the issues and challenges involved in implementing and operating systems that use AI;
- identifying the areas that are the highest priority for AI use;
- developing, in addition to the concept, a series of recommendations and national standards for AI use, and a code of AI ethics;
- adopting a National Strategy for the Development of AI Technologies, for example covering a 10-year period, and an AI Act which will, first and foremost, introduce effective legal regulation of the use of AI-generated content, a classification system based on risk level, a ban on high-risk AI practices, and oversight and legal liability for any harm that may be caused by this technology;
- improving the legal framework governing all social relations relating to safe and reliable AI technologies use.

It is worth noting the implementation of certain components of this algorithm. In particular, on 31 March 2026, the Ministry of Digital Transformation of Ukraine published a draft Artificial Intelligence Development Strategy up to 2030 for public consultation (The path of AI development through 2030: explore the draft Strategy and provide feedback, 2026).

In order to develop a national public administration ecosystem in the AI field in Ukraine, we believe it would be advisable to take into account the findings of the Research Service's experts regarding global practices in shaping the institutional architecture of the AI sector (Analytical note (comparative legislation) on the system and functions of state bodies and other institutions in field of artificial intelligence following the example of certain foreign states, 2023). Thus, in the countries whose experiences were studied, regardless of the specific features of their state structure and political regime, varying levels of financial capacity or geographical location, special state institutions and other administrative mechanisms for coordination and control are being established. The coordination activities of these speciali-

sed state institutions in this field involve fostering constructive dialogue and fruitful cooperation between the private sector and state institutions regarding AI technologies research, development and implementation, with the involvement of academics and the provision of state support and funding for relevant start-ups.

The Research Service also organises and conducts training sessions for Members of the Ukrainian Parliament and their parliamentary advisers, as well as staff of the Secretariat of the Verkhovna Rada of Ukraine, with the aim of providing knowledge, skills and competences needed to understand and apply AI as a tool for optimising the search for and processing of necessary information, as well as for the preparation of various types of documents. These events are prepared and conducted in close cooperation with international and national partners, such as the Research Service of the Seimas of Lithuania, the parliaments of Greece and the Republic of Italy, and the Ministry of Digital Transformation of Ukraine.

Since October 2024, the Research Service's training centre has been organising numerous webinars focusing on various aspects of AI use in parliamentary work, in particular the value and appropriateness of AI use by parliamentary research service staff, and AI integration into the work of Ukrainian MPs and their parliamentary advisers. In addition, participants are introduced to specific AI technologies, such as large language models (LLMs). The legal, technical and social aspects of AI technologies are also explored.

4. Discussion

Table 1. Comparative patterns of parliamentary AI incorporation

Case	Governance approach	Technical/data focus	Human/organisational focus	Transferable lesson
Germany (Bundestag)	Central coordination of AI use cases	Shared tools for legal research, text processing and information retrieval	Cross-departmental coordination	Portfolio governance can reduce duplication and fragmented risk management.
Canada (House of Commons)	AI strategy, internal guidance and risk management	Controlled institutional deployment and internal resources	Staff awareness, surveys and continuous communication	Adoption should be people-centred and accompanied by institutional learning.
Spain (Senate)	Use of the IPU maturity framework for self-assessment	Assessment of technical capability alongside other dimensions	Organisational culture treated as a maturity factor	Maturity assessment should include governance and democratic impact, not technology alone.
Switzerland (Federal Assembly Library)	Pilot-based deployment with user control and source traceability	Semantic search combined with generative AI	Human judgement and user sovereignty	Source attribution and reversible user control are central to trustworthy research support.
Indonesia (House of Representatives)	Phased digital and AI transformation	Data consolidation, metadata standards and knowledge management	Institutional readiness precedes wider AI adoption	Reliable data infrastructure is a prerequisite for useful AI.

Case	Governance approach	Technical/data focus	Human/organisational focus	Transferable lesson
Bahrain (Council of Representatives)	Formal AI-management system aligned with ISO/IEC 42001	Integrated digital parliament and AI-enabled legislative tools	Governance, risk and oversight mechanisms	Management-system standards can institutionalise continuous AI governance.

In this part of the article, it is appropriate to discuss certain aspects of AI technologies use within the administrative bodies—in particular the research departments—of the national parliaments of Germany, Canada, Spain, Switzerland, Indonesia and Bahrain, without focusing on the Research Service of the Verkhovna Rada of Ukraine, as the issues and challenges faced by all these institutions are universal in nature. This approach has been adopted in line with the 'Guidelines for AI in Parliaments', which were developed by the Inter-Parliamentary Union (IPU) in collaboration with the Centre for Innovation in Parliament and published at the end of 2024 (Guidelines for AI in parliaments, 2024). It is worth noting that the document in question makes no mention of specific departments within parliamentary services, as it concerns AI implementation in parliaments as holistic ecosystems, of which the services supporting their operations—in particular research services—form an integral part. Furthermore, AI modernisation is viewed as a comprehensive process, the components of which are closely interlinked, and AI tools can be applied across all organisational units within parliamentary administrations. In view of the above, the guiding principles and recommendations for their implementation are relevant to all elements of the organisational structures of parliaments and parliamentary services, in particular research units.

In the context of this article, it is worth highlighting certain key recommendations from the UIP regarding compliance with these guiding principles. Firstly, the recommendation to prioritise the AI use in areas such as legislative research (identifying trends in legislative development, as well as similarities or contradictions in draft legislation and existing laws) and support for the legislative process (impact assessment of draft legislation; analysis of amendments to understand their impact on the draft legislation; analysis of the draft legislation impact; collecting comprehensive data on the application of the law and monitoring its impact). These activities are carried out by staff in the research departments of parliamentary secretariats to provide research, expert and analytical support for parliamentary activities (Guidelines for AI in parliaments, 2024).

According to the Guidelines for AI in Parliaments, the organisational framework for the AI-driven modernisation of parliamentary activities and parliamentary services should consist of the following key elements: small-scale pilot projects to gain the necessary experience in digital transformation; a focus on AI use provided that specific benefits are realised and risks are managed; reliable human oversight of AI systems; prioritising transparency and accountability in AI; investment in raising awareness of AI amongst parliamentary staff; and engagement with all stakeholders throughout the process of introducing AI technologies (Guidelines for AI in parliaments, 2024).

To address the unique risks associated with AI introduction into the work of parliament and its administrative secretariat, the following is recommended: guidelines development

to ensure human oversight of AI tools use in the legislative process; establishment of rules governing information disclosure on AI use in the legislative process; developing a flexible AI strategy that can be adapted to rapid technological changes; establishing mechanisms for equitable access to AI resources; and developing protocols for international cooperation on the exchange of experience regarding AI implementation in parliaments and parliamentary services.

The example of the German Bundestag (Prioritizing AI use cases at the German Bundestag, 2025) demonstrates the value of a systematic and comprehensive AI implementation in the work of parliament, in particular the parliamentary service, which entails the proper administration, management and oversight of the relevant technologies. The two priority areas selected for AI use relate directly to the research service: the legislative process and the functioning of the parliamentary secretariat/parliamentary service departments. The AI Cloverleaf Model, implemented in the Bundestag, is based on a comprehensive approach that enables staff across all departments to use a single programme, as its text processing, information retrieval and analytical tools are universal in nature. In our opinion, the argument put forward by Martin Kamprath, the Bundestag's AI coordinator, regarding the budgetary and organisational pragmatism of this approach is compelling, as it enables the parliamentary administration departments to develop coordinated strategies for AI use, thereby optimising the necessary resources and reducing the potential risks associated with AI technologies use (Prioritizing AI use cases at the German Bundestag, 2025; Kamprath, M., 2025). The range of tasks carried out to provide support, particularly to research staff, is quite broad: from automating legal research to producing information documents.

The work of the Secretariat of the lower house of the Canadian Parliament (The AI journey of the House of Commons of Canada, 2025) on the introduction of AI is people-centred and is based on striking a balance between technological innovation, data protection, the responsible use of financial resources to ensure AI implementation, and ongoing communication between the department responsible for implementing the relevant policy and staff from other units of the Parliamentary Service.

Gradual AI integration into the work of the House of Commons in general, and the Parliamentary Service in particular, began in April 2024. It should be noted that, given this article subject, the analysis focuses solely on that part of the Parliamentary Service's work related to AI introduction specifically for its staff. At the same time, it is worth noting that the House of Commons' Parliamentary Service is also focused on implementing AI for Members of Parliament. Firstly, specialised organisational structures were established to oversee specific aspects of this process. In June of that same year, the AI centre was launched on the House of Commons' intranet, containing resources and guidance on the responsible AI tools use by all users of this internal network. To refine the AI tools and improve the skills of intranet users, the results of regular surveys on their experience of using the relevant technologies were taken into account. For example, in April 2025, an educational campaign was launched to raise AI awareness.

In November 2025, the House of Commons' AI strategy was unveiled (Report to Canadians 2026, 2026), the key components of which are strategic vision and management; data and risk management; the expertise of parliamentary service staff; the experience of users of

materials produced using AI tools; a project-based approach; and the value of the outcomes of implementing the latest technologies. It is clear that cybersecurity and institutional resilience have been identified as priorities.

The experience of the Spanish Senate (New insights into AI maturity in the Senate of Spain, 2026) demonstrates the importance of evaluating the process and outcomes of AI implementation. International standards, such as those set out in the Framework for the Maturity of AI Use in Parliaments, can serve as a guide (Maturity Framework for AI in Parliaments) (Maturity Framework for AI in Parliaments, 2025), developed by the Centre for Innovation in Parliament of the Inter-Parliamentary Union in 2025. According to the document, AI technologies use should be considered across four dimensions: governance (rules, policies and control mechanisms to ensure the responsible AI use, including risk management and ethical guidelines), technical capabilities (infrastructure, data and security management for the successful deployment and operation of AI tools), organisational culture (the human factor and institutional culture necessary to support AI implementation), and the 'democratic impact' on democracy (the impact of AI implementation on the functioning of parliament, on citizen engagement, parliamentary transparency and accountability, and the preservation or strengthening of democratic values and processes) (Maturity Framework for AI in Parliaments, 2025).

The results of an assessment of the state of AI implementation in the upper house of the Spanish Parliament revealed technological achievements and shortcomings across all other dimensions. In light of this, it is clear that the decisive factors for the successful AI implementation are not the technologies themselves, but rather the right organisational culture, people and processes. In our view, all parliamentary services, particularly research departments, would do well to take this experience into account. At the same time, the national context must be taken into consideration, as AI introduction is not merely a matter of IT modernisation, and culture is a fundamental factor in this process. It is well known that national cultures have significant distinctive features, which makes it impossible to devise universal formulas for AI introduction into the work of parliaments and the departments that support their functioning.

It is also worth looking at the experience of the Library of the Federal Assembly of Switzerland (Federal Assembly of Switzerland embeds trust at the heart of technology, 2026), whose staff faced the operational challenge of indexing several thousand parliamentary documents annually in the three official languages. With this in mind, a pilot project to integrate AI into its operations was launched in collaboration between the parliamentary library and the Bern University of Applied Sciences. The technological essence of the project lies in combining semantic search with generative AI. However, given the subject matter of this article, it is worth focusing on other aspects of this institution's experience.

The chosen AI design was based on elements such as the absolute sovereignty of the user, who is granted the right to completely block AI generation and process only source documents; the primacy of human judgement, as AI merely assists humans rather than replacing them, placing full responsibility for the outcomes of using such technologies on humans, which is crucial for their incorporation into the legislative body activities; building trust in AI by establishing transparency, traceability and source attribution as key requirements,

thereby reducing the risks of losing source traceability or receiving misleading content; building trust in AI through the establishment or provision of user control functions regarding language, visible sources, feedback. etc.

Also of interest is the conclusion, drawn from the aforementioned pilot project results, regarding the advisability of a phased approach – within the framework of specific projects – to AI introduction into the parliamentary services work. The gradual integration of the latest technologies makes it possible to identify their shortcomings and rectify them swiftly.

Over the past few years, the lower house of the Indonesian Parliament (AI journey of the House of Representatives of Indonesia: A phased approach to responsible digital transformation, 2026) has been gradually digitising its operations, with the key measures set out in the master plan for the development of information and communication technologies (hereinafter 'ICT') (Caperna, A., 2010) for 2020–2024.

During the phase of developing the digital foundations (2020–2022), priority was given to system integration through the consolidation of ICT system components and the strengthening of digital coordination between departments within the administration, as well as to enhancing cyber security and establishing a big data infrastructure. The data management development phase (2022–2023) proved to be a turning point. Thanks to these innovations – in particular, the launch of the One Data portal (a central big data repository), the standardisation of metadata used by the lower house's administrative departments, and the introduction of several data quality initiatives – there was a rise in confidence among the staff of the lower house's administrative departments regarding the AI technologies use for analytics. This was followed by the phase of AI implementation through specialised projects (2024–2025), which was carried out in line with the vision of AI technologies as a support mechanism and analytical assistant, rather than as a decision-maker. As of today, the final phase involves the refinement of knowledge management in the field of legislation (Knowledge management tools and processes, 2026) (2025–2027), which is being implemented in accordance with the House of Representatives' Master Plan for ICT Development for 2025–2027. Data on legislation, the findings of parliamentary oversight and public opinion have already been consolidated into unified platforms and systems, which will help improve AI ability to recognise patterns and enrich the institutional memory of the Indonesian House of Representatives. AI, under the supervision of specialists, will help to identify trends in legislative development and formulate evidence-based policies.

In our opinion, all parliamentary research units, in particular the Research Service, should take into account the key findings arising from the ICT modernisation of the lower house of the Indonesian Parliament when undertaking the digital transformation of their operations. The modernisation key elements should be harmonisation of data standards across all departments of the parliamentary service, integration of traditional and modern infrastructure, development of comprehensive AI management systems, assurance of effective cybersecurity and data protection, as well as enhancement of staff knowledge and awareness regarding AI. In light of this, the most important conclusion is the realisation that the priority lies not with the technological challenge, but with the challenge of the House of Representatives' institutional readiness for the relevant changes. This refers to the need to prevent the premature AI integration into the institution operations whilst its data proces-

sing system remains underdeveloped, as this will inevitably have a negative impact on both the technological component of digital transformation and the staff confidence in modern digital technologies.

The Bahrain Council of Representatives is the first legislative body in the world to have its AI governance system certified (The smart governance benchmark: Council of Representatives of Bahrain achieves ISO certification for AI, 2026). This refers to ISO/IEC 42001 – the world's first standard setting out requirements for the establishment, implementation, maintenance and continuous improvement of the AI management system within organisations (ISO/IEC 42001:2023. Information technology – Artificial intelligence – Management system, 2023). The standard requires the establishment of a governance framework, risk management protocols and oversight mechanisms to ensure the safe, transparent and ethical operation of AI programmes implemented within organisations. The requirements set out take into account the unique challenges arising from AI use – ethics, transparency and continuous learning – and strike a balance between digital innovation and its governance.

The digital modernisation of Bahrain's lower house of parliament was achieved through: the creation of a comprehensive e-parliament system, one of whose functions is AI use to analyse legislative acts; the introduction of a paperless operating model in the parliament's day-to-day activities; and robust data management protocols to ensure data quality, security and confidentiality. These measures have undoubtedly also had an impact on the Centre for Parliamentary Research and Training, which provides research and analytical support to the legislature. For example, the integration of an AI-powered chatbot into the parliamentary service digital infrastructure has provided analysts, in particular, with real-time access to all draft legislation and other parliamentary materials, thereby helping to optimise the analysis of these documents (AI-powered parliamentary bill and document chatbot for enhanced legislative analysis, 2024).

In addition to international certification of its AI management system, the Bahrain Council of Representatives has received certificates confirming that the information security and environmental management systems implemented in its operations comply with international standards (ISO/IEC 27001 and ISO 14001) (Certifying the First Legislative Body Worldwide Against ISO/IEC 42001, 2026). This international recognition attests to the successful application of a comprehensive, systemic approach to the digital modernization of the operations of the lower house of Bahrain's parliament.

Given the rapidly growing AI capabilities to manipulate and alter information, the study by the European Parliament Research Service (EPRS) on the threats posed by the deepfake technology use (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 (Artificial Intelligence Act) (Text with EEA relevance)), that needs to be taken into account by the staff of parliamentary research services while searching for information to prepare analytical materials (Bentzen, N., 2025).

This is geopolitical influence – e.g., shaping negative global public opinion on how the international community perceives Ukraine amidst the Russian Federation's large-scale

armed aggression; influencing elections in numerous countries, including Moldova, Slovakia, the USA, India, and the UK; shaping public opinion on any given issue; discrediting women and minorities; as well as propagating societal prejudices – such as stereotypes – concerning specific individuals or population groups; ”information laundering” – legitimization of false or misleading information, particularly regarding historical events or scientific achievements, through a network of intermediaries, employing a set of methods to distort and conceal the original source.

5. Limitations

The study is based on publicly available institutional documents, parliamentary publications and scholarly sources. It does not include interviews with parliamentary staff, access to internal technical logs, independent security testing or direct measurement of time savings, accuracy gains or user satisfaction. Accordingly, references to benefits, maturity or institutional readiness should be interpreted as documentary and comparative assessments rather than causal evaluations.

The six comparative cases were selected purposively because recent documentation was available and because they represent contrasting governance pathways. They are not a representative sample of all national parliaments. In addition, AI tools and institutional policies evolve quickly; the analysis therefore reflects the documented state of practice up to mid-2026 and should be revisited as parliamentary AI governance matures.

6. Conclusion

The comparison shows that responsible AI incorporation into parliamentary research services is primarily an institutional-governance task rather than a question of tool acquisition. Across the cases examined, five recurring conditions are visible: explicit governance rules, reliable and permission-aware data practices, human oversight, investment in staff competence, and staged implementation through pilots or controlled use cases. The IPU framework is useful precisely because it connects technical capability with organisational capability, governance and democratic impact.

The Research Service of the Verkhovna Rada of Ukraine demonstrates an emerging model consistent with these principles. Its internal regulatory documents treat AI as an auxiliary instrument, restrict the use of non-public or protected information, require professional verification and preserve human responsibility for analytical conclusions. The Service’s experience can be understood through four vectors: regulation of AI use; development and dissemination of institutional guidance; preparation of comparative analytical materials on AI regulation and applications; and AI-literacy activities for parliamentarians, advisers and parliamentary staff.

The principal scientific contribution of the study is the distinction between technological adoption and governance capacity in parliamentary research. The comparative cases suggest that sustainable AI incorporation depends on the quality of institutional arrangements around the technology: source traceability, data governance, role-based access, transparent

responsibility, professional review and continuous learning. These conditions are particularly important for parliamentary research services because errors or opaque automation may affect legislative analysis and, indirectly, democratic decision-making.

For practice, the findings support a staged roadmap for parliamentary research services: define authorised and prohibited uses; classify data and access rights; pilot bounded use cases; require source-linked verification; train staff; monitor incidents and user experience; and periodically reassess maturity against parliament-specific governance criteria. Future research should test these propositions empirically through interviews, workflow observation, accuracy audits and comparative measures of productivity and trust.

Funding

This research received no external funding.

Conflicts of Interest

The authors declare no conflicts of interest.

Data Availability

The study is based on publicly available institutional documents, parliamentary publications and sources listed in the References. No original dataset was generated.

Ethics Statement

The study did not involve human participants, personal data collection or experimental intervention; ethics committee approval was therefore not required.

Declaration of Generative AI Use

Generative AI tools were used to support language editing during the preparation of this manuscript. The authors verified all factual and legal claims and take full responsibility for the content of the article.

References

AI journey of the House of Representatives of Indonesia: A phased approach to responsible digital transformation. (2026). Innovation tracker. Issue 25. https://www.ipu.org/innovation-tracker/story/ai-journey-house-representatives-indonesia-phased-approach-responsible-digital-transformation

AI-powered parliamentary bill and document chatbot for enhanced legislative analysis. (2024). https://www.ipu.org/ai-use-cases/ai-powered-parliamentary-bill-and-document-chatbot-enhanced-legislative-analysis

Analytical note (comparative legislation) on legislation in the area of use of artificial intelligence technologies (current conditions and development prospects in the EU and in other countries). (2023). [In Ukrainian]. https://research.rada.gov.ua/documents/analyticRSmaterialsDocs/industry_policy/analytical_notes--indst/73835.html

Analytical note (comparative legislation) on the implementation of the Smart City concept in the European

Union, USA, Canada and South Korea. (2024). [In Ukrainian]. https://research.rada.gov.ua/uploads/documents/34149.pdf

Analytical note (comparative legislation) on the system and functions of state bodies and other institutions in field of artificial intelligence following the example of certain foreign states. (2023). [In Ukrainian]. https://research.rada.gov.ua/uploads/documents/32593.pdf

Analytical note on comparative legislation regarding regulatory and legal regulation of the field of robotics and robotisation. (2025). [In Ukrainian]. https://research.rada.gov.ua/uploads/documents/33596.pdf

Analytical note on comparative legislation regarding the regulation of artificial intelligence technologies in Ukraine, European countries and the United States. (2025). [In Ukrainian]. https://research.rada.gov.ua/uploads/documents/33722.pdf

Bentzen, N. (2025). Information manipulation in the age of generative artificial intelligence. European Parliamentary Research Service. https://www.europarl.europa.eu/RegData/etudes/BRIE/2025/779259/EPRS_BRI(2025)779259_EN.pdf

Caperna, A. (2010). Integrating ICT into Sustainable Local Policies. Handbook of Research on E-Planning: ICTs for Urban Development and Monitoring. 25 p. https://doi.org/10.4018/978-1-61520-929-3.ch018. https://www.igi-global.com/chapter/integrating-ict-into-sustainable-local/43194

Catalog of analytical and informational materials of the Research Service of the Verkhovna Rada of Ukraine (2026). [In Ukrainian]. https://research.rada.gov.ua/documents/analyticRSmaterialsDocs/73288.html

Certifying the First Legislative Body Worldwide Against ISO/IEC 42001. (February 12, 2026). SGS website. https://www.sgs.com/en/news/2026/02/sgs-certifies-the-first-legislative-body-worldwide-against-iso-iec-42001

Cifuentes-Silva, F., Astudillo, H., Labra Gayo, J. (2025). Transforming parliamentary libraries: Enhancing processes delivering new services with artificial intelligence. IFLA Journal, 51, 3. https://journals.sagepub.com/doi/10.1177/03400352251315844

Federal Assembly of Switzerland embeds trust at the heart of technology. (2026). Innovation tracker. Issue 25. https://www.ipu.org/innovation-tracker/story/federal-assembly-switzerland-embeds-trust-heart-technology

Gonzalo, M. Á. (2024). The role of Artificial Intelligence in Open Parliament: enhancing transparency, critical thinking, and combating disinformation. IFLAPARL Annual Conference, Madrid. https://repository.ifla.org/rest/api/core/bitstreams/a1eb5f5e-6be2-4f97-8045-ee41b79d2eb2/content

Guidelines for AI in parliaments. (2024). https://www.ipu.org/ai-guidelines

How the Parliament of Austria uses TikTok. (2025). Innovation tracker. Issue 21. https://www.ipu.org/innovation-tracker/story/how-parliament-austria-uses-tiktok

Implementing artificial intelligence best practices will ensure a higher level of transparency and openness in Parliament. (November 29, 2024). Official webportal of the Parliament of Ukraine. [In Ukrainian]. https://www.rada.gov.ua/news/Novyny/256186.html

Information note on the use of artificial intelligence in the media:potential and risks. (2025). [In Ukrainian]. https://research.rada.gov.ua/uploads/documents/33465.pdf

Information note on trends in the legal regulation of artificial intelligence technologies in Ukraine and India. (2025). [In Ukrainian]. https://research.rada.gov.ua/uploads/documents/33682.pdf

Information reference on the peculiarities of the functioning of parliamentary websites: structure, content, methods of efficiency assessment. (2025). [In Ukrainian]. https://research.rada.gov.ua/uploads/documents/33537.pdf

Informational Reference on Current Trends in the Development and the State of Ensuring the Independence of Judges and the Judicial System in Ukraine (2024–2025). (2026). [In Ukrainian]. https://research.rada.gov.ua/uploads/documents/34099.pdf

ISO/IEC 42001:2023. Information technology – Artificial intelligence – Management system. https://www.iso.org/ru/standard/42001

Kamprath, Martin. (2025). The AI Cloverleaf Model - Mapping AI Use Cases in Parliaments. https://www.researchgate.net/publication/395576488_The_AI_Cloverleaf_Model_-_Mapping_AI_Use_Cases_in_Parliaments

Knowledge management tools and processes. (2026). Website The Centre for Legal Leadership. https://www.legalleadership.co.uk/knowledge/delivering-services/technology-and-innovation/knowledge-management-tools-and-processes/

Koryzis, D., Dalas, A., Spiliotopoulos, D. and Fitsilis, F. (2021). ParlTech: Transformation Framework for the Digital Parliament. Big Data and Cognitive Computing, 5, 1, 1-16. https://www.mdpi.com/2504-2289/5/1/15 ;

Leston-Bandeira, C. (2007). The Impact of the Internet on Parliaments: A Legislative Studies Framework. Parliam. Aff. 60, 655–674. https://www.agora-parl.org/sites/default/files/agora-documents/The%20Impact%20of%20the%20Internet%20on%20Parliament%20-%20a%20Legislative%20Studies%20Framework.pdf

Lucke, J., Etscheid, J. and Fitsilis, F. (2022). Using Artificial Intelligence for Legislation – Thinking About and Selecting Realistic Topics. EGOV-CeDEM-ePart, Linköping University, Sweden (Hybrid). https://ceur-ws.org/Vol-3399/paper3.pdf

Lucke, J., Fitsilis, F. and Etscheid, J. (2023). Research and Development Agenda for the Use of AI in Parliaments. In 24th Annual International Conference on Digital Government Research - Together in the unstable world: Digital government and solidarity, Gdańsk, Poland. ACM, New York, NY, USA, 15 p. https://doi.org/10.1145/3598469.3598517

Maturity Framework for AI in Parliaments. (2025). https://www.ipu.org/resources/publications/toolkits/2025-11/maturity-framework-ai-in-parliaments

New insights into AI maturity in the Senate of Spain. (2026). Innovation tracker. Issue 25. https://www.ipu.org/innovation-tracker/story/new-insights-ai-maturity-in-senate-spain

On the Approval of the E-Parliamentarism Strategy for 2018–2020: Order of the Chairman of the Verkhovna Rada of Ukraine No. 278 dated July 5, 2018. [In Ukrainian]. https://zakon.rada.gov.ua/laws/show/278/18-%D1%80%D0%B3#Text

Parliamentary research on the institutional establishment and assessment of the capabilities of the DPRK's cyber forces (2025). [In Ukrainian]. https://research.rada.gov.ua/uploads/documents/33304.pdf

Parliamentary research on the legislative trends in the implementation of artificial intelligence tools in the field of justice in the European Union. (2025). [In Ukrainian]. https://research.rada.gov.ua/uploads/documents/33379.pdf

Parliamentary Study on the Legislative Regulation of the Use of Artificial Intelligence Technologies Across Countries Worldwide. (2026). [In Ukrainian]. https://research.rada.gov.ua/uploads/documents/34035.pdf%20

Prioritizing AI use cases at the German Bundestag. (2025). Innovation tracker, Issue 22. https://www.ipu.org/innovation-tracker/story/prioritizing-ai-use-cases-german-bundestag

Recommendations from the Research Service of the Verkhovna Rada of Ukraine. (2026). AI in Comparative Law: How to Cover the Experience of 30 Countries in One Hour. Digest of News on Artificial Intelligence Technologies and Digital Innovations. April 2026, No. 5. [In Ukrainian].

Recommendations of the Research Service of the Verkhovna Rada of Ukraine. (2026). AI as a tool for parliamentary analysis: from large document sets to concise conclusions. Digest of news on artificial intelligence technologies and digital innovations. June 2026, No. 7. [In Ukrainian].

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 (Artificial Intelligence Act) (Text with EEA relevance). https://eur-lex.europa.eu/eli/reg/2024/1689/oj/eng

Regulation on the Implementation of Artificial Intelligence. (2026). Technologies in the Activities of the Research Service of the Verkhovna Rada of Ukraine: Approved by Order No. 32-o.d. of the Head of the Research Service of the Verkhovna Rada of Ukraine dated March 16, 2026. [In Ukrainian]. https://research.rada.gov.ua/news/novyny/77362.html

Report to Canadians 2026. Reporting on Results. https://www.ourcommons.ca/reporttocanadians/en/reporting-on-results

Strategy for the Digital Development of Innovation Activities in Ukraine for the Period up to 2030: Approved by Order of the Cabinet of Ministers of Ukraine No. 1351-p dated December 31, 2024. Official webportal of the Parliament of Ukraine. [In Ukrainian]. https://zakon.rada.gov.ua/laws/show/1351-2024-%D1%80#top

Szentgáli-Tóth, B. A. and Berkes, R. (2025). Artificial Intelligence in the Service of Parliaments: Some Arguments for the Necessity of a Normative Legal Framework at the European Level. MASARYK UNIVERSITY JOURNAL OF LAW AND TECHNOLOGY, 19 (2), 237-272. ISSN 1802-5943. https://real.mtak.hu/228484/1/ArtificialIntelligenceintheServiceofParliaments.pdf

The AI journey of the House of Commons of Canada. (2025). Innovation tracker. Issue 23. https://www.ipu.org/innovation-tracker/story/ai-journey-house-commons-canada

The path of AI development through 2030: explore the draft Strategy and provide feedback. (2026). Website of the Ministry of Digital Transformation of Ukraine. [In Ukrainian]. https://thedigital.gov.ua/news/shtuchnyy-intelekt/shliakh-rozvytku-shi-do-2030-roku-znayomtesia-z-proyektom-stratehiyi-ta-davayte-fidbek

The smart governance benchmark: Council of Representatives of Bahrain achieves ISO certification for AI. (2026). Innovation tracker. Issue 25. https://www.ipu.org/innovation-tracker/story/smart-governance-benchmark-council-representatives-bahrain-achieves-iso-certification-ai

Ukraine plans to integrate AI into government bodies by 2030 and become one of the top three global leaders. Sudovo-yurydychna hazeta. (June 20, 2026). [In Ukrainian]. https://sud.ua/uk/news/publication/364025-ukraina-planiruet-integrirovat-ii-v-gosudarstvennyy-sektor-do-2030-goda-i-voyti-v-top-3-mirovykh-liderov

United Nations et al. (2008). The World E-Parliament Report. https://unpan.un.org/sites/default/files/d8-files/DPIDG%20Publications/2008/World%20e-Parliament%20Report%202008.pdf

Vaolevska, L. A. & Myshchak, I. M. (2025). Improving the Legislative Activity Planning of the Verkhovna Rada of Ukraine of the IX Convocation. Law of Ukraine. No 5, 65–77. https://pravoua.com.ua/en/store/pravoukr/pravo_2025_5/pravo_2025_5-s4242

What is Semantic Web and Semantic Technology? (January 29, 2026). Website Graphwise. https://graphwise.ai/fundamentals/what-is-semantic-web-and-semantic-technology/

Ziouvelou, X., Giannakopoulos, G. and Giannakopoulos, V. (2022). Artificial Intelligence in the Parliamentary Context. In Fitsilis, F. and Mikros, G. (eds.). Smart Parliaments - Data-Driven Democracy. 43-53. DOI: https://doi.org/10.53121/ELFTPS4

Human Dignity And The Legitimacy Of Public Authority In The Digital Transformation Of The State: A Two-Axis Governance Test For Automated Administration

Svitlana Bobrovnyk
Department of Theory and History of Law and State
Educational and Scientific Institute of Law
Taras Shevchenko National University of Kyiv
Kyiv, Ukraine
ORCID iD: 0000-0002-9225-8871

Anatolii Shevchenko
Department of Law, Public Management, and Administration
Zhytomyr Polytechnic State University
Zhytomyr, Ukraine
ORCID iD: 0000-0003-2663-9892
shevchenko2757@ukr.net

Olha Varych
Department of Theory and History of Law and State
Educational and Scientific Institute of Law
Taras Shevchenko National University of Kyiv
Kyiv, Ukraine
ORCID iD: 0000-0003-0289-4039

Abstract.

The digital transformation of the state increasingly places public authority behind digital interfaces, data infrastructures, automated administrative procedures and artificial-intelligence-assisted decision systems. This article develops a theoretical-legal framework for assessing whether such transformation remains compatible with human dignity and with the legitimacy of public authority. It treats dignity as the substantive limit that prevents the individual from being reduced to a data object or passive object of administration, and legitimacy as the public-law condition that requires authority to remain intelligible, contestable, accessible and accountable when exercised through digital systems. Using doctrinal and comparative normative analysis, the article reads these concepts alongside European legal benchmarks, including the Charter of Fundamental Rights of the European Union, the General Data Protection Regulation, the EU Artificial Intelligence Act and Council of Europe instruments on algorithmic systems and artificial intelligence. The principal contribution is a two-axis governance test that translates dignity and legitimacy into operational questions for the design and review of digital public procedures. The test examines preservation of the person's legal subjecthood and individual circumstances, intelligibility of reasons, effective human review and remedy, equal accessibility, and identifiable institutional responsibility. The article argues that digitalisation strengthens public authority only when efficiency gains are accompanied by procedural safeguards, data protection, non-exclusion and meaningful avenues of challenge. The framework is conceptual rather than empirical and is offered as a normative assessment tool for sustainable digital governance.

Keywords: *human dignity; legitimacy of public authority; digital transformation of the state; automated administration; AI governance; sustainable digital governance.*

1. Introduction

The digital transformation of the modern state has become one of the principal ways in which the forms and methods of exercising public authority are changing in the twenty-first century. Its manifestations are the digitalisation of administrative procedures, the development of electronic services and of digital identification, the automated processing of data, the algorithmisation of administrative decisions, and the growing role of digital platforms in mediating the relationship between the state and the individual. The introduction of elements of artificial intelligence into public administration has substantially altered the character of that relationship.

Such processes are usually assessed through the prism of efficiency, speed, accessibility and institutional modernisation. Their effects, however, extend well beyond the technical renewal of public administration, and they cannot be evaluated solely as a technical modernisation of the state apparatus. Digitalisation bears directly on the value foundations of the modern state, because it changes the limits of authoritative influence, the degree of transparency of administrative decisions, the individual's access to the protection of their rights and interests, and the conditions under which public authority is recognised by society. In short, digital transformation alters not only the instruments of state activity but the character of public authority itself, the conditions under which it is perceived, and the limits of permissible authoritative interference.

The question that follows is whether the human being remains the centre of state policy under conditions of digitalisation, or whether the significance of the individual is gradually diminished and the person reduced to a digital profile or a set of data subject to automated processing. In this context, two categories acquire particular importance: human dignity and the legitimacy of public authority.

Human dignity makes it possible to assess whether digital transformation turns the person into a passive object of digital administration, and whether it reduces the person to a collection of data to be processed automatically. It is in this sense that dignity operates as a fundamental value of the modern state. Legitimacy, in turn, makes it possible to establish whether public authority retains social recognition under conditions in which authoritative procedures are becoming ever more complex, technologically mediated and potentially less intelligible to those subject to them. Digitalisation also changes the grounds of legitimacy. Whereas in the traditional understanding legitimacy was associated principally with legality, social recognition and trust in state institutions, digital transformation adds new criteria: the transparency of digital procedures, the accessibility of the substance of decisions taken by state bodies, the fairness of those decisions, and the possibility of oversight and appeal.

The central problem is therefore not whether the state should digitalise, but under what legal and institutional conditions digitalisation remains compatible with the status of the person as a rights-holder and with the justified exercise of public authority. A formally lawful digital procedure may still be normatively defective if it renders the person invisible as an individual, prevents them from understanding why a decision was taken, or leaves no effective human route for correction and challenge. Conversely, digitalisation may strengthen public authority where it expands access, reduces arbitrary discretion, improves traceability and preserves meaningful procedural guarantees.

This inquiry belongs squarely to the agenda of law, digital technologies and sustainable governance. Sustainable digital governance is understood here not as the persistence of a technical system but as the capacity of digitally mediated public authority to remain legally justified, socially recognisable, procedurally fair and institutionally accountable over time. Human dignity and legitimacy are therefore treated not as external ethical commentary on digital government but as internal conditions of its durability.

2. The State Of Research And The Research Gap

Contemporary scholarship addresses e-government, automated administration, data protection, digital constitutionalism, algorithmic accountability and AI governance with considerable intensity. Yet three strands of the debate often remain separated. Human dignity is frequently invoked as a foundational value without being translated into concrete questions for system design; legitimacy is discussed as trust or social acceptance without sufficient connection to procedural safeguards; and technical or regulatory AI-risk frameworks do not always explain how defects in digital administration affect the justification of public authority as such. The resulting gap is therefore not a lack of discussion about digital government, but a lack of an integrated legal test linking the status of the person to the conditions under which digitally mediated authority can remain legitimate.

The present study addresses that gap through four propositions:

1. human dignity should operate as an assessable limit on the reduction of the person to data, categories or automated outputs;
2. legitimacy should be expressed through intelligibility, procedural fairness, accessibility, contestability and identifiable responsibility;
3. digital transformation should be evaluated against those two axes in addition to efficiency, legality and technical performance; and
4. a combined dignity–legitimacy test can be used ex ante when public bodies design digital procedures and ex post when their effects are reviewed.

3. Aim, Scope And Method

The aim of the article is to substantiate human dignity and the legitimacy of public authority as interrelated criteria for assessing the digital transformation of the state and to operationalise those criteria in a two-axis governance test applicable to automated and algorithmically assisted public procedures. The study asks three questions: what dignity requires from digitally mediated authority; what conditions sustain legitimacy when decisions are technologically mediated; and how those requirements can be converted into practical design and review criteria.

Methodologically, the article proceeds by theoretical-legal (doctrinal) and comparative normative analysis. It reconstructs human dignity and legitimacy in general legal theory and tests those categories against contemporary forms of digital public authority. European legal materials are used as normative benchmarks: Article 1 of the Charter of Fundamental Rights of the European Union, the Charter's guarantees of good administration and effec-

tive remedy, the General Data Protection Regulation's rules on solely automated decisions with legal or similarly significant effects, the EU Artificial Intelligence Act, Council of Europe Recommendation CM/Rec(2020)1, and the Council of Europe Framework Convention on Artificial Intelligence and Human Rights, Democracy and the Rule of Law (CETS No. 225). As of August 2026, the EU AI Act has entered its general application phase, although specified obligations remain subject to staged dates. The study does not assume that each European instrument applies identically to every Ukrainian public body; they are used to identify converging principles relevant to comparative governance analysis. No original empirical data are presented, and the proposed test is normative rather than a validated psychometric or administrative-performance instrument.

4. Human Dignity As The Axiological Foundation Of The Modern State

4.1 Dignity as a value-based limit on public authority

Human dignity occupies a central place in the axiological structure of the modern state. It is not merely one legal value among many, but the normative and philosophical foundation on which the legitimacy of public authority must itself rest. In the contemporary understanding of statehood, dignity operates as the criterion that determines both the permissible limits of the exercise of public authority and the value orientation of legal regulation. For that reason, any analysis of the digital transformation of the state that ignores the role of human dignity risks remaining incomplete: it will reduce digitalisation to a purely technical or institutional process and pass over its profound effect on the legal status of the person (Charter of Fundamental Rights of the European Union, 2016; De Gregorio, 2022).

In legal theory, human dignity is traditionally understood as an inalienable quality of the person and as a principle shaping the relationship between the individual and the state. This understanding is reflected expressly in Article 1 of the Charter of Fundamental Rights of the European Union, which places dignity at the beginning of the Charter's normative architecture. For digital administration, the implication is not that every use of automation violates dignity, but that the person must remain a legal subject rather than becoming merely the object of classification, scoring or automated processing. The state may organise and modernise its institutions, but it must retain procedures capable of recognising rights, individual circumstances and legitimate interests (Charter of Fundamental Rights of the European Union, 2016; De Gregorio, 2022).

This understanding acquires particular significance where public authority relies on digital identity, linked databases, automated eligibility checks or AI-assisted administrative decisions. Data representations are necessarily selective: they describe the person through attributes that a system is designed to process. The legal risk arises when that representation becomes functionally equivalent to the person for decision-making purposes and no institutional mechanism remains for correcting incomplete data, presenting relevant circumstances or obtaining meaningful human reconsideration. European data-protection law addresses one part of this problem through safeguards surrounding certain decisions based solely on automated processing; these rules are not a general prohibition on automation, but they illustrate the broader requirement that significant decisions remain procedurally

governable (European Parliament and Council of the European Union, 2016; European Data Protection Board, 2018).

From an axiological standpoint, dignity therefore generates three requirements for digital public authority. First, the system must preserve legal subjecthood: the individual must be able to appear before the administration as more than a data profile. Second, the procedure must preserve agency: the person must be able to receive relevant information, submit material, correct data and seek human intervention where required by law. Third, technological mediation must remain proportionate to the public purpose pursued, particularly where biometric, behavioural, location or other intrusive data are involved. These requirements connect dignity to privacy, procedural fairness and the possibility of effective remedy without collapsing dignity into any one of those rights.

4.2 The three functions of human dignity under digital transformation

In this context it may be argued that human dignity performs at least three interrelated functions under conditions of the digital transformation of the state.

First, dignity operates as a foundational value of the modern legal order. It confirms that the legitimacy of state activity cannot be measured solely by efficiency, expediency or administrative rationality. Even where digital systems increase the speed and accessibility of administrative procedures, that alone cannot justify their use if they undermine the standing of the human being as an autonomous subject of law.

Second, dignity performs the function of a substantive limit on the digitalisation of public authority. Public authority cannot legitimately rely on digital systems in a manner that levels out the individual characteristics of the human being, the person and the citizen, or that makes it impossible to challenge individual decisions of state bodies effectively. In this sense dignity constrains the expansion of digital public authority, so that technological innovation remains compatible with the inalienable value of the human being.

Third, dignity serves as a criterion for assessing the admissibility of digital models of governance. It allows the question to be posed whether a particular digital system or platform is compatible with the value foundations of the modern state. Even where a digital procedure is formally permitted by law, it may nonetheless run counter to human dignity and may to some degree deprive the person of the realisation of their subjective rights and of the possibility of protecting them.

It follows that, where public authority relies on such systems, the human being becomes visible to the system only to the extent that they correspond to a predefined set of input data or to a predefined category — something that is capable, overall, of weakening the significance both of the human being and of legality in the relationship between the state and the individual. A state that organises digital public authority in such a way that people become invisible, interchangeable or procedurally defenceless risks undermining the very value foundation on which modern statehood rests.

The digital transformation of the state cannot, therefore, be regarded as axiologically neutral. It bears directly on the state's capacity to preserve its humanistic and legal orientation. Where digitalisation strengthens accessibility, transparency and procedural fairness

without eroding respect for the person, it can reinforce the value foundations of modern statehood. Human dignity should accordingly be regarded as the first and fundamental criterion for assessing the effectiveness of the digital transformation of public authority.

5. The Legitimacy Of Public Authority In The Digital Age

Legitimacy concerns the justified recognition of public authority. In this article it is used in a normative public-law sense rather than as an empirical measure of popularity or trust. Digitalisation alters the conditions of legitimacy because the citizen increasingly encounters the state through interfaces, automated workflows and outputs generated from data rather than through an identifiable official exercising visible discretion. The question is therefore whether authority remains understandable, answerable and open to challenge when its exercise is technologically mediated.

Four conditions become especially important. The first is intelligibility: a person affected by a significant digital decision must be able to understand its legal and factual basis to the extent required for effective participation and challenge. The second is contestability: the procedure must preserve a realistic route to correction, review and remedy rather than merely provide a technically final output. The third is equal accessibility: digital-by-default administration must not convert lack of connectivity, disability, age, displacement or limited digital literacy into practical exclusion. The fourth is accountable attribution: responsibility must remain attached to an identifiable public institution and, where appropriate, to human decision-makers, rather than being displaced onto a vendor, dataset or model (Greenstein, 2022; Kouroutakis, 2024; Langer, 2024; Røhl, 2023).

A digitally transformed procedure may therefore comply with formal competence rules yet still suffer a legitimacy deficit if the person cannot understand the decisive grounds, cannot reach an effective reviewer, or cannot identify which authority is responsible for correcting an error. European law increasingly expresses these concerns through overlapping guarantees of good administration, data protection, transparency, human oversight and effective remedy. The EU AI Act and the Council of Europe Framework Convention on AI are significant not because they replace administrative law, but because they reinforce the proposition that technologically mediated authority must remain subject to human-rights, accountability and risk-management requirements (European Parliament and Council of the European Union, 2024; Council of Europe, 2024).

Legitimacy in the digital age should accordingly be understood as compatible with, rather than opposed to, efficiency. Faster services, reduced administrative burden and more consistent decisions may strengthen the justification of public authority when they are achieved within procedures that remain intelligible, inclusive and reviewable. The relevant distinction is therefore not between human and digital administration, but between governable and ungovernable digitalisation.

6. The Dual Nature Of Digital Transformation
6.1 Opportunities

Considered in its functional dimension, the digital transformation of the state opens up a number of evident opportunities.

The first is an increase in the promptness and effectiveness of public administration. Digital systems make it possible to reduce the time required to deliver services, to simplify administrative procedures, to reduce the bureaucratic burden, to increase the speed at which information is processed, and to optimise communication between public authorities and citizens. In this respect digitalisation contributes to the modernisation of the state mechanism and to the strengthening of its institutional capacity.

A second substantial opportunity is the widening of citizens' access to public services. Electronic services, digital personal accounts, remote forms of interaction with the state and electronic document flow are capable of making the realisation of rights and legitimate interests more convenient and faster, and less dependent on territorial or other organisational obstacles. In this respect digital transformation potentially strengthens the service orientation of the state and may be regarded as a way of bringing public authority closer to the needs of the individual (Røhl, 2023; da Rosa Lazarotto, 2025).

A further opportunity concerns the transparency of public authority. Where they are properly organised, digital instruments can facilitate access to public information, promote the openness of state registers, improve procedures for monitoring the activity of public bodies, and strengthen the capacity for public oversight — and thereby reduce corruption risks.

6.2 Risks

Alongside these opportunities, however, the digital transformation of the state generates risks that are fundamentally new, and that are legal as well as axiological in character. Digitalisation cannot therefore be assessed exclusively as a positive instrument of modernisation. Its effect is dual in nature: on the one hand digital transformation opens new resources for the development of the modern state; on the other, it creates new threats to that state's humanistic, legal and democratic nature.

Depersonalisation of public authority. One of the most serious risks is the depersonalisation of public authority. The more the state's interaction with the individual is conducted through digital systems, the greater the probability that the person will be perceived by public authority not as an individualised subject of law but as a profile in a database or a set of formalised characteristics. Under such conditions public authority loses its immediate human dimension, and the legal relationship between the state and the individual is ever more extensively mediated by technological mechanisms. This creates the danger that the personal, individual and humanistic element will be progressively displaced from the sphere of public administration.

Identification of the person with their data. Closely connected with depersonalisation is the risk of identifying the person with their digital data. Where the individual comes to be

perceived primarily through a set of digital records, there is a danger that the real individual circumstances and the substance of the legal situation will fall outside proper consideration. Law then loses its just and human-centred nature.

Opacity of digital decisions. A person may receive a digital outcome without being able to identify the decisive factual inputs, legal rules or institutional reasoning behind it. The concern is not that every algorithm must be technically explainable to every user; the public-law requirement is that the administration remain capable of giving reasons sufficient for the affected person to understand and contest a decision where such reasons are legally required. Opacity becomes especially serious where automated or AI-assisted systems affect benefits, registration, licensing, taxation, migration, social support or other legally significant interests (Council of Europe, 2020; Greenstein, 2022; Langer, 2024).

Digital inequality. The risk of digital inequality requires particular attention. Not all persons possess the same level of digital literacy, technical access, stable connectivity, capacity to use electronic services or ability to understand digital procedures. Socially vulnerable groups, and persons located in the temporarily occupied territories of Ukraine, may find themselves in a situation in which formally accessible digital mechanisms in fact become a barrier. Digitalisation is thus capable not only of simplifying access to rights, but also of generating new forms of inequality in their realisation (Kouroutakis, 2024; da Rosa Lazarotto, 2025).

Expanded state supervision and control. Digital transformation expands the state's capacity to link datasets, infer behaviour and conduct large-scale monitoring. Such capacities may pursue legitimate public aims, but they also increase the risk of function creep, disproportionate surveillance and secondary uses of information unrelated to the purpose for which it was collected. A dignity-compatible digital state therefore requires purpose limitation, lawful data governance, proportionality and effective institutional oversight rather than an assumption that technical availability of data is equivalent to legal permission to use it.

Weakening of procedural protection. Simplification and automation can reduce administrative friction, but they must not eliminate notice, participation, correction of inaccurate data, reason-giving or access to review where those safeguards are required. Article 47 of the EU Charter provides an important European benchmark for effective remedy, while Article 22 GDPR illustrates the additional safeguards relevant to a defined category of solely automated decisions producing legal or similarly significant effects. The broader governance lesson is that digital convenience cannot be purchased by making the individual procedurally defenceless.

The digitalisation of the modern state is therefore a complex process that simultaneously opens new opportunities for improving the quality of public authority and generates new challenges to its legal and value-based nature.

7. A Two-Axis Governance Test For Digital Public Authority

For the purposes of this study, the digital transformation of public authority is defined as the institutional, procedural and technological reorganisation of how state authority is

exercised through digital systems, assessed simultaneously against effectiveness, compatibility with human dignity and the capacity to preserve legitimate and accountable public decision-making. This definition moves the analysis beyond the adoption of technology and focuses on the legal quality of the authority exercised through it.

The principal practical contribution is a two-axis governance test. It is not intended to replace a data-protection impact assessment, AI risk assessment, judicial proportionality test or sector-specific legality review. Rather, it provides a common public-law structure for asking whether a digital procedure remains human-centred and institutionally justified before deployment and during subsequent audit.

Table 1. Two-axis governance test for digitally mediated public authority

Assessment dimension	Primary axis	Risk indicator	Governance safeguard
Legal subjecthood and individual circumstances	Dignity	Person reduced to a fixed data profile; no route to correct or supplement relevant information	Correction mechanisms; capacity to submit individual circumstances; human reconsideration where legally required
Privacy and proportionality of data use	Dignity	Function creep, excessive data linkage or intrusive monitoring unrelated to the administrative purpose	Purpose limitation; data minimisation; proportionality review; access controls and oversight
Intelligibility and reasons	Legitimacy	Affected person receives an outcome but cannot identify its legal or factual basis	Meaningful notice; reason-giving appropriate to the decision; documentation of decisive inputs and rules
Contestability and remedy	Both	No realistic route to challenge an automated or AI-assisted outcome	Accessible human review; correction and appeal mechanisms; preservation of effective remedy
Equal accessibility	Legitimacy	Digital channel excludes persons because of disability, displacement, connectivity or limited digital literacy	Accessible design; assisted and alternative channels; monitoring of exclusion effects
Accountability and traceability	Legitimacy	Responsibility is shifted to software, a model or an external vendor	Named responsible authority; audit logs; procurement controls; human oversight and incident accountability

Note. The test is an authorial conceptual synthesis based on the dignity and legitimacy framework developed in this article; it should be applied together with sector-specific legal requirements.

Applied ex ante, the dignity axis asks whether the proposed system preserves the status, agency and individual circumstances of the person. Public bodies should identify what data representation the system will use, whether affected persons can correct or supplement that representation, whether the system creates disproportionate monitoring or profiling risks, and where human intervention must remain available. This assessment is especially important where automated processing can materially affect rights, entitlements or access to public services.

The legitimacy axis asks whether the authority exercised through the system remains intelligible, contestable, accessible and attributable to a responsible institution. Efficiency is relevant but not decisive. A system that shortens processing time while making errors practically unchallengeable, excluding non-digital users or obscuring responsibility may improve administrative throughput while weakening legitimate governance.

Applied together, the two axes generate a governance rule: the more consequential the digital intervention for an individual's legal position, the stronger the requirements of reason-giving, human review, data governance, accessibility and auditability should become. This proportional relationship also provides a bridge between general legal theory and contemporary risk-based AI governance. Human dignity identifies what public authority must not lose sight of; legitimacy identifies the procedural and institutional conditions under which digitally mediated authority remains justified.

8. Limitations And Scope Of Application

The proposed test is conceptual and normative. It does not measure public trust empirically, establish causal relationships between particular technologies and legitimacy, or determine the legality of a specific administrative system without reference to the law governing that system. Human dignity and legitimacy are contested concepts, and their concrete application will vary across legal orders and sectors.

The European instruments used in the analysis are comparative normative benchmarks rather than a claim of uniform direct applicability to Ukrainian public administration. Future research should therefore test the framework against concrete administrative domains, such as social benefits, taxation, licensing or digital identity, and should combine doctrinal analysis with user studies, administrative data and institutional audits. Such validation is necessary before the framework can be used as an empirical evaluation instrument.

9. Conclusions

The digital transformation of the modern state is not merely a technical renewal of administrative infrastructure. It changes how public authority sees the individual, how decisions are produced and explained, and how responsibility is allocated when public functions are mediated by data and automated systems. For that reason its success cannot be assessed by speed, convenience or cost reduction alone.

Human dignity operates as the substantive axis of assessment. It requires the digital state to preserve the person as a legal subject, to avoid treating a data profile as an exhaustive representation of the individual, and to retain procedures through which relevant circumstances can be presented, inaccurate information corrected and disproportionate data practices constrained. Dignity does not prohibit automation; it determines the conditions under which automation remains human-centred.

Legitimacy operates as the institutional and procedural axis. Digitally mediated authority remains justified where it is intelligible, contestable, accessible and attributable to a responsible public institution. A digital decision that cannot be effectively explained or challenged,

or a service that is formally available but practically inaccessible to significant groups, creates a legitimacy deficit even where the underlying technological system performs efficiently.

The two-axis governance test developed in this article translates those propositions into six operational dimensions: legal subjecthood and individual circumstances; proportional data use; intelligibility and reasons; contestability and remedy; equal accessibility; and accountability and traceability. Its scientific contribution lies in connecting the axiological category of dignity with the public-law category of legitimacy in a single assessment structure for digital administration.

The practical implication is a requirement of graduated safeguards. The more strongly a digital or AI-assisted procedure affects a person's legal position, the stronger the requirements for data governance, documentation, reason-giving, human review, accessibility and audit should be. This approach is compatible with the emerging European tendency toward risk-based AI regulation while retaining a specifically public-law focus on the justification of state authority.

Accordingly, sustainable digital governance should be understood as the capacity to preserve legitimate public authority through technological change. Digitalisation strengthens the state where it improves services while maintaining recognition of the person, effective legal protection and institutional responsibility. It undermines the state where technical efficiency is achieved through opacity, exclusion or procedural defenselessness. Future empirical and sector-specific research should test the proposed framework against real administrative systems and identify indicators capable of measuring how these safeguards operate in practice.

Funding

This research received no external funding.

Conflicts of Interest

The authors declare no conflicts of interest.

Ethics Statement

This theoretical-legal study used publicly available legal and scholarly sources and did not involve human participants, personal data collection or experimental procedures; institutional ethics approval was therefore not required.

Data Availability

No original datasets were generated or analysed. All legal and scholarly materials used in the study are identified in the reference list.

References

Charter of Fundamental Rights of the European Union. (2016). Official Journal of the European Union, C 202, 389–405.

Convention for the Protection of Human Rights and Fundamental Freedoms. (1950, November 4). Rome.

Council of Europe. (2020). Recommendation CM/Rec(2020)1 of the Committee of Ministers to member States on the human rights impacts of algorithmic systems.

Council of Europe. (2024). Framework Convention on Artificial Intelligence and Human Rights, Democracy and the Rule of Law (CETS No. 225). https://www.coe.int/en/web/conventions/full-list?module=treaty-detail&treatynum=225

da Rosa Lazarotto, B. (2025). The role of technology in citizens' right to good administration: Examining the impact of smart governments. In Public governance and emerging technologies: Values, trust and regulatory compliance (pp. 43–59). Springer. https://doi.org/10.1007/978-3-031-84748-6_3

De Gregorio, G. (2022). Digital constitutionalism: An introduction. In E. Celeste & G. De Gregorio (Eds.), Digital constitutionalism in Europe: Reframing rights and powers in the algorithmic society (pp. 1–37). Cambridge University Press. https://doi.org/10.1017/9781009071215.002

European Data Protection Board. (2018). Guidelines on automated individual decision-making and profiling for the purposes of Regulation 2016/679. https://www.edpb.europa.eu/documents/guideline/automated-decision-making-and-profiling_en

European Parliament and Council of the European Union. (2016). Regulation (EU) 2016/679 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 (General Data Protection Regulation). Official Journal of the European Union, L 119, 1–88. https://eur-lex.europa.eu/eli/reg/2016/679/oj

European Parliament and Council of the European Union. (2024). Regulation (EU) 2024/1689 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 (Artificial Intelligence Act). Official Journal of the European Union, L, 2024/1689. https://eur-lex.europa.eu/eli/reg/2024/1689/oj

Greenstein, S. (2022). Preserving the rule of law in the era of artificial intelligence (AI). Artificial Intelligence and Law, 30(3), 291–323. https://doi.org/10.1007/s10506-021-09294-4

Kouroutakis, A. E. (2024). Rule of law in the AI era: Addressing accountability and the digital divide. Discover Artificial Intelligence, 4, 115. https://doi.org/10.1007/s44163-024-00191-8

Langer, C. (2024). Decision-making power and responsibility in an automated administration. Discover Artificial Intelligence, 4, 59. https://doi.org/10.1007/s44163-024-00152-1

Røhl, U. B. U. (2023). Automated decision-making and good administration: Views from inside the government machinery. Government Information Quarterly, 40(4), 101864. https://doi.org/10.1016/j.giq.2023.101864

Protection Of Human Rights By The Notariat Under Martial Law: Digital Resilience, Legal Certainty And Directions For Reform

Anatolii Shevchenko
Department of Law, Public Management, and Administration
Zhytomyr Polytechnic State University
Zhytomyr, Ukraine
ORCID iD: 0000-0003-2663-9892
shevchenko2757@ukr.net

Myroslav Hryhorchuk
Department of Law and Law Enforcement
State University "Zhytomyr Polytechnic"
Zhytomyr, Ukraine
ORCID iD: 0000-0003-0523-030X
miroslavg@ukr.net

Ivanna Markelova
Kolomyia City Notarial District
Ivano-Frankivsk Region, Ukraine

Abstract.

This article examines the notariat as an institution of preventive human-rights protection under martial law in Ukraine, focusing on its growing dependence on digital public infrastructure. Using doctrinal legal analysis, analysis of legislation in force and conceptual synthesis of scholarship on wartime notarial practice and digitalisation, the study identifies four dimensions of institutional resilience: continuity of access to State registers, territorial accessibility of services, integrity and security of notarial data, and the legally controlled transition to the Unified State Electronic E-Notariat System. The article shows that wartime regulation has preserved important functions relating to property, inheritance, family and other civil rights, while access restrictions, territorial displacement, cyber risks and dependence on electronic registers can also obstruct the exercise of those rights. Particular attention is paid to extraterritoriality, services for displaced persons and citizens abroad, the protection and backup of notarial records, and the staged legal architecture of e-notariat. The article argues that e-notariat should not be equated with unrestricted remote notarisation: digital procedures require an explicit legal basis, reliable identification, preservation of notarial secrecy, access control, auditability and effective fallback mechanisms. A governance matrix is proposed using four criteria: legal continuity, accessibility, data resilience and procedural safeguards. The study concludes that resilient digital infrastructure is now part of the substantive capacity of the notariat to protect human rights and maintain legal certainty under prolonged emergency conditions.

Keywords: *notariat; human rights protection; martial law; e-notariat; digital resilience; legal certainty; sustainable governance.*

1.Introduction

The full-scale armed aggression against Ukraine and the continuing legal regime of martial law have created exceptional conditions for the functioning of institutions that protect private rights. The notariat is one of those institutions. Its role is distinct from judicial protection: a notary acts primarily before a dispute arises, certifying rights and legally significant facts, ensuring the authenticity of documents and transactions, and reducing uncertainty in civil circulation. During wartime, this preventive function becomes especially important because individuals may need to formalise inheritance, manage or dispose of property, issue powers of attorney, certify wills, confirm family or civil-law facts, and secure documentary evidence while simultaneously facing displacement, occupation, damaged infrastructure and disrupted access to public institutions.

The wartime problem is therefore not limited to whether notaries are formally authorised to act. It concerns whether the infrastructure required for the exercise of that authority remains available, secure and legally reliable. Modern Ukrainian notarial practice depends on access to State electronic registers, digital identification and information exchange, protected storage of data, functioning communication networks and reliable mechanisms for verifying the authority and identity of participants. A failure of that infrastructure can transform a technical disruption into a human-rights problem by preventing a person from exercising or proving a civil right.

This connection places the subject within the broader field of law, digital technologies and sustainable governance. The sustainability of a legal institution under emergency conditions depends on its ability to preserve its essential functions when ordinary territorial, administrative and technological arrangements are disrupted. For the notariat, this requires not merely more digital tools but a governance model that combines accessibility with security, continuity with legal certainty, and technological innovation with procedural safeguards.

The aim of the article is to determine how the notariat protects human rights under martial law, to identify the main legal and infrastructural risks affecting the continuity of notarial protection, and to formulate directions for reform based on digital resilience and sustainable governance. The article asks three questions: (1) which human-rights protection functions of the notariat become especially important during martial law; (2) how wartime regulation and digital dependence reshape access to those functions; and (3) which legal and organisational safeguards are necessary so that digitalisation strengthens, rather than weakens, legal certainty and accessibility.

2. Prior Research And The Research Gap

Ukrainian scholarship has examined the constitutional role of the notariat, its preventive function, the protection of property and inheritance rights, and the digitalisation of notarial procedures. Ivashkova (2024) emphasises the protective role of notaries in providing legally secure transactions and executive instruments. Bysaha (2023) and Marchenko (2020) discuss the increasing use of digital technologies in notarial activity, while Chyzhykov (2024)

highlights information-security and regulatory challenges. More recent work by Vdovichena (2025) addresses the preservation and relocation of notarial records under emergency conditions, and Zozulia et al. (2025) analyse the notariat as an institution for securing constitutional guarantees of rights and freedoms.

These strands of research are valuable but are often considered separately. Studies of wartime notarial practice tend to focus on emergency rules and accessibility; studies of digital notariat focus on technological modernisation; studies of human-rights protection focus on the preventive legal function. The remaining gap concerns their interdependence. Under wartime conditions, the notary can protect rights only if the digital and organisational infrastructure through which notarial authority is exercised remains available, trustworthy and legally controlled. This article therefore treats digital resilience not as a technical annex to notarial law but as part of the institutional capacity to secure human rights.

A second gap concerns the legal status of the e-notariat transition. Discussion in the literature sometimes uses „electronic notariat" as if it already meant general remote performance of notarial acts. The current regulatory architecture is more cautious and staged. The Unified State Electronic E-Notariat System has a legal framework, while the commencement of particular registers and software components is tied to separate technical-readiness decisions and official notices. This distinction is important because digitalisation of records, workflows and verification is not the same thing as legally unrestricted remote notarisation.

3. Materials And Methods

The study is doctrinal and conceptual. It analyses the Constitution of Ukraine, the Civil Code of Ukraine, the Law of Ukraine „On Notariat", wartime resolutions of the Cabinet of Ministers, subordinate regulation of notarial procedures, and the legal framework of the Unified State Electronic E-Notariat System. The regulatory material was checked against the official Legislation of Ukraine database and updated through 14 August 2026. In particular, the analysis takes account of Resolution No. 164 of 28 February 2022 in its current wartime form, the Procedure for the Performance of Notarial Acts by Notaries of Ukraine (Order No. 296/5), Resolution No. 1406 of 29 December 2023 on the E-Notariat System, and subsequent acts governing the staged integration of particular notarial registers.

The formal-legal method is used to identify the legal status, powers and safeguards relevant to notarial protection. Systemic analysis is used to examine how wartime restrictions, register access, territorial rules and data-protection requirements interact. A functional approach is used to assess the notariat not only through the formal list of notarial acts but through the human-rights functions those acts serve: prevention of disputes, preservation of property and inheritance rights, legal certainty, authentication and access to remedies. Conceptual synthesis is then used to formulate a governance matrix for resilient notarial services.

The study does not contain an empirical survey, statistical measurement or evaluation of the performance of individual notaries. Statements about institutional risks and reform priorities are normative conclusions derived from legislation and published scholarship. This limitation is important: the proposed governance model requires subsequent empiri-

cal testing using data on service accessibility, interruptions of register access, user experience, cyber incidents and cross-border notarial demand.

4. The Notariat As An Institution Of Preventive Human-Rights Protection

Articles 3 and 8 of the Constitution of Ukraine place the human being, human rights and the rule of law at the centre of State activity (Konstytutsiia Ukrainy, 1996). In the sphere of private-law relations, the notariat contributes to this constitutional orientation by giving legal authenticity to rights, facts and transactions and by preventing disputes before they require judicial resolution. Article 18 of the Civil Code recognises a specific mechanism of protection of civil rights by a notary, while the Law of Ukraine „On Notariat" defines the notary as a natural person authorised by the State to certify rights and legally significant facts and to perform other notarial acts (Tsyvilnyi kodeks Ukrainy, 2003; Pro notariat, 1993).

The protective function of the notariat should therefore be understood more broadly than the performance of individual technical procedures. It includes at least five functions: safeguarding the realisation and proof of property rights; securing inheritance rights and continuity of succession; protecting family and other private-law interests; preventing conflicts through verification and authentication; and maintaining legal certainty in civil circulation. Unlike a court, which usually intervenes after a dispute or violation has materialised, the notary generally acts ex ante, reducing the probability that uncertainty, fraud, defective form or an evidential gap will later undermine a person's legal position.

This preventive function becomes more visible under martial law. War produces sudden changes in residence, family circumstances, access to property, documentary control and the territorial availability of institutions. In such circumstances, the inability to execute a will, establish an inheritance file, obtain a power of attorney, certify a transaction or retrieve legally significant information may have consequences that persist long after the immediate emergency. Vdovichena (2025) therefore rightly links the preservation of notarial records with the preservation of property and personal rights.

At the same time, the notary's protective role is not equivalent to the exercise of judicial power or general public administration. The notary is authorised by the State and performs legally defined public functions, but operates within a distinctive preventive-justice model. This distinction matters for digital transformation: technology should support the notary's legally structured professional judgment and verification duties rather than replace them with an automated administrative process.

5. Wartime Transformation Of Notarial Services

5.1. Emergency regulation and access to State registers

After the introduction of martial law, the Cabinet of Ministers adopted Resolution No. 164 of 28 February 2022, „Certain Issues of the Notariat under Martial Law". The resolution has been amended repeatedly as the security environment and territorial classification of hostilities have changed; the official legislative database records a current revision from 22

May 2026 following Resolution No. 635 of 20 May 2026 (Kabinet Ministriv Ukrainy, 2022, 2026b). The continuing amendment of the instrument demonstrates that wartime notarial regulation is not a one-time emergency response but an adaptive legal regime.

The emergency framework has combined two competing objectives. The first is continuity: individuals must retain access to legally significant services even when ordinary institutions are displaced or unavailable. The second is security: State registers and property-related procedures cannot remain open in the same manner where there is a high risk of unauthorised access, coercion, document abuse, occupation or cyberattack. Restrictions on access to registers and on specific registration or property operations must therefore be understood as risk-control measures, but they also create direct barriers to the exercise of private rights when they last too long or when alternative procedures are unavailable.

The legal-policy task is consequently to apply the principle of proportionality to digital restrictions. A restriction that is justified by an immediate security threat should be linked to the nature of that threat, periodically reviewed, and accompanied where possible by alternative procedures. Otherwise, information security can itself become a source of legal insecurity.

5.2. Territorial accessibility, displaced persons and the extraterritorial principle

The displacement of individuals and notaries, the temporary occupation of territory and the destruction or interruption of local institutional capacity make territorial accessibility one of the principal wartime challenges. The Procedure for the Performance of Notarial Acts by Notaries of Ukraine provides as a general rule that notarial acts may be performed by any notary throughout Ukraine, subject to statutory exceptions (Ministerstvo yustytsii Ukrainy, 2012). This general extraterritorial logic is especially important in wartime because a person's need for a notarial act may be disconnected from the person's place of permanent residence or from the location in which an earlier notarial file was created.

Extraterritoriality, however, should not be described as unlimited. Certain acts remain tied to statutory territorial or procedural requirements, and the practical ability to act depends on access to relevant registers and records. The proper reform direction is therefore not simply to „broaden extraterritoriality" in the abstract, but to identify which remaining territorial restrictions are substantively necessary, which can be removed without creating fraud or jurisdictional risks, and which require secure electronic access to records before they can be relaxed.

Internally displaced persons are particularly affected by these constraints. For them, the accessibility of notarial services is connected not only with physical proximity but also with documentary continuity: the ability of a notary in a new region to verify information, open or continue an inheritance matter where legally permissible, and access secure records. This makes interoperability and continuity of State registers part of equality of access to legal protection.

5.3. Citizens abroad and the consular dimension

Large-scale displacement outside Ukraine has also increased the importance of consular notarial functions. Article 38 of the Law of Ukraine „On Notariat" assigns a range of notarial acts to authorised consular officials. The practical significance of this channel lies in enabling citizens abroad to execute legally significant acts without returning to Ukraine solely for notarial purposes. The effectiveness of the mechanism nevertheless depends on consistent access to relevant information systems, clear division of competence between consular officials and notaries in Ukraine, and reliable recognition and transmission of the resulting records.

The emerging e-notariat architecture reinforces this cross-border dimension. For example, the 2026 regulation of the Inheritance Register expressly provides for access by authorised officials of consular institutions and embassies within the E-Notariat System (Kabinet Ministriv Ukrainy, 2026a). At the cut-off date of this study, however, Resolution No. 52 of 21 January 2026 had not yet entered fully into force because its operative commencement depends on an official Ministry of Justice notice regarding the functioning of the relevant software. This is a useful illustration of why planned digital interoperability must be distinguished from functionality already available in practice.

5.4. Information security, data integrity and continuity of records

Notarial protection depends on the integrity, confidentiality and availability of data. The classic paper archive remains important, but the modern notariat also relies on electronic registers containing information about powers of attorney, inheritance, encumbrances, real rights, civil-status acts and other legally significant data. Wartime cyberattacks, power disruptions, communication failures and physical damage to infrastructure create risks not only of temporary unavailability but also of loss, corruption or unauthorised disclosure of information.

Three dimensions of information security have direct legal significance. Confidentiality is connected with notarial secrecy and personal-data protection. Integrity ensures that the legal system can rely on the authenticity and completeness of registry information. Availability determines whether a person can actually exercise a right when the relevant information is needed. A resilient notarial system must therefore treat backup, redundancy, disaster recovery, access logging and secure authentication as components of legal protection rather than purely technical IT functions.

Resolution No. 475 of 21 April 2025 is relevant to the broader emergency-management framework because it amends the general evacuation procedure, but it should not be treated as creating a dedicated legal regime for the relocation of notarial offices or archives. The more precise conclusion is that evacuation and preservation of notarial records must be coordinated with general emergency-management rules while also requiring sector-specific procedures for chain of custody, access rights, confidentiality, restoration and evidentiary integrity of notarial records.

5.5. E-notariat as a staged legal and technological transition

The most important structural development in the digital transformation of the Ukrainian notariat is the Unified State Electronic E-Notariat System. Resolution No. 1406 of 29 December 2023 establishes the general legal and organisational framework of the system and its components (Kabinet Ministriv Ukrainy, 2023). The system is designed to automate notarial activity, integrate information exchange, support registers within the Ministry of Justice system, and enable verification and access mechanisms while preserving notarial secrecy.

It is essential, however, to distinguish the existence of the regulatory framework from the commencement of every technological component. The 2025 and 2026 acts dealing with particular registers continue to tie full operation to official notices on the availability or commencement of the necessary software. Resolution No. 52 of 2026 concerning the Inheritance Register is a particularly clear example: most of its operative provisions take effect only after the Ministry of Justice publishes notice that the relevant E-Notariat software is functioning (Kabinet Ministriv Ukrainy, 2026a). The transition is therefore phased.

This staged model has an important human-rights implication. E-notariat should not be equated with a general right or possibility to perform all notarial acts remotely. Digital records, electronic identifiers, register integration and online verification can increase resilience and accessibility, but remote performance of a notarial act raises separate questions of identity assurance, free and informed will, capacity, coercion, confidentiality, territorial competence, evidence and professional liability. Each remote or partially remote procedure therefore requires an explicit legal basis and safeguards appropriate to the legal consequences of the act.

For sustainable governance, the correct objective is not maximal digitalisation but controlled digital resilience: the ability to continue lawful notarial services through secure digital infrastructure while preserving human professional responsibility and maintaining fallback procedures when electronic channels fail.

6. A Governance Framework For Resilient Notarial Protection

The analysis above suggests that reform should be organised around institutional functions rather than around isolated technologies. The central question is whether a proposed measure improves the capacity of the notariat to protect rights under stress without introducing disproportionate new risks. Four criteria are especially important: legal continuity, accessibility, data resilience and procedural safeguards.

Legal continuity means that emergency rules, digital systems and territorial arrangements should preserve the legal validity and traceability of notarial acts across disruptions. Accessibility means that displaced persons, persons in territories affected by hostilities, persons with limited digital access and citizens abroad should have realistic routes to obtain necessary services. Data resilience means that records must remain confidential, accurate, recoverable and available. Procedural safeguards mean that digitalisation must preserve the notary's verification duties, professional independence, legal responsibility and the pos-

sibility for the person to understand and challenge an adverse legal consequence where appropriate.

Table 1. Governance matrix for resilient notarial services under martial law

Governance issue	Current legal / institutional position	Human-rights risk	Recommended safeguard
Access to State registers	Emergency rules permit security-based restrictions and differentiated access; the regime remains adaptive.	A person may be unable to prove or exercise a right when registry access is interrupted.	Proportional, reviewable restrictions; documented fallback procedures; prioritised restoration of rights-critical registers.
Territorial accessibility	A general extraterritorial principle operates subject to statutory exceptions and technical access conditions.	Displaced persons may face delay or practical exclusion from inheritance, property or representation procedures.	Review residual territorial limits; enable secure cross-regional file continuity; publish clear routing rules for exceptional cases.
Data and archive resilience	Notarial practice depends on electronic registers and protected records; general emergency evacuation rules also apply.	Loss, corruption or disclosure of records can create long-term legal uncertainty and privacy harm.	Multi-level backup, disaster recovery, integrity checks, access logging, sector-specific chain-of-custody procedures and periodic resilience testing.
Citizens abroad	Consular officials perform defined notarial acts; digital register integration is being developed.	Fragmented access and delays may prevent timely formalisation of rights.	Secure consular access to relevant registers, clear competence rules, interoperable record transmission and user guidance.
E-notariat transition	Resolution No. 1406 establishes the system; particular components enter operation in stages and may depend on official technical-readiness notices.	Treating planned functionality as already available can create false expectations; over-automation can weaken safeguards.	Explicit legal basis for each digital procedure, strong identification, least-privilege access, auditability, notarial secrecy, human professional control and non-digital contingency routes.

Note. The matrix is an authorial synthesis based on the legislation and scholarship analysed in this article. It is intended as a policy-evaluation tool rather than as a statement that all listed measures are already implemented.

6.1. Priority directions for reform

1. Complete the staged introduction of e-notariat while preserving the distinction between digital workflow and legally authorised remote notarisation. The Ministry of Justice should publish clear implementation milestones, legal status of each component, and contingency rules for periods of technical unavailability.

2. Establish sector-specific continuity and disaster-recovery standards for notarial data and records. These standards should define redundancy, backup frequency, restoration priorities, access control, incident reporting and preservation of evidentiary integrity.

3. Review territorial restrictions through a rights-and-risk lens. Restrictions that remain necessary for fraud prevention or jurisdictional coherence should be retained; those that survive only because records are not interoperable should be reconsidered as digital continuity improves.

4. Strengthen cross-border accessibility through consular integration. Citizens abroad should receive clear information on which acts may be performed by consular officials, which require action by a notary in Ukraine, and how electronic records move between the two systems.

5. Introduce periodic accessibility and resilience assessment. Sustainable governance requires evidence on service interruption, regional access, restoration times, user barriers and cyber incidents. Without such evidence, the success of digital reform cannot be evaluated only by the number of services placed online.

7. Conclusions

Under martial law, the notariat remains an important part of the national mechanism for protecting civil rights and legal certainty. Its preventive function is especially significant in relation to property, inheritance, family and representation matters, because wartime displacement and institutional disruption increase the cost of legal uncertainty and make delayed formalisation of rights more dangerous.

The principal conclusion of this study is that the effectiveness of notarial protection now depends on the resilience of the digital and organisational infrastructure through which the notary acts. Access to State registers, secure identification, continuity of electronic records, protected archives and cross-regional information exchange are not merely administrative conveniences. They determine whether a person can obtain a legally effective notarial act at the moment it is needed.

The wartime regulatory response has demonstrated considerable adaptability, but it also reveals a structural tension between security and accessibility. Register restrictions and territorial limitations may be justified by concrete security risks, yet they should remain proportionate, reviewable and accompanied by viable alternatives. The extraterritorial principle is valuable precisely because it reduces the dependence of legal protection on a person's pre-war place of residence, but it must operate together with reliable access to records and clear procedural rules.

The development of the Unified State Electronic E-Notariat System is a central element of future reform. Its legal architecture shows that implementation is staged and technologically conditional. Consequently, e-notariat should not be described as if unrestricted remote notarisation were already available. The appropriate model is one of controlled digital resilience in which electronic infrastructure supports, rather than replaces, the notary's professional verification and responsibility.

For sustainable governance, five priorities follow: completion of legally transparent e-notariat implementation; sector-specific data-continuity and disaster-recovery standards; evidence-based review of territorial restrictions; strengthened integration with consular services; and regular assessment of accessibility and infrastructure resilience. These measures would connect digital transformation with the core purpose of the notariat: preserving legal certainty and enabling individuals to realise and protect their rights even under prolonged emergency conditions.

The scientific contribution of the article lies in reframing wartime notarial reform as a

problem of institutional and digital resilience. The proposed governance matrix links technical continuity with substantive human-rights protection and provides a basis for future empirical evaluation. Further research should test the model using regional service data, interviews with notaries and users, measures of register downtime and restoration, and comparative analysis of digital notarial systems in European jurisdictions.

Funding

This research received no external funding.

Conflicts of Interest

The authors declare no conflicts of interest.

Ethics Statement

Not applicable. The study is doctrinal and uses publicly available legislation and scholarly sources; it does not involve human participants, personal data collection or experimental procedures.

Data Availability

No original dataset was generated or analysed. The legal materials discussed in the article are publicly available through official Ukrainian legislative databases.

Declaration of Generative AI Use

Generative AI tools were used for language editing and structural revision during the preparation of this manuscript. The authors reviewed and verified all substantive statements and references and take full responsibility for the final text.

References

Bysaha, Yu. Yu. (2023). Tsyfrovi tekhnolohii v notariati: Sutnist ta osoblyvosti [Digital technologies in the notariat: Essence and features]. Naukovi Visnyk Uzhhorodskoho Natsionalnoho Universytetu. Seriia: Pravo [Scientific Bulletin of Uzhhorod National University. Series: Law], 78(2), 11–16. https://doi.org/10.24144/2307-3322.2023.78.2.1 [in Ukrainian]

Chyzhykov, O. O. (2024). Pravovi aspekty rehuliuvannia notarialnoi diialnosti v umovakh tsyfrovoi transformatsii [Legal aspects of regulating notarial activity under conditions of digital transformation]. Akademichni Vizii [Academic Visions], (38). https://doi.org/10.5281/zenodo.14506910 [in Ukrainian]

Ivashkova, T. O. (2024). Mistse ta rol advokatury i notariatu v systemi zakhystu prav viiskovosluzhbovtsiv [The place and role of the bar and the notariat in the system of protection of the rights of military personnel]. Analitychno-Porivnialne Pravoznavstvo [Analytical and Comparative Jurisprudence]. https://doi.org/10.24144/2788-6018.2024.01.21 [in Ukrainian]

Kabinet Ministriv Ukrainy [Cabinet of Ministers of Ukraine]. (2022, February 28). Deiaki pytannia notariatu v umovakh voiennoho stanu [Certain issues of the notariat under martial law] (Resolution No. 164; current

revision from May 22, 2026). https://zakon.rada.gov.ua/laws/show/164-2022-%D0%BF [in Ukrainian]
Kabinet Ministriv Ukrainy [Cabinet of Ministers of Ukraine]. (2023, December 29). Deiaki pytannia funktsionuvannia Yedynoi derzhavnoi elektronnoi systemy e-notariatu [Certain issues of functioning of the Unified State Electronic E-Notariat System] (Resolution No. 1406). https://zakon.rada.gov.ua/laws/show/1406-2023-%D0%BF [in Ukrainian]
Kabinet Ministriv Ukrainy [Cabinet of Ministers of Ukraine]. (2025, April 21). Pro vnesennia zmin v dodatok 1 do Poriadku provedennia evakuatsii u razi zahrozy vynyknennia abo vynyknennia nadzvychainykh sytuatsii [On amendments to Annex 1 to the Procedure for conducting evacuation in the event of a threat of, or occurrence of, emergency situations] (Resolution No. 475). https://zakon.rada.gov.ua/laws/show/475-2025-%D0%BF [in Ukrainian]
Kabinet Ministriv Ukrainy [Cabinet of Ministers of Ukraine]. (2026a, January 21). Deiaki pytannia funktsionuvannia Spadkovoho reiestru [Certain issues of functioning of the Inheritance Register] (Resolution No. 52). https://zakon.rada.gov.ua/laws/show/52-2026-%D0%BF [in Ukrainian]
Kabinet Ministriv Ukrainy [Cabinet of Ministers of Ukraine]. (2026b, May 20). Pro vnesennia do deiakykh aktiv Kabinetu Ministriv Ukrainy zmin shchodo zabezpechennia yedynoho pidkhodu do zastosuvannia pereliku terytorii, na yakykh vedutsia (velysia) boiovi dii abo tymchasovo okupovanykh Rosiiskoiu Federatsiieiu [Amendments to certain acts of the Cabinet of Ministers concerning the unified application of the list of territories affected by hostilities or temporary occupation] (Resolution No. 635). https://zakon.rada.gov.ua/laws/show/635-2026-%D0%BF [in Ukrainian]
Konstytutsiia Ukrainy [Constitution of Ukraine]. (1996). Vidomosti Verkhovnoi Rady Ukrainy, (30), Art. 141. https://zakon.rada.gov.ua/laws/show/254%D0%BA/96-%D0%B2%D1%80 [in Ukrainian]
Marchenko, V. M. (2020). Okremi pytannia vprovadzhennia v Ukraini systemy E-notariatu [Selected issues of introducing the e-notariat system in Ukraine]. Prykarpatskyi Yurydychnyi Visnyk [Precarpathian Legal Bulletin], 1(30), 42–46. https://doi.org/10.32837/pyuv.v0i1(30).513 [in Ukrainian]
Ministerstvo yustytsii Ukrainy [Ministry of Justice of Ukraine]. (2012, February 22). Pro zatverdzhennia Poriadku vchynennia notarialnykh dii notariusamy Ukrainy [On approval of the Procedure for the performance of notarial acts by notaries of Ukraine] (Order No. 296/5; current revision from June 14, 2025). https://zakon.rada.gov.ua/laws/show/z0282-12 [in Ukrainian]
Pro notariat: Zakon Ukrainy [On Notariat: Law of Ukraine]. (1993, September 2). No. 3425-XII (current revision from April 24, 2026). https://zakon.rada.gov.ua/laws/show/3425-12 [in Ukrainian]
Tsyvilnyi kodeks Ukrainy [Civil Code of Ukraine]. (2003, January 16). No. 435-IV. https://zakon.rada.gov.ua/laws/show/435-15 [in Ukrainian]
Vdovichena, L. (2025). Vplyv relokatsii na pravovyi rezhym peremishchennia dokumentiv notarialnoho dilovodstva v umovakh voiennoho stanu [The impact of relocation on the legal regime for the transfer of notarial records under martial law]. In Zakarpatski pravovi chytannia. Relokatsiia v umovakh ekstraordynarnykh pravovykh rezhymiv: Materialy XVII Mizhnarodnoi naukovo-praktychnoi konferentsii, m. Uzhhorod, 25–26 kvitnia 2025 r. [Transcarpathian legal readings. Relocation under extraordinary legal regimes: Proceedings of the 17th International Scientific and Practical Conference, Uzhhorod, 25–26 April 2025] (pp. 57–60). Liha-Pres. https://doi.org/10.36059/978-966-397-493-4-12 [in Ukrainian]
Zozulia, O. I., Holovashchenko, O. S., & Novikov, Ye. A. (2025). Notariat yak instytut zabezpechennia konstytutsiinykh harantii zakhystu prav i svobod liudyny [The notariat as an institution for ensuring constitutional guarantees of the protection of human rights and freedoms]. Akademichni Vizii [Academic Visions], (50), 1–11. [in Ukrainian]

Perepolkin, D. S., & Perepolkin, S. M. (2026). Classification of non-governmental organisations in modern legal scholarship: Towards a multidimensional model for digital governance. ESS Conference Series Social Science and Humanities, 1(1). https://doi.org/10.54658/esscssh.2026.1.1.04

Classification Of Non-Governmental Organisations In Modern Legal Scholarship: Towards A Multidimensional Model For Digital Governance

Danylo S. Perepolkin
Department of Administrative and Criminal Law
Oles Honchar Dnipro National University
Dnipro, Ukraine
ORCID iD: 0000-0001-5821-1810
danil6875@gmail.com

Serhii M. Perepolkin
Department of International Law
University of Customs and Finance
Dnipro, Ukraine
ORCID iD: 0000-0003-2914-5898
psm-13@ukr.net

Abstract.

The classification of non-governmental organisations (NGOs) is not merely a taxonomic exercise: the categories used by legal scholarship, public registers, statistical systems and funding platforms shape how civil society is described and governed. This article re-examines Ukrainian scholarly classifications of NGOs against the current Law of Ukraine „On Public Associations" and international statistical standards. Using doctrinal legal analysis, comparative classification analysis and conceptual modelling, it identifies three recurring problems in legacy typologies: reliance on repealed statutory criteria; conflation of legal status, membership and beneficiary orientation; and treatment of funding sources as a direct proxy for organisational autonomy. Particular attention is paid to the transition from the International Classification of Non-profit Organizations (ICNPO) to the United Nations International Classification of Non-profit and Third Sector Organizations (ICNP/TSO). The article proposes a multidimensional model based on four analytical axes: primary functional/economic activity, operational reach, beneficiary or constituency orientation, and resource/funding profile. Legal attributes, including legal-person status and all-Ukrainian status under Ukrainian law, are treated as a separate legal overlay rather than as substitutes for analytical classification. The model is further translated into a machine-readable metadata structure suitable for digital public registers, statistical systems and funding portals. Its practical value lies in enabling more accurate comparison and governance while avoiding the assumption that any single category determines an organisation's independence, legitimacy or regulatory treatment.

Keywords: *non-governmental organisations (NGOs); civil society; NGO classification; ICNP/TSO; digital governance; public associations.*

1. Introduction

Non-governmental organisations are heterogeneous institutions. They differ in legal form, scale, field of activity, constituency, funding structure, relationship with public authorities and degree of formalisation. This diversity has generated numerous classifications in legal and social-science scholarship, but no single scheme can serve every purpose equally

well. A category that is useful for legal registration may be too coarse for statistical analysis; a functional classification may be well suited to national accounts but unable to describe who benefits from an organisation's work; and a funding classification may reveal patterns of resource dependence without determining the organisation's actual decision-making autonomy. Recent scholarship illustrates this functional diversity in fields as different as participation in United Nations human-rights reporting and disaster-risk reduction (Doyle et al., 2026; Vogel et al., 2026).

The problem is particularly visible in Ukraine because part of the earlier scholarly literature was constructed under the former Law of Ukraine „On Associations of Citizens". Some criteria derived directly from that statute ceased to have the same legal meaning when the Law of Ukraine „On Public Associations" entered into force. At the same time, the current law did not eliminate territorial questions from legal analysis. It establishes freedom to choose the territory of activity and retains a specific all-Ukrainian status for associations that satisfy statutory requirements. Consequently, the legal category of status must be distinguished from the empirical scale at which an organisation actually operates (Verkhovna Rada of Ukraine, 2012).

International standards have also evolved. The ICNPO developed by Salamon and Anheier (1996) provided a widely used functional classification for nonprofit institutions. In 2018, however, the United Nations published the Satellite Account on Non-profit and Related Institutions and Volunteer Work and introduced the International Classification of Non-profit and Third Sector Organizations (ICNP/TSO) as the first revision of ICNPO. The revised system preserves backward compatibility but expands the coverage and reorganises categories for contemporary statistical use (United Nations, 2018). A modern legal study of NGO classification should therefore treat ICNPO as a foundational historical model rather than as the latest international standard.

This issue also belongs to the agenda of digital and sustainable governance. Public registers, open-data portals, grant-management systems and civil-society dashboards increasingly require structured metadata. If legal status, functional activity, beneficiary orientation and funding profile are collapsed into one label, digital systems reproduce conceptual errors at scale. Conversely, a transparent multidimensional classification can improve interoperability, statistical visibility and policy analysis while preserving legal certainty and organisational self-government.

The aim of this article is to critically reassess selected approaches to the classification of NGOs in Ukrainian and international scholarship and to formulate a multidimensional model suitable for contemporary legal analysis and digital governance. The objectives are to: (1) separate repealed statutory criteria from still-relevant analytical criteria; (2) clarify the place of territorial scope and all-Ukrainian status under current Ukrainian law; (3) update the discussion from ICNPO to ICNP/TSO; (4) distinguish membership from beneficiary or constituency orientation; (5) reconceptualise funding as a resource-dependence dimension rather than a direct measure of autonomy; and (6) translate the resulting model into a practical metadata structure for digital governance.

2. Materials And Methods

The study is doctrinal and conceptual rather than empirical. It combines formal-legal analysis, comparative classification analysis and conceptual modelling. The formal-legal component examines the current Law of Ukraine „On Public Associations" and the transition from the repealed Law of Ukraine „On Associations of Citizens". The purpose is not to provide a complete account of the regulation of every type of civil-society organisation, but to determine which classification criteria retain legal relevance for public associations under the current statutory framework.

The comparative component examines selected Ukrainian scholarly classifications, particularly those proposed by Mendzhul (2009), Haieva (2017) and Kravchuk (2007), alongside the international functional tradition represented by ICNPO and the updated ICNP/TSO. Additional literature on nonprofit resource dependence is used to evaluate the claim that funding source can be treated as a proxy for organisational autonomy (Arvidson & Linde, 2021; Banks et al., 2015).

The conceptual-modelling stage evaluates each criterion according to four questions: what characteristic does it measure; whether the categories are sufficiently distinct to be useful; whether the criterion is legal, descriptive or analytical in nature; and whether it can be represented consistently in a digital register or statistical system. On that basis, a four-axis analytical model is proposed together with a separate legal overlay. No survey, interview, database coding exercise or quantitative measurement of NGOs was undertaken. The proposed model therefore requires empirical testing in future research.

3. Results And Discussion

3.1 Legacy Ukrainian classifications and the problem of statutory change

Mendzhul (2009) classified NGOs using criteria that included membership composition, field of activity, territorial scope, method of membership registration, method of legalisation, purpose of establishment and number of members. The historical value of this approach is clear: it captured the institutional environment existing under the Law of Ukraine „On Associations of Citizens". Its direct use today, however, requires qualification. Criteria tied to the former procedures of legalisation and fixed or non-fixed membership registration cannot simply be reproduced as current legal categories after the repeal of that statute. The former statute on which part of that logic rested is now repealed (Verkhovna Rada of Ukraine, 1992).

The territorial criterion requires a more precise correction. It would be inaccurate to state that territorial status disappeared entirely under the current law. Article 3 of the Law of Ukraine „On Public Associations" recognises free choice of the territory of activity, while Article 19 retains an all-Ukrainian status that may be confirmed by a registered public association meeting the statutory conditions (Verkhovna Rada of Ukraine, 2012). Accordingly, two different concepts must be separated. The first is legal status, including the specific statutory category of all-Ukrainian status. The second is operational reach: the geographic area

in which an organisation actually conducts sustained activities. Local, regional, national and transnational reach remain useful analytical descriptors, but they should not be presented as a complete list of current statutory statuses.

A similar distinction is needed for membership. Membership is a legally and organisationally relevant attribute of many associations, but it does not necessarily identify the group that benefits from the organisation's work. A professional association may primarily serve its members; a youth organisation may involve adult organisers while directing programmes towards young people; a humanitarian NGO may have a small professional membership but serve a large external population. Classification should therefore record membership structure where legally relevant while using a separate beneficiary or constituency dimension to describe social orientation.

The public-benefit/private-benefit distinction also requires moderation rather than wholesale rejection. Member-serving and mutual-benefit organisations exist and can be analytically distinguished from organisations whose principal activities are directed to the wider public or external beneficiary groups. The difficulty lies in treating the distinction as an undefined binary. A more useful model asks who the principal beneficiaries or constituencies are and allows mixed orientations, rather than presuming that every targeted activity is either purely public or purely private.

Sector-specific classifications remain useful when their limits are stated explicitly. For example, Vakhovych and Smolych (2023) classify Ukrainian business-support NGOs through legal and functional characteristics and assess organisational, coalition and sectoral capacity. Such models are valuable for a defined field but should not automatically be generalised to the entire civil-society sector.

3.2 From ICNPO to ICNP/TSO: updating the international reference point

The International Classification of Non-profit Organizations developed by Salamon and Anheier (1996) became an influential framework because it organised nonprofit institutions principally by field of activity. Its functional logic remains valuable, and its residual category for organisations not elsewhere classified recognised that civil society continuously produces new organisational forms.

For current international comparison, however, the 2018 United Nations Satellite Account is the more appropriate reference point. It describes ICNP/TSO as the first revision of ICNPO and recommends it for classification of nonprofit and related third-sector institutions. ICNP/TSO retains the basic structure of ICNPO while introducing new fields, reconfiguring groups and improving correspondence with the International Standard Industrial Classification. It classifies institutions by economic activity and provides hierarchical sections, groups and subgroups; the numeral 9 is reserved for catch-all categories not elsewhere classified (United Nations, 2018).

This update has two implications for legal scholarship. First, a contemporary study should not present the 1996 ICNPO categories as if they were the latest international statistical standard. Second, the logic of ICNP/TSO supports the use of a primary functional or economic-activity axis, but it does not by itself answer legal questions about status, constituency,

governance relations or funding. The international statistical classification and the proposed legal-governance model therefore perform complementary rather than competing functions.

3.3 Evaluating recurrent classification criteria

Table 1. Evaluation of recurrent NGO classification criteria in contemporary legal analysis

Criterion	Current value	Main problem	Recommended treatment
Legalisation / membership-registration method	Low as a current classification axis	Derived from repealed statutory procedures	Use only historically; replace with current legal attributes
Legal form and legal-person status	High legal relevance	Often confused with social or functional type	Record as a separate legal overlay
All-Ukrainian status	High where applicable	May be incorrectly treated as the same as operational reach	Record as a statutory legal attribute under current law
Field / functional activity	High	Many NGOs are multifunctional	Use primary activity plus secondary activity tags; align where possible with ICNP/TSO
Territorial scope	High analytically	Can be mistaken for statutory status	Use as operational reach: local, regional, national, transnational
Membership composition	Medium	Does not necessarily identify beneficiaries	Keep as organisational metadata; do not substitute for beneficiary orientation
Beneficiary / constituency orientation	High	Categories may overlap	Allow multiple or mixed beneficiary groups
Number of members	Low without thresholds	Arbitrary boundaries between “mass” and “ordinary” organisations	Avoid as a universal typology unless operational thresholds are defined
Funding source	High as a resource-profile dimension	Does not mechanically determine autonomy	Use to analyse dependence, accountability and diversification; never as an autonomy score
Relationship with the state	Potentially high	Relationships change across programmes and over time	Treat as contextual/relational metadata rather than a fixed organisational type

Note. Authors’ synthesis based on the current Ukrainian legal framework, the reviewed scholarship and international classification standards.

3.4 The proposed multidimensional classification model

The analysis supports a model that separates legal attributes from analytical classification. Legal attributes answer the question „what is the organisation in law?”; analytical dimensions answer questions about what it does, where it works, whom it principally serves and how it is resourced. This separation is important because a public association may have the same legal form as another association while differing substantially in function, reach, constituency and funding structure.

The proposed model contains four complementary analytical axes. None of them is inten-

ded to produce a single permanent label. Rather, together they create a profile that can be updated when an organisation changes programmes, territory or funding structure.

Table 2. Proposed multidimensional classification model for NGOs

Analytical axis	Classification question	Illustrative categories	Primary governance use
1. Primary functional / economic activity	What does the organisation principally do?	Education; health; social services; culture; environmental protection; advocacy; professional services; philanthropy; other/not elsewhere classified	Statistics; sector mapping; consultation; programme matching; comparison with ICNP/TSO
2. Operational reach	At what geographic scale are activities actually delivered?	Local; regional; national; transnational/international; multi-level	Coverage analysis; regional policy; service-access mapping; cross-border cooperation
3. Beneficiary / constituency orientation	Who principally benefits from or is represented by the organisation?	General public/community; defined social group; vulnerable groups; members/profession; institutional beneficiaries; mixed	Targeting analysis; inclusion monitoring; representation and accountability assessment
4. Resource / funding profile	What resource streams sustain the organisation?	Grant/donor-dominant; donations/member contributions; contracts or earned income; philanthropic/endowment; mixed/diversified	Resource-dependence analysis; transparency design; financial resilience and funding-platform metadata

Note. The categories are illustrative rather than exhaustive. The model is designed to permit multiple secondary tags and periodic updating.

3.5 Functional orientation as the primary comparative axis

Functional orientation should remain the primary axis for broad comparison because it answers the most basic substantive question: what activity does the organisation perform? This is also the dimension most directly comparable with ICNP/TSO. For organisations with multiple programmes, the model should distinguish a primary activity from secondary activities. The primary activity may be identified by the activity that accounts for the largest share of expenditure, personnel, programme volume or another transparent indicator appropriate to the dataset. Secondary tags prevent the loss of information that would result from forcing multifunctional NGOs into a single exclusive category.

The category „not elsewhere classified" should be retained, but its role should be understood correctly. It is not evidence of conceptual failure; it is a controlled residual category that allows the system to absorb new forms of civic activity without immediately redesigning the entire classification. This is consistent with the updated ICNP/TSO structure, which reserves catch-all codes for activities not otherwise classified (United Nations, 2018).

3.6 Operational reach: analytical scale versus legal status

Operational reach should describe actual activity rather than simply replicate a historical legal status. A local organisation may participate in a national coalition; a national organisation may implement only a limited set of programmes in selected regions; and a Ukrainian

organisation may participate in cross-border networks without acquiring a distinct territorial status under domestic law. The classification should therefore permit both a primary reach category and, where needed, multiple territorial tags.

This approach is compatible with the current Ukrainian principle of free choice of territory for operation. It also prevents a legal error: all-Ukrainian status under Article 19 is not synonymous with the analytical category of national operational reach. The former is a statutory attribute confirmed under defined conditions; the latter is an empirical description of organisational activity. Digital public registers and scholarly datasets should store these as separate fields.

3.7 Beneficiaries, constituencies and membership

The beneficiary axis is the principal refinement proposed in place of older uses of „membership composition" as a proxy for social orientation. It distinguishes internal organisational structure from external social function. Beneficiary categories may include the general public, a geographic community, children and young people, internally displaced persons, veterans, persons with disabilities, professional groups, enterprises, other civil-society organisations or mixed populations.

This dimension must remain flexible because beneficiaries and represented constituencies are not always identical. Advocacy organisations may represent a constituency without providing direct services; professional associations may serve members while also producing public benefits; grant-making foundations may support other organisations rather than individuals. The model therefore uses the broader expression beneficiary/constituency orientation and permits multiple categories where necessary.

3.8 Resource and funding profile: from deterministic claims to resource-dependence analysis

Funding is analytically important, but the original proposition that a funding source directly determines an NGO's institutional autonomy is too strong. Resource-dependence scholarship shows a more complex relationship. External funding can create control mechanisms, reporting obligations and incentives for mission adaptation, but autonomy depends on the terms of the funding relationship, the organisation's bargaining power, diversification, alternative resources and governance capacity (Arvidson & Linde, 2021; Banks et al., 2015).

Accordingly, the model replaces an autonomy ranking with a resource/funding profile. A grant-dominant organisation may face donor conditions but still preserve substantial discretion; an organisation financed by many small donations may enjoy diversified income yet remain dependent on reputational expectations; a contractor may be constrained by procurement specifications; and a mixed model may reduce concentration risk without eliminating external accountability. The correct inference is therefore that resource structure can shape patterns of dependence and accountability, not that one source is inherently more autonomous than another.

This distinction is also important for regulatory fairness. Funding information may legitimately support transparency, financial-risk analysis or programme eligibility, but it should not automatically trigger assumptions about legitimacy, independence or political alignment. A classification system should describe the resource structure first and leave evaluative conclusions to a separate, evidence-based assessment.

3.9 From legal typology to digital governance metadata

The practical significance of the proposed model becomes clearer when it is translated into digital governance. Contemporary public administration increasingly relies on electronic registers, open-data portals, digital grant platforms and automated statistical reporting. A digital system needs fields that are stable enough to compare organisations but flexible enough to reflect organisational change. For that reason, the classification should be implemented as structured metadata rather than as one exclusive NGO type.

The legal overlay should be stored separately from analytical dimensions. For Ukrainian public associations, relevant legal fields include organisational form, legal-person status and, where applicable, confirmed all-Ukrainian status. Analytical fields should then describe activity, reach, beneficiaries and resource profile. Each field should have a source or evidence basis, a date of last update and, where possible, controlled vocabularies aligned with international standards.

Table 3. Minimum metadata structure for a digital NGO register or analytical database

Metadata field	Purpose	Design rule
Legal form / legal-person status	Records the organisation's current legal position	Mandatory legal field; do not infer social function from it
All-Ukrainian status, if applicable	Records the specific statutory status under Ukrainian law	Separate boolean/status field; do not use as a substitute for operational reach
Primary activity code	Supports comparison and statistics	Prefer alignment with ICNP/TSO or a mapped national code
Secondary activity codes	Preserves multifunctionality	Allow multiple values
Operational reach	Describes actual geographic scale	Use controlled categories and update when programmes change
Beneficiary / constituency tags	Describes social orientation	Allow multiple values; distinguish from membership
Resource / funding profile	Supports transparency and dependence analysis	Use descriptive categories; never calculate autonomy automatically
Provenance and update date	Supports accountability and data quality	Record source of information and date of verification

Note. A machine-readable implementation should preserve source provenance and allow updates rather than treating classification as permanent.

3.10 Governance implications and safeguards

A multidimensional classification can improve sustainable governance in at least four ways. First, it increases statistical visibility by enabling public authorities and researchers to distinguish fields of activity without discarding legal attributes. Second, it supports better policy targeting because beneficiary and territorial data can be analysed independently. Third, it improves interoperability between public registers, statistical systems and funding platforms when shared vocabularies are used. Fourth, it reduces the need for repeated statutory redesign when new forms of civic activity emerge, because secondary tags and residual categories can accommodate organisational change.

At the same time, classification creates governance risks. A dataset may become discriminatory if funding source is treated as proof of dependence or political alignment; a single activity code may erase multifunctionality; beneficiary categories may disclose sensitive information about vulnerable groups; and automated systems may convert descriptive metadata into eligibility decisions without adequate review. For these reasons, digital implementation should follow proportionality, data-minimisation and contestability principles. Organisations should be able to correct inaccurate metadata, and consequential decisions should not rely on one classification field in isolation.

The model therefore does not propose a new statutory hierarchy of NGOs. Its purpose is narrower and more defensible: to provide a legal-analytical framework that distinguishes what the law formally recognises from the descriptive dimensions required for contemporary governance, statistics and funding analysis.

4. Limitations And Directions For Further Research

The study has several limitations. First, it is conceptual and doctrinal; the proposed model has not been tested against a large administrative dataset of Ukrainian NGOs. Second, the term NGO covers organisations governed by different legal regimes, while the formal-legal analysis here focuses primarily on public associations regulated by the Law of Ukraine „On Public Associations". Charitable organisations, religious organisations, trade unions and other institutional forms may require additional legal overlays. Third, classification is purpose-dependent: a system designed for national statistics may need different detail from a grant-management platform or academic database.

Future research should therefore test the model on real registry and organisational data, develop coding rules for multifunctional organisations, examine correspondence between Ukrainian administrative classifications and ICNP/TSO, and evaluate whether beneficiary and resource-profile fields can be collected without imposing disproportionate reporting burdens. A separate empirical question is whether funding diversification correlates with autonomy or resilience in the Ukrainian civil-society sector; this should be measured rather than assumed.

5. Conclusions

The classification of NGOs remains a relevant problem of legal scholarship because the categories used to describe civil society have practical consequences for registration, statistics, policy analysis and funding. The review demonstrates that legacy classifications cannot be transferred mechanically into the current legal environment. Criteria derived from repealed legalisation procedures should be treated historically, while current legal attributes must be read directly from the Law of Ukraine „On Public Associations".

The study makes three principal corrections to the earlier classification logic. First, territorial analysis must distinguish operational reach from statutory status: the current Ukrainian law combines freedom to choose the territory of activity with a specific all-Ukrainian status. Second, membership should not be used as a substitute for beneficiary or constituency orientation. Third, source of funding should be treated as a resource-dependence dimension rather than as a direct measure of organisational autonomy.

The proposed model therefore combines four analytical axes: primary functional/economic activity, operational reach, beneficiary/constituency orientation, and resource/funding profile. Legal form, legal-person status and all-Ukrainian status operate as a separate legal overlay. This design preserves the original aim of constructing an integrated classification while avoiding the conceptual problem of mixing legal status with descriptive social characteristics.

A further contribution is the update from ICNPO to the United Nations ICNP/TSO framework. ICNPO remains historically important, but contemporary international statistical practice provides a revised classification with expanded fields, hierarchical coding and residual categories. Aligning the functional axis of the proposed model with ICNP/TSO increases its comparative value without requiring legal scholarship to adopt a purely statistical approach.

Finally, the model is suited to digital governance because it can be represented as machine-readable metadata rather than a single fixed organisational label. Such a structure can support public registers, civil-society statistics and funding platforms while maintaining clear boundaries between descriptive classification and legal judgement. The model should therefore be understood not as a new hierarchy of civil society, but as an open analytical architecture for more accurate, interoperable and sustainable governance of information about NGOs.

Funding

This research received no external funding.

Conflicts of Interest

The authors declare no conflicts of interest.

Data Availability

No new empirical dataset was created or analysed. The study is based on publicly available legislation, international classification documents and published scholarship cited in the References.

Ethics Statement

The study did not involve human participants, personal data collection or experimental procedures; therefore, research ethics approval was not required.

References

Arvidson, M., & Linde, S. (2021). Control and autonomy: Resource dependence relations and non-profit organizations. Journal of Organizational Ethnography, 10(2), 207–221. https://doi.org/10.1108/JOE-05-2020-0021

Banks, N., Hulme, D., & Edwards, M. (2015). NGOs, states, and donors revisited: Still too close for comfort? World Development, 66, 707–718. https://doi.org/10.1016/j.worlddev.2014.09.028

Doyle, D. M., Higgins, N., & Murphy, M. (2026). Non-governmental organisations, the United Nations Human Rights System and access to education in Europe. International Journal of Discrimination and the Law, 26(1), 6–38. https://doi.org/10.1177/13582291251340937

Haieva, N. P. (2017). Classification of non-governmental organizations: Theoretical approaches. Chasopys Kyivskoho universytetu prava [Journal of Kyiv University of Law], (3), 83–87. [in Ukrainian]

Kravchuk, V. M. (2007). Some approaches to the classification of non-governmental organizations in Ukraine. Vybory ta demokratiia [Elections and Democracy], 1(11), 1–12. [in Ukrainian]

Mendzhul, M. V. (2009). Types of non-governmental organizations in Ukraine. Problemy tsyvilnoho ta pidpryiemnytskoho prava v Ukraini [Problems of Civil and Entrepreneurial Law in Ukraine], (1), 184–188. [in Ukrainian]

Salamon, L. M., & Anheier, H. K. (1996). The International Classification of Nonprofit Organizations: ICNPO--Revision 1 (Working Papers of the Johns Hopkins Comparative Nonprofit Sector Project, No. 19). Johns Hopkins Institute for Policy Studies.

United Nations. (2018). Satellite account on non-profit and related institutions and volunteer work (Handbook of National Accounting, Studies in Methods, Series F, No. 91, Rev. 1). United Nations Department of Economic and Social Affairs, Statistics Division. https://unstats.un.org/unsd/nationalaccount/docs/UN_TSE_HB_FNL_web.pdf

Vakhovych, I., & Smolych, D. (2023). Definition and classification of non-governmental business support organizations in Ukraine in the context of liberalization and entrepreneurship stimulation. Financial and Credit Activity Problems of Theory and Practice, 6(53), 417–431. https://doi.org/10.55643/fcaptp.6.53.2023.4262

Verkhovna Rada of Ukraine. (1992). Law of Ukraine 'On Associations of Citizens' No. 2460-XII (repealed). https://zakon.rada.gov.ua/laws/show/2460-12 [in Ukrainian]

Verkhovna Rada of Ukraine. (2012). Law of Ukraine 'On Public Associations' No. 4572-VI (current version). https://zakon.rada.gov.ua/laws/show/4572-17 [in Ukrainian]

Vogel, A., Heinkel, S.-B., & Kraas, F. (2026). Between hope and hype: Civil society organisations in disaster risk reduction – A systematic global review and future research agenda. International Journal of Disaster Risk Reduction, 143, Article 106258. https://doi.org/10.1016/j.ijdrr.2026.106258

Muliarevych, O. (2026). Cybersecurity and privacy risks of AI assistants in academic institutions: A risk classification and governance framework. ESS Conference Series Social Science and Humanities, 1(1). https://doi.org/10.54658/esscssh.2026.1.1.05

Cybersecurity And Privacy Risks Of Ai Assistants In Academic Institutions: A Risk Classification And Governance Framework

Oleksandr Muliarevych
Lviv Polytechnic National University
Lviv, Ukraine
ORCID iD: 0000-0002-4644-7962
oleksandr.v.muliarevych@lpnu.ua

Abstract.
Large language model-based AI assistants are rapidly becoming part of academic work, supporting students, teachers, researchers, and administrators in writing, summarisation, translation, coding, and information retrieval. However, their adoption in academic institutions creates cybersecurity and privacy risks that extend beyond the commonly discussed problem of academic integrity. Using a qualitative literature review and conceptual synthesis of recent research on generative AI in higher education, LLM security, privacy protection, and institutional AI governance, this article classifies the main risks of AI assistants into four groups: data-related risks, model-related risks, application and integration risks, and human and governance risks. It shows that universities process sensitive categories of information — student records, grades, unpublished research, examination materials, administrative documents — which makes uncontrolled AI use a significant institutional risk. Special attention is given to prompt injection, sensitive data disclosure, insecure integrations, overreliance on AI outputs, and policy fragmentation. The article proposes an Academic AI Security and Privacy Governance Framework based on six layers: governance and policy; data classification and privacy; secure AI architecture; prompt and output security; human oversight and AI literacy; and monitoring, audit, and continuous improvement. Because each layer translates external legal and regulatory requirements — data-protection obligations, accountability, auditability — into institutional rules and technical controls, the framework is offered as a contribution to the governance of digital technology in education as much as to information security practice. The study concludes that AI assistants should be treated as security- and privacy-sensitive socio-technical systems requiring coordinated institutional governance.

Keywords: *AI assistants; large language models; AI governance; data protection; higher education; prompt injection.*

1.Introduction

Artificial intelligence assistants based on large language models (LLMs) are rapidly becoming part of academic work. Students use them for explanation, summarisation, writing support, translation, coding, and examination preparation. Teachers use them to prepare educational materials, generate examples, assess drafts, and support communication with students. Researchers use them for literature exploration, editing, coding, data interpretation, and administrative work. AI assistants are therefore no longer optional productivity tools. In many academic institutions they are becoming an informal layer between users and knowledge, educational content, research data, and institutional processes.

The adoption of AI assistants in universities, however, creates risks that go beyond academic integrity. The most visible discussion is usually focused on plagiarism, cheating, and authorship. These issues are important, but they represent only one part of the problem. AI assistants also introduce cybersecurity and privacy risks, because they process unstructured prompts, uploaded files, personal data, source code, research materials, student records, and institutional information. When such tools are integrated with learning management systems (LMS), email, cloud storage, research repositories, or administrative services, the potential risk surface becomes significantly broader. This is especially relevant for academic institutions, because universities process many sensitive categories of information: student grades, personal identifiers, disability accommodations, research data, unpublished manuscripts, examination materials, grant proposals, employment data, and sometimes commercially or nationally sensitive research results. UNESCO guidance on generative AI in education and research warns that public access to generative AI developed faster than regulatory and institutional safeguards, leaving many institutions insufficiently prepared to address data privacy, human oversight, and responsible use (Miao & Holmes, 2023).

From a cybersecurity perspective, LLM-based assistants differ from traditional educational software because natural-language input can act simultaneously as content and as an instruction to the model. The OWASP Top 10 for LLM and Generative AI Applications 2025 identifies prompt injection, sensitive information disclosure, supply-chain weaknesses, data and model poisoning, improper output handling, excessive agency, system-prompt leakage, vector and embedding weaknesses, misinformation, and unbounded consumption as major risk classes (OWASP Foundation, 2025). In universities, these risks become especially consequential when an assistant processes institutional documents, student data, research outputs or untrusted external content, or when it is connected to retrieval systems and action-taking tools.

The privacy dimension is equally important. A report prepared for the European Data Protection Board under its Support Pool of Experts programme emphasises that LLM-based systems require systematic identification, assessment, and mitigation of privacy and data-protection risks, and it develops one of its worked use cases around an LLM system for monitoring and supporting student progress — showing that LLM privacy risks are not abstract technical concerns but concrete institutional governance problems (European Data Protection Board, 2025). The problem is therefore socio-technical. It is not enough to ask whether AI assistants are useful for learning or whether they improve productivity. Academic institutions must also ask what data enters these systems, who controls the processing, whether outputs can leak sensitive information, how users verify generated content, how institutional policies define acceptable use, and how technical controls limit damage in case of misuse.

Posed in those terms, the question is not primarily one of information-security engineering but of institutional governance. Universities routinely process personal data and may process special categories of personal data; they also make decisions affecting admission, assessment, progression, employment and discipline. The precise legal role of an institution, vendor or platform depends on jurisdiction, deployment architecture, contractual allocation of responsibilities and the relevant data flow. The governance problem is therefore to alloca-

te responsibility, identify the lawful and proportionate conditions for processing, preserve meaningful human oversight in consequential decisions, and make AI-assisted operations sufficiently traceable to support accountability and contestability. The six-layer framework developed below translates those concerns into institutional policy, privacy, architecture, security, literacy and audit controls. Read in this way, an institutional AI policy is not merely an IT procedure but part of the organisation's internal governance of digital technology.

This article analyses the cybersecurity and privacy risks of AI assistants in academic institutions by combining recent literature from education, cybersecurity, privacy law, AI governance, and LLM security. Its main goal is to connect two areas that are usually discussed separately: university AI policy and technical LLM security. The article argues that universities need a complete risk-management approach combining AI literacy, data protection, secure system design, vendor checks, clear university policies, and human oversight. Without this integration, universities risk treating AI assistants only as a threat to academic honesty while ignoring their risks as systems that process sensitive data and support decisions. The contribution of this paper is practical and integrative. It does not consist in inventing basic security controls such as data minimisation, least privilege, prompt filtering, or human oversight; these come from well-established frameworks and guidance produced by OWASP, NIST, the EDPB, and UNESCO. The original contribution lies in adapting them specifically for universities through four outputs:

(1) a four-part classification of AI-assistant risks in academia;

(2) a mapping of risk sources, affected university data, and institutional impact;

(3) a six-layer Academic AI Security and Privacy Governance Framework;

(4) practical instruments including a data-classification model, secure architecture patterns, an implementation roadmap, and a prioritised risk matrix.

By connecting existing security standards with real university workflows, the article offers a model that academic institutions can apply directly.

2. Literature Review

2.1. Generative AI adoption and the institutional policy gap in higher education

The first major research stream concerns the rapid adoption of generative AI in higher education and the institutional difficulty of responding to it. UNESCO's guidance for generative AI in education and research provides one of the most influential policy-level contributions. It frames generative AI as a technology with educational potential but also with significant risks related to human agency, privacy, inclusion, ethics, and institutional readiness (Miao & Holmes, 2023). The guidance matters for this article because it does not treat AI as a purely pedagogical innovation; it positions AI adoption as a governance challenge requiring regulation, institutional policy, and data protection.

A related UNESCO document, the AI competency framework for teachers, argues that teachers need specific knowledge, skills, and values to use AI responsibly, and notes that many countries have not yet clearly defined the AI competencies teachers require, which leaves educators without sufficient guidance in a fast-changing technological environment (Miao

& Cukurova, 2024). This is relevant because many cybersecurity and privacy failures in academic AI use arise not from technical weakness but from users not knowing what data may safely be entered into an AI assistant, what outputs require verification, and which tools are approved for institutional use.

Several empirical and policy-analysis studies show that universities are still developing their response to generative AI. Moorhouse et al. (2023) analysed guidelines from top-ranked universities and showed that institutions were forced to create or modify assessment guidance quickly after the emergence of ChatGPT; their work is useful because it shows that early university responses were often focused on assessment, academic honesty, and acceptable use, while broader security and privacy controls were less central. An et al. (2025) studied generative AI guidelines and policies in higher education institutions across teaching, learning, research, and administration, supporting the argument that AI assistants are becoming cross-functional institutional tools requiring more systematic governance than classroom-level rules. Wilson (2025) and Wu et al. (2024) similarly show that policy development differs significantly between institutions and that effective governance requires coordination between academic, technical, administrative, and legal units.

The Ukrainian context is also important. Borodiyenko et al. (2025) investigated opportunities and risks of AI-based applications in research in Ukrainian universities. Their study shows that AI adoption in Ukrainian academic environments is shaped by expert opinion, media narratives, and scientific literature, while institutional readiness and risk awareness remain developing areas. This provides regional relevance for the present article and supports the need for practical governance models.

2.2. LLM SECURITY RISKS AND THEIR RELEVANCE TO ACADEMIC INSTITUTIONS

The second research stream comes from cybersecurity and LLM application security. The OWASP 2025 taxonomy is particularly useful because it reflects a shift from early plugin-centred descriptions to a broader application lifecycle: prompt injection and sensitive-information disclosure remain central, while improper output handling, excessive agency, system-prompt leakage, vector/embedding weaknesses, misinformation and unbounded consumption capture risks that become more important as AI assistants acquire retrieval and action capabilities (OWASP Foundation, 2025).

Prompt injection deserves special attention. The UK National Cyber Security Centre argues that it is not equivalent to classical SQL injection, because LLMs do not enforce a boundary between data and instructions, so the risk can be reduced but not eliminated in the deterministic way that traditional injection vulnerabilities can (National Cyber Security Centre, 2025b); the mechanism and its academic implications are examined in Section 4.4. The point is especially important for universities, because academic workflows are rich in untrusted text: AI assistants may process student submissions, web pages, PDF files, research papers, emails, forum posts, and external datasets, any of which may carry hidden instructions. If the assistant has access to institutional systems, the consequences may include data exposure, incorrect grading support, leakage of internal documents, or unauthorised actions.

Technical surveys reinforce this conclusion. Yao et al. (2024) review LLM security and privacy from the perspective of beneficial uses, harmful uses, and inherent vulnerabilities. Das et al. (2025) provide a broader survey of LLM security and privacy challenges, including jailbreaking, prompt injection, data poisoning, and leakage of personally identifiable information. These studies support the claim that AI assistants should be assessed as cybersecurity-relevant systems, especially when connected to institutional data and services.

The NCSC's broader assessment of AI and cyber threats warns that AI will increase the effectiveness and accessibility of cyber operations, including social engineering, intrusion activity, and exploitation workflows (National Cyber Security Centre, 2025a). Academic institutions are especially exposed to this trend, because they often combine open networks, diverse user groups, decentralised IT practices, bring-your-own-device usage, international collaboration, and valuable research data.

2.3. Privacy and data-protection risks of AI assistants

The third research stream focuses on privacy and data protection. This is central to academic institutions because they manage large amounts of personal and confidential information. The European Data Protection Board's 2025 report on LLM privacy risks provides a risk-management methodology and discusses collection, inference, retrieval-augmented generation, feedback loops and emerging agentic systems. It also makes an important governance distinction: LLM-specific mitigation guidance can support data protection by design and security of processing, but it does not replace a Data Protection Impact Assessment where one is legally required (European Data Protection Board, 2025). Opinion 28/2024 further cautions against assuming that an AI model trained on personal data is automatically anonymous (European Data Protection Board, 2024).

Technical privacy surveys provide additional depth. Neel and Chang (2024) review privacy issues in LLMs, including training-time privacy, inference-time leakage, model deletion, and red-teaming. Miranda et al. (2025) survey privacy-preserving approaches for LLMs, including anonymisation, differential privacy, and machine unlearning. These works help explain why privacy risk is not limited to what users intentionally share in prompts: it can also arise from memorisation, logs, embeddings, and downstream integrations.

Empirical research shows that users are increasingly aware of these risks. Xu et al. (2025) investigated learners' perceptions of data privacy when using AI language models and found concerns about data leakage, unethical data exploitation, and algorithmic bias, while also indicating that students may not know how AI systems process or retain their data. Xue et al. (2025) compared AI privacy concerns in higher education through news coverage in China and Western countries, showing that AI privacy in education is a global concern.

Dahabiyeh et al. (2026) studied privacy awareness in the context of ChatGPT use among university students and showed that privacy awareness and perceptions of data handling influence users' intention to use generative AI. Taken together, these findings suggest that institutional AI adoption must include transparency and user education, not only access to tools.

2.4. Academic integrity, research integrity, and institutional risk

Academic integrity remains one of the most visible concerns in generative AI adoption. Bittle and El-Gayar (2025) provide a systematic review of generative AI and academic integrity in higher education, identifying both opportunities and risks, including improved engagement and efficiency but also increased risk of academic dishonesty and the need for digital literacy, detection tools, and institutional policy.

Chang et al. (2024) approach ChatGPT in higher education from a risk-management perspective, discussing academic integrity, critical thinking, and workforce readiness, and showing that institutions need to move beyond simple prohibition or acceptance. Their approach is useful here because cybersecurity and privacy should likewise be treated as risk--management problems rather than isolated technical issues.

Research integrity is another important dimension. The European Commission's living guidelines on the responsible use of generative AI in research emphasise reliability, honesty, respect, accountability, transparency, privacy, confidentiality, and protection of intellectual property (European Commission, Directorate-General for Research and Innovation, 2026). This is directly connected to cybersecurity and privacy, because a researcher may upload unpublished data to an external AI assistant, use AI-generated text containing fabricated references, or rely on generated summaries of sensitive documents.

Academic integrity and cybersecurity should therefore not be treated as separate domains. In AI-assisted academic work they overlap: a hallucinated citation may damage research quality; an uploaded confidential dataset may violate privacy rules; an AI-generated examination question stored in a third-party system may create assessment-security issues; and an unverified AI recommendation may affect student outcomes.

2.5. Human factors and educator perspectives

The fifth research stream concerns human factors. Even strong technical controls will not be sufficient if users do not understand AI risks or if institutional rules are unclear. Pikhart and Al-Obaydi (2025) studied educators' subjective perspectives on the risks of AI in higher education; their findings highlight concerns about privacy, academic integrity, data misuse, unauthorised access, plagiarism, and reduced critical thinking. UNESCO's AI competency framework for teachers supports this point from the competency side, arguing that educators need competencies spanning a human-centred mindset, ethics, AI foundations, pedagogy, and professional development (Miao & Cukurova, 2024).

For the purposes of this article this means that cybersecurity and privacy training should not be confined to IT security departments. Teachers and researchers also need practical AI security literacy: how to classify data, when not to use public AI tools, how to verify outputs, how to disclose AI use, and how to recognise unsafe AI integrations.

2.6. Governance frameworks and the remaining research gap

Recent governance-oriented sources provide useful foundations for institutional AI risk management. The NIST Generative Artificial Intelligence Profile (NIST AI 600-1) adapts the AI Risk Management Framework to generative AI and organises risk work around the functions Govern, Map, Measure and Manage (Autio et al., 2024). It is cross-sectoral rather than education-specific, which makes institutional adaptation necessary. UNESCO contributes human-centred and competency-oriented guidance for education (Miao & Holmes, 2023; Miao & Cukurova, 2024), while the EDPB adds privacy-specific governance requirements. The EU AI Act adds a further regulatory benchmark: certain systems used in education and vocational training can be classified as high-risk because of their potential effect on access, learning outcomes, level assessment or test monitoring (European Parliament & Council of the European Union, 2024). These sources are complementary rather than interchangeable: security taxonomies identify technical risk, privacy guidance structures data-protection analysis, and institutional governance determines how controls are assigned and enforced.

The reviewed literature shows a clear gap. Higher-education studies usually focus on academic integrity, assessment, policy development, and educator or student perceptions. Technical LLM-security studies focus on prompt injection, data leakage, model vulnerabilities, and adversarial misuse.

Privacy and legal sources focus on data protection, governance, and compliance. Fewer works combine these perspectives into a practical institutional model for academic AI assistants. This article addresses that gap by framing AI assistants in academic institutions as socio-technical systems that are simultaneously learning tools, data-processing systems, cybersecurity interfaces, and governance challenges. Its regulatory and technical foundations are drawn from existing sources; what is proposed here is the domain-specific synthesis set out in Section 1 — the classification, its alignment with the academic domain, and the integrated implementation model.

3. Methodology

3.1. Research design and source selection strategy

This study uses a qualitative literature review and conceptual synthesis approach to analyse the cybersecurity and privacy risks of AI assistants in academic institutions. Its purpose is not to test a single technical vulnerability or to measure the performance of a specific AI tool. The aim is to synthesise recent academic, technical, legal, and policy-oriented literature in order to identify the main categories of risk that arise when LLM-based AI assistants are used in universities and other academic environments. A literature-based methodology is appropriate because the problem is interdisciplinary, spanning the technical, educational, legal, and governance literatures reviewed in Section 2; the study combines those perspectives into a unified institutional risk model.

The methodology follows three stages:

1. identification of relevant sources;
2. thematic analysis of the selected literature; and

3. synthesis of the findings into a structured cybersecurity and privacy risk framework for academic institutions.

The literature search prioritised publications and institutional documents issued between 2020 and August 2026, with earlier sources retained where they provided enduring conceptual foundations. The search covered four categories: peer-reviewed studies on generative AI in higher education; systematic reviews and surveys on LLM security and privacy; primary policy and regulatory documents; and technical risk frameworks and cybersecurity guidance. Search combinations included terms such as „generative AI higher education privacy", „AI assistants academic institutions cybersecurity", „LLM prompt injection education", „AI governance universities", „student data privacy AI language models" and „LLM sensitive information disclosure". Because the study is a qualitative integrative review rather than a systematic review or meta-analysis, the search was designed for interdisciplinary conceptual coverage and source triangulation, not exhaustive bibliometric retrieval.

Sources were included if they directly analysed generative AI, ChatGPT, or LLM-based tools in higher education; discussed cybersecurity risks of LLM applications; analysed privacy or data-protection risks of AI systems; proposed governance, policy, or risk-management approaches for responsible AI use; provided evidence about student, teacher, or institutional perceptions of AI-related risks; or offered a framework applicable to academic institutions. Sources were excluded if they focused only on technical model performance without discussing security, privacy, or institutional use; addressed AI in education only from a narrow pedagogical perspective without risk analysis; discussed cybersecurity in general without connection to AI, LLMs, or data governance; were opinion pieces without clear analytical, empirical, technical, or policy value; or were outdated in relation to current generative AI development.

3.2. Analytical approach and risk-classification logic

The selected sources were analysed using thematic coding, focusing on repeated risk categories, institutional challenges, and mitigation strategies across the literature. In the first stage, sources were grouped into four broad domains: AI in higher education, LLM security, privacy and data protection, and governance and risk management. In the second stage, these domains were compared in order to identify overlapping issues. Academic-integrity literature, for example, often discusses student misuse of AI tools, while cybersecurity literature discusses prompt injection and manipulation; these topics appear different, but both involve user behaviour, system trust, verification, and control of AI-generated outputs. Similarly, privacy literature discusses personal data leakage while institutional-policy literature discusses acceptable use and governance, and the two overlap as soon as students or staff upload confidential materials to external AI assistants. In the third stage, the recurring themes were synthesised into risk categories relevant to academic institutions: input data leakage, sensitive information disclosure in outputs, prompt injection, insecure integration with institutional systems, vendor data-processing risks, academic and research integrity risks, student privacy and surveillance risks, overreliance on AI-generated outputs, and policy fragmentation.

The risk categories were then classified along three dimensions: source of risk, affected asset, and institutional impact. The source of risk describes whether a risk originates in user behaviour, model behaviour, system integration, vendor data practices, or institutional policy gaps. The affected asset describes what may be harmed, including student data, research data, examination materials, unpublished manuscripts, institutional documents, learning management systems, staff accounts, academic reputation, and trust in educational processes. The institutional impact describes the possible consequence, such as privacy violations, data leakage, academic misconduct, reputational damage, regulatory non-compliance, compromised research integrity, unauthorised system actions, or reduced quality of decision-making.

3.3. Ethical considerations and limitations

This study is based on publicly available academic publications, policy documents, technical frameworks, and regulatory guidance. It does not involve human participants, interviews, surveys, experiments with students, or the processing of personal data, and no formal ethics committee approval was therefore required. The subject of the article is nevertheless ethically sensitive, because it concerns student privacy, research confidentiality, responsible AI use, and institutional accountability.

The methodology has several limitations. First, the study rests on literature review and conceptual synthesis rather than on empirical measurement; the framework proposed below has not been implemented or evaluated in a live institutional setting. Second, the field is developing rapidly, and new AI models, regulations, institutional policies, and attack techniques appear frequently. Third, the selected literature reflects mainly English-language sources and internationally visible publications. Fourth, cybersecurity and privacy risks differ depending on the technical deployment model — a public chatbot, an enterprise AI assistant, a locally hosted model, or a retrieval-augmented university knowledge assistant each present a different risk profile.

4. Results And Discussion: Classification Of Cybersecurity And Privacy Risks

4.1. General classification logic

The analysis of recent literature shows that the cybersecurity and privacy risks of AI assistants in academic institutions are multidimensional. They cannot be reduced to plagiarism, cheating, or inaccurate answers. AI assistants create a broader socio-technical risk landscape, because they interact with user prompts, uploaded files, institutional documents, student data, research materials, external services, and sometimes internal university systems.

The risks are accordingly classified across four connected dimensions: data-related risks, model-related risks, application and integration risks, and human and governance risks. Figure 1 presents the classification. It is broadly consistent with current OWASP 2025 risk categories while deliberately reorganising them around university assets, workflows and

responsibilities rather than reproducing a generic technical taxonomy (OWASP Foundation, 2025).

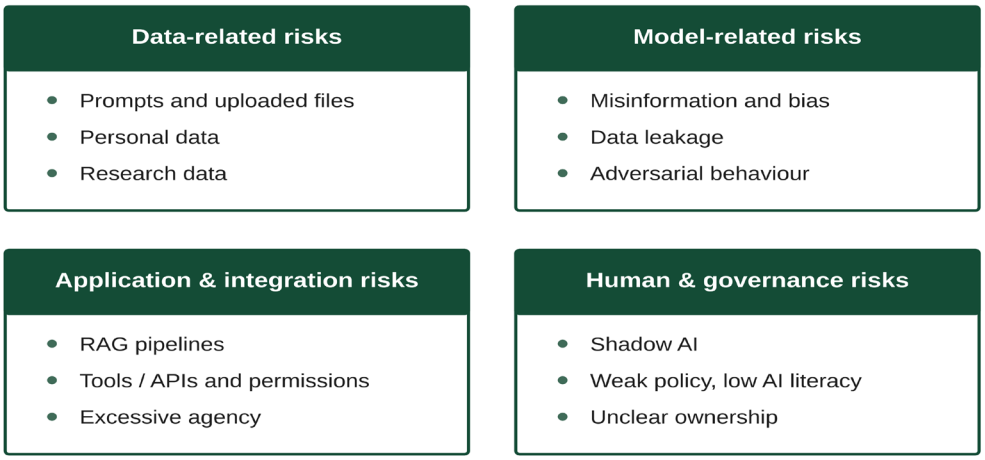


Figure 1. Classification of cybersecurity and privacy risks of AI assistants in academic institutions

4.2. Data-related risks

Data-related risks appear when students, teachers, researchers, or administrative staff enter sensitive information into AI assistants. This may include student names, grades, disability accommodations, unpublished research, examination materials, internal meeting notes, grant proposals, or confidential university documents. These risks are especially important when public or third-party AI systems are used without institutional control. Table 1 summarises the principal data-related risks, with academic examples and possible institutional impacts.

Table 1. Data-related risks of AI assistants in academic institutions

Risk category	Description	Academic example	Possible impact
Input data leakage	Sensitive data is entered into an external AI assistant.	A lecturer uploads student essays with names and grades to a public chatbot.	Privacy violation, GDPR risk, reputational damage.
Research confidentiality loss	Unpublished research materials are processed by third-party AI tools.	A researcher uploads a draft grant proposal or experimental dataset.	Loss of novelty, exposure of intellectual property, breach of project agreement.
Examination material exposure	Examination questions or assessment rubrics are entered into AI tools.	A teacher asks an AI assistant to improve examination questions.	Assessment compromise, unfair student advantage.
Data retention uncertainty	Users do not know whether prompts or files are stored or reused.	Staff use free AI tools for administrative summaries.	Lack of control over institutional information.
Model memorisation risk	Personal or confidential data may be memorised or reproduced.	Fine-tuning is performed on student records without sufficient safeguards.	Data-protection violation, future leakage.
Weak data classification	The institution has no clear rule on what data may be used with AI.	Different departments follow different informal practices.	Inconsistent compliance and unmanaged risk.

A report published by the European Data Protection Board on LLM privacy risks is directly relevant here, because it proposes a risk-management methodology for LLM systems and includes a use case on monitoring and supporting student progress (European Data Protection Board, 2025). This confirms that educational LLM systems are not merely pedagogical tools but also privacy-sensitive data-processing systems.

The most important practical conclusion is that academic institutions need a clear data-classification model for AI use: not all data should be treated equally. The categories in Table 2 are a proposed institutional control model rather than legal classifications. Their purpose is to translate sensitivity, contractual obligations and potential harm into operational rules for approved tools, access control and escalation. Responsibility for enforcement should be allocated to appropriate institutional roles — for example data owners, information-security teams, legal/data-protection functions and system administrators — rather than assumed to belong to a single technical unit.

Table 2. Suggested data classification for AI use in academic institutions

Data class	Examples	AI usage recommendation
Public	Published syllabi, public course descriptions, open educational resources.	Usually allowed.
Internal	Internal teaching materials, non-confidential methodological notes.	Allowed only in approved tools.
Confidential	Student grades, internal reports, unpublished research drafts.	Restricted; use only controlled institutional systems.
Highly sensitive	Health and disability data, disciplinary records, examination banks, personal identifiers.	Prohibited in public AI tools; requires formal approval and safeguards.

4.3. Model-related risks

Model-related risks arise from the behaviour of the LLM itself. They include hallucinations, incorrect citations, fabricated sources, biased outputs, unsafe recommendations, privacy leakage, and overconfident responses. In academic institutions such risks may affect teaching, student support, research writing, administrative decisions, and assessment. Table 3 sets them out.

Table 3. Model-related risks of AI assistants in academic institutions

Risk category	Description	Academic example	Possible impact
Hallucination	AI generates false or unsupported information.	A student receives fabricated references for a research paper.	Poor academic quality, misinformation.
Fabricated citations	AI invents sources or misrepresents existing publications.	A teacher uses an AI-generated bibliography without verification.	Research integrity violation.
Bias and unfairness	AI output reflects biased training data or assumptions.	AI gives feedback of different quality depending on language style.	Unequal treatment of students.
Unsafe recommendations	AI provides harmful, misleading, or non-compliant advice.	AI gives incorrect legal, medical, or psychological guidance to students.	Harm to users, institutional liability.

Risk category	Description	Academic example	Possible impact
Memorisation and leakage	Model reproduces sensitive content from training data or context.	AI reveals parts of uploaded confidential documents.	Data breach, confidentiality loss.
Explainability gap	Users cannot understand why a recommendation was produced.	AI suggests academic intervention for a student without transparent reasoning.	Accountability and fairness concerns.
Prompt injection and jailbreaks	Malicious or manipulated input changes the behaviour of the AI assistant or forces it to ignore intended instructions.	A student submits a document containing hidden instructions that manipulate an AI-assisted grading or feedback tool.	Unauthorised disclosure, incorrect feedback, bypass of institutional rules, or unsafe system actions.

Model-related issues are not limited to technical error. In an academic environment, a single hallucinated answer, fabricated citation, or biased recommendation can directly affect the quality of learning, assessment, research writing, or administrative decision-making — the more so because LLM outputs are fluent and authoritative in style, which may lead users to trust them without sufficient verification. These risks should therefore be managed through mandatory human oversight, verification of generated references, clear rules for using AI-generated content, and careful limitation of AI use in high-impact academic decisions. AI assistants may support educational and research processes, but they should not replace academic judgement, expert review, or institutional accountability. In sensitive scenarios — student assessment, academic intervention, research conclusions, administrative recommendations — AI-generated outputs should be treated as advisory and must be reviewed by a responsible human user before being acted on. Hallucination and overconfidence are thus not only technical risks but educational and organisational ones.

Prompt injection appears in Table 3 as a model-related and adversarial-interaction risk, but it is discussed separately below because it is not only a model issue. It is also an application-security and governance issue, and effective mitigation requires more than improved prompting: it requires input filtering, separation of trusted and untrusted content, least-privilege tool access, output validation, logging, and human approval for sensitive actions.

4.4. Prompt injection and adversarial manipulation

Prompt injection is one of the most important technical risks for AI assistants. It occurs when malicious or untrusted text manipulates the behaviour of an LLM by causing the model to treat data as instructions. This is especially relevant in academic institutions, because AI assistants may process untrusted content such as student submissions, uploaded PDF files, web pages, emails, forum posts, and research documents. The UK National Cyber Security Centre explains that prompt injection differs from classical SQL injection because LLMs do not maintain a robust internal distinction between data and instructions: in an LLM prompt, both trusted instructions and untrusted content are processed as token sequences, which makes complete mitigation difficult (National Cyber Security Centre, 2025b). In an academic environment, a student could insert hidden instructions into an essay submitted to an AI-assisted grading-support tool; a malicious web page could contain instructions that manipulate a research assistant summarising online content; an uploaded PDF file could

include text instructing the AI assistant to reveal system prompts, ignore policy constraints, or access unrelated documents.

In earlier work, the present author proposed an additional filter layer for LLM-based systems (Muliarevych, 2024). That architecture includes a prompt analyser and an attack validator module that use an LLM to classify prompts before they reach the core model, and it evaluates several protection strategies, including core GPT models without additional protection, fuzzy-search-based filtering, and validator-based approaches. The approach is relevant to academic AI assistants because it provides a concrete technical mitigation pattern that can be adapted to university tools. Building on that model, the present article adapts the filter-layer concept to the academic context: user prompts, student submissions, uploaded documents, and external content should pass through a prompt-analysis and validation stage before reaching the core model, and suspicious inputs should be blocked, logged, quarantined, or escalated for human review.

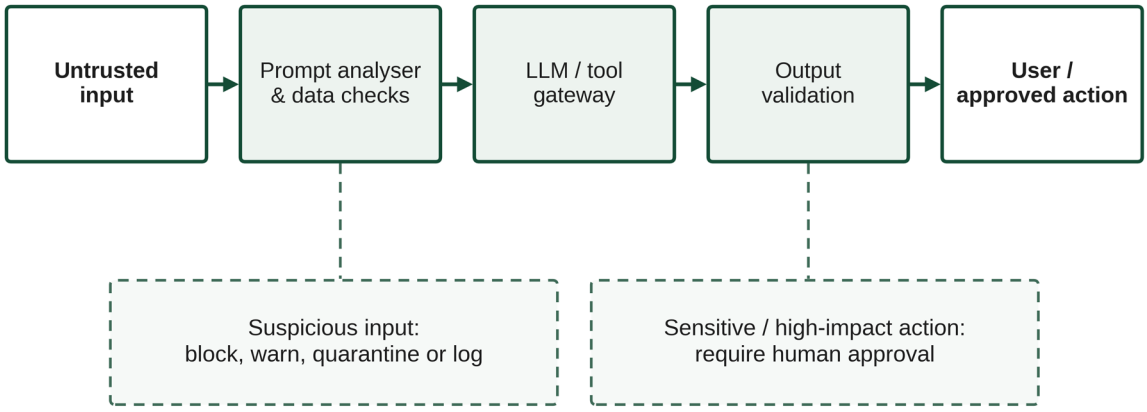


Figure 2. Prompt-injection defence pattern for AI assistants in academic institutions, adapted from the filter-layer approach proposed by Muliarevych (2024)

The key design principle, illustrated in Figure 2, is that a university AI assistant should not process untrusted content directly in a privileged execution context. It should instead apply layered controls: input pre-processing, data classification, prompt-injection detection, separation of trusted instructions from untrusted content, least-privilege tool access, output validation, logging, anomaly detection, and human approval for sensitive actions. This defence should not, however, be presented as a complete solution. Prompt injection remains difficult to eliminate because the model processes instructions and data within the same language-based context. Academic institutions should therefore assume residual risk and focus not only on detecting prompt injection but also on limiting the damage if an attack succeeds. AI assistants should have restricted permissions, controlled access to institutional systems, and no ability to perform high-impact actions without human confirmation.

4.5. Application and integration risks

The risk level increases significantly when AI assistants are integrated with institutional systems. A standalone assistant that only answers general questions has a narrower impact surface than one connected to an LMS, email, document repositories, student-information systems, research databases or action-taking tools. In the OWASP 2025 taxonomy, the relevant risks are captured especially by prompt injection, sensitive information disclosure, improper output handling, excessive agency, system-prompt leakage and vector/embedding weaknesses (OWASP Foundation, 2025). Table 4 sets out common academic integration scenarios.

Table 4. Application and integration risks of AI assistants in academic institutions

Integration scenario	Risk	Example
AI assistant + learning management system (LMS)	Unauthorised access to course or student data.	Assistant retrieves grades or private submissions without proper access control.
AI assistant + email	Indirect prompt injection through emails.	Malicious email instructs AI to forward confidential information.
AI assistant + document repository	Sensitive-information disclosure or permission bypass.	AI summarises documents outside the user's permission scope.
AI assistant + research database	Exposure of unpublished/restricted data; vector or embedding weaknesses.	Research assistant retrieves sensitive data for an unauthorised user.
AI assistant + administrative workflow	Excessive agency or unintended automated actions.	AI creates, approves, or modifies forms without human confirmation.
AI assistant + code repository	Source-code and credential leakage.	AI assistant exposes internal scripts, API keys, or configuration files.

Integration risks appear when an AI assistant moves from a passive question-answering role to an active institutional component connected to university systems, where it may retrieve, summarise, modify, or transmit information. The main security concern is therefore not only the behaviour of the LLM itself but also the level of access granted to the assistant and the quality of controls around each integration point. Each scenario in Table 4 creates a different type of institutional risk, and code repositories are the most sensitive of them. AI assistants should accordingly not be integrated with institutional systems through direct and unrestricted access. Each integration should pass through a controlled tool or API gateway, permission checks, logging, and, where needed, human approval. The assistant should operate under the same access-control rules as the user, and preferably under stricter limitations for high-risk actions. This reduces the probability that an AI assistant becomes a shortcut around existing university security policies.

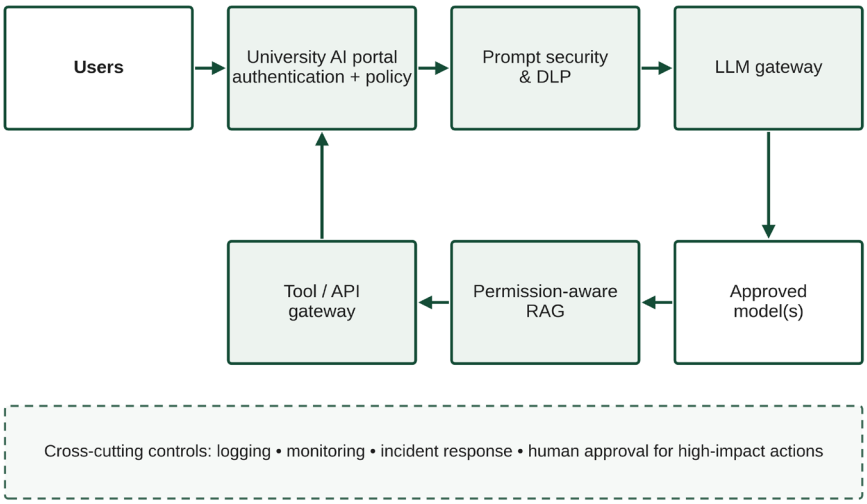


Figure 3. Secure architecture pattern for university AI assistants

The architecture also includes a permission-aware retrieval-augmented generation (RAG) knowledge base and a tool/API gateway, including Model Context Protocol (MCP) or similar tool-integration mechanisms, so that the assistant retrieves institutional knowledge or interacts with university systems only through controlled interfaces. This matters because the AI assistant must not bypass existing access-control rules: if a user does not have permission to access a document or system directly, the AI assistant should not expose that information indirectly. The output validation layer checks generated responses before they are returned to the user and can help detect sensitive information disclosure, unsupported claims, unsafe recommendations, or policy violations. Logging, monitoring, and incident response then provide operational visibility into AI assistant usage, blocked attempts, suspicious behaviour, and possible data-leakage incidents. The design principle underlying the whole pattern is that an AI assistant should be treated as a security-sensitive component of the university information system rather than as an application added on top of it.

4.6. Human and governance risks

Human and governance risks are often underestimated. Even a technically secure AI assistant can be misused if users do not understand its limitations or if institutional rules are unclear. Table 5 sets out the principal governance failures and their institutional consequences.

Table 5. Human and governance risks of AI assistants in academic institutions

Governance risk	Description	Institutional consequence
No AI usage policy	Users choose tools independently.	Shadow AI usage and uncontrolled data sharing.
Policy focused only on plagiarism	Security and privacy are ignored.	Hidden institutional risk.
No data-classification rules	Users do not know what may be entered into AI tools.	Accidental leakage of sensitive data.

Governance risk	Description	Institutional consequence
No approved tool list	Departments use different public AI services.	Vendor and compliance fragmentation.
No auditability	AI-assisted actions are not logged.	Difficult incident investigation.
Weak AI literacy	Students and staff do not understand hallucination, privacy, or prompt injection.	Unsafe and uncritical AI use.
No ownership model	Responsibilities of IT, legal, academic departments, and data-protection roles are unclear.	Delayed response and inconsistent enforcement.

As Table 5 shows, these risks arise not from technical failure but from unclear institutional responsibility and inconsistent user behaviour. Governance of AI assistants should therefore be distributed rather than assigned to IT departments alone. University leadership, cybersecurity teams, legal or data-protection officers, academic boards, research ethics committees, teaching staff, and student representatives should jointly define rules for acceptable AI use, approved tools, accountability, training, and incident response. This reduces fragmentation and makes AI adoption more predictable, transparent, and secure.

5. The Academic AI Security and Privacy Governance Framework

5.1. Framework overview

On the basis of the classification set out above, this article proposes a practical framework, the Academic AI Security and Privacy Governance Framework, designed for universities and academic institutions that use or plan to use AI assistants in teaching, research, administration, or student support. The framework has six layers: governance and policy; data classification and privacy; secure AI architecture; prompt and output security; human oversight and AI literacy; and monitoring, audit, and continuous improvement. It is presented in Figure 4.

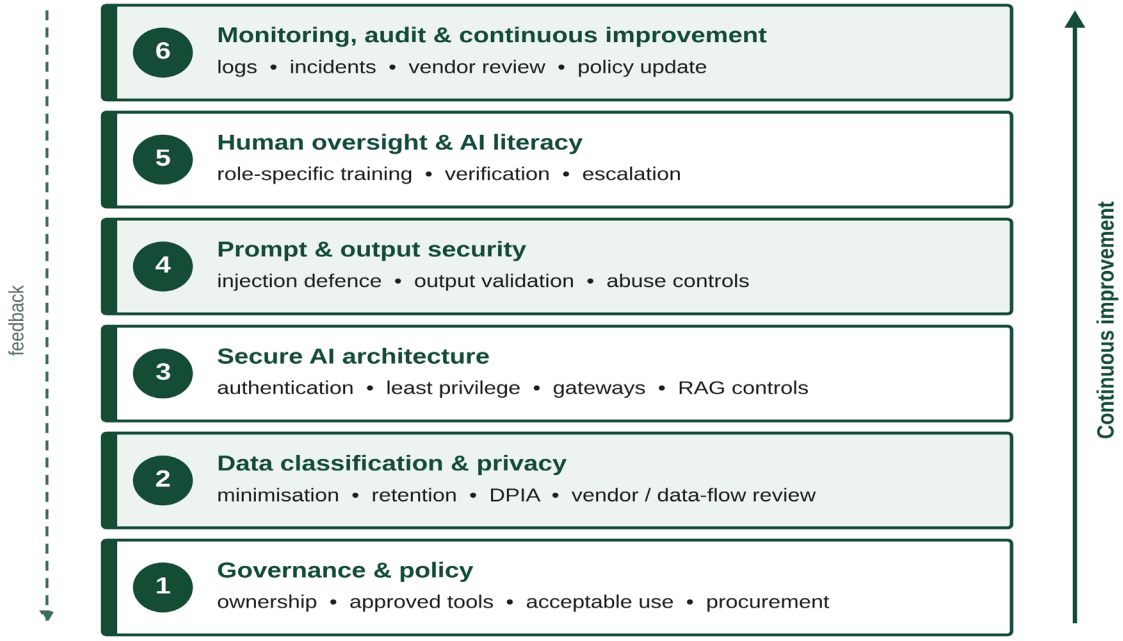


Figure 4. Academic AI Security and Privacy Governance Framework, with layered controls and a continuous-improvement feedback loop

The framework is organised as a layered model because each layer depends on the one before it: policy determines what is permitted, data classification determines what may be processed, architecture enforces both in technical controls, and the remaining three layers protect, inform, and audit what results. The feedback arrow in Figure 4 is important, because AI governance should not be treated as a one-time implementation activity. AI models, institutional use cases, regulations, and attack techniques change rapidly, and lessons learned from monitoring and incidents should continuously improve policies, data-classification rules, technical controls, and user training. The six layers are described in turn below.

5.2. Layer 1: Governance and policy

The first layer defines institutional rules for the use of AI assistants. Without it, users will independently adopt public AI tools, creating shadow AI usage and uncontrolled data flows. The governance layer should include an institutional AI acceptable-use policy; lists of approved and prohibited AI tools; rules for using AI in teaching, assessment, research, and administration; authorship and citation rules; vendor approval processes; and incident-reporting procedures. For institutions subject to or aligning with European regulation, the policy should also distinguish ordinary low-impact uses from educational AI systems whose purpose may bring them within the AI Act's high-risk categories, such as systems used to determine access, evaluate learning outcomes, assess educational level or monitor prohibited behaviour during tests (European Parliament & Council of the European Union, 2024).

5.3. Layer 2: Data classification and privacy

The second layer focuses on data protection. Academic institutions should classify data before deciding whether it may be processed by AI assistants, using an operational model such as Table 2. Controls should include data minimisation; anonymisation or pseudonymisation where appropriate; review of purpose, legal basis and retention; vendor and data-flow assessment; transparency to affected users; and a Data Protection Impact Assessment where the applicable legal threshold is met. LLM-specific mitigations should support, not substitute for, that assessment (European Data Protection Board, 2025).

5.4. Layer 3: Secure AI architecture

The third layer concerns technical architecture. Its key principle is that AI assistants should be deployed through controlled institutional gateways rather than through uncontrolled direct use of public tools for sensitive tasks. Controls should include authentication, role-based access control, AI gateways, data-loss prevention, retrieval control, API gateways, least privilege, human approval, and logging, along the lines set out in Figure 3.

5.5. Layer 4: Prompt and output security

The fourth layer addresses prompt injection, jailbreaks, sensitive-information disclosure, improper output handling and other adversarial or unsafe interactions. It should include prompt-injection testing and detection, separation and labelling of trusted and untrusted

context, sensitive-data checks, output validation, deterministic checks around tool calls, rate and resource limits, abuse detection, and explicit human approval for consequential actions. These controls reduce risk but should not be described as eliminating prompt injection; residual risk must be constrained by least privilege and impact limitation.

5.6. Layer 5: Human oversight and AI literacy

The fifth layer addresses people, since technical controls are not sufficient if users do not understand the risk. Academic institutions should provide AI literacy training for students, teaching staff, researchers, administrative staff, IT teams, and academic managers. Training should cover data privacy, hallucination, citation verification, disclosure of AI use, the basics of prompt injection, safe handling of documents, and incident reporting.

5.7. Layer 6: Monitoring, audit, and continuous improvement

The sixth layer ensures that AI governance does not become static. AI models, tools, regulations, and attack methods change quickly. Universities therefore need logging of AI assistant usage, records of blocked prompt-injection attempts, detection of sensitive-data leakage, audit of vendor terms, regular review of approved AI tools, incident-response procedures, and periodic policy updates informed by incident reports and user feedback.

5.8. Implementation roadmap

While the six layers define the logical structure of AI security and privacy governance, universities also need a practical sequence for implementation; the framework should be translated into concrete institutional actions rather than left as a theoretical model. Table 6 sets out a proposed roadmap.

Table 6. Proposed institutional implementation roadmap

Stage	Action	Expected result
Stage 1	Identify current AI tool usage across departments.	Visibility of shadow AI usage.
Stage 2	Define data classes and prohibited AI use cases.	Clear rules for sensitive data.
Stage 3	Approve institutional AI tools and vendors.	Reduced uncontrolled third-party exposure.
Stage 4	Create an AI acceptable-use policy.	Common rules for students and staff.
Stage 5	Deploy an AI gateway or controlled access model.	Centralised technical control.
Stage 6	Add prompt-injection and data-leakage filters.	Reduced technical risk.
Stage 7	Train staff and students.	Improved AI security literacy.
Stage 8	Establish monitoring and incident response.	Operational risk management.
Stage 9	Review and update policy every semester.	Continuous adaptation.

The roadmap follows a risk-based logic. Implementation begins with visibility and governance rather than with technology, because an institution cannot secure AI use effectively if it does not know which tools are already in use, what data is processed, and who is responsible for decisions; unmanaged or „shadow" AI usage creates immediate privacy

and compliance risks. Implementation is not completed when a policy is published or a tool deployed: it requires continuous monitoring, incident response, and regular policy updates as AI technologies, institutional practices, and cybersecurity threats evolve.

5.9. Prioritising risks: a practical risk matrix

Universities also need a practical way to prioritise the risks identified above. Table 7 therefore provides an illustrative qualitative matrix, not an empirically estimated probability model. The likelihood and impact labels are expert-informed screening categories intended to support local workshops; institutions should recalibrate them using their own incident history, architecture, data inventory, deployment model and regulatory context.

Table 7. Practical AI assistant risk matrix for academic institutions

Risk	Likelihood	Impact	Recommended treatment
Students use AI for undisclosed academic work	High	Medium	Academic-integrity policy, AI disclosure rules, assessment redesign.
Staff upload student data to public AI tools	Medium	High	Data-classification rules, approved tools, privacy training.
Researchers upload unpublished manuscripts or datasets	Medium	High	Research AI policy, confidentiality guidance, secure institutional AI tools.
Prompt injection manipulates AI assistant behaviour	Medium	High	Prompt filtering, least privilege, tool isolation, monitoring.
AI assistant leaks sensitive institutional information	Medium	High	Access control, permission-aware retrieval, output validation.
AI-generated hallucinations affect learning or research	High	Medium	Verification rules, citation checks, human review.
AI assistant performs unintended action through plugins	Low–Medium	High	Human approval, deterministic controls, API gateway.
Vendor stores or reuses confidential data	Medium	High	Vendor assessment, contractual controls, enterprise settings.
Fragmented AI governance between departments	High	Medium–High	Central AI governance committee and policy.
Users overtrust AI outputs	High	Medium	AI literacy, warnings, verification practices.

The matrix shows that the most critical risks are not always the most technically complex. Several high-priority risks — staff uploading student data to public AI tools, researchers using external AI systems for unpublished materials, fragmented AI governance between departments — are primarily organisational and policy-related, while technical risks such as prompt injection, sensitive-information leakage, and unintended tool-based actions require architectural controls, monitoring, and human approval. Risk treatment should accordingly be layered rather than uniform, and the framework should be implemented not as a single technical solution but as a coordinated institutional governance model.

5.10. Implications for stakeholder groups

The practical meaning of these risks differs across stakeholder groups. University leadership, teachers, students, researchers, and IT and cybersecurity teams interact with AI as-

sistants in different ways and therefore carry different responsibilities.

University leadership should treat AI assistant adoption as a strategic governance issue rather than an educational trend. The use of AI assistants affects institutional reputation, legal compliance, research quality, data security, and student trust, and responsibility for AI governance should therefore not be delegated solely to individual teachers or IT specialists.

Teachers need clear rules about when AI use is allowed, when it must be disclosed, and how assessment should adapt. Traditional written assignments may become less reliable as evidence of independent student work if they can be completed almost entirely by AI. Assessment may need to incorporate oral defence, process-based assessment, reflective explanation, practical tasks, in-class components, version history, project logs, personalised assignments, and explicit declarations of AI use.

Students should understand that AI assistants can be useful learning tools but that unsafe or undisclosed use can create academic and privacy problems. They should be informed that AI-generated text may contain errors, that AI may fabricate references, that entering personal or confidential data into public tools may be unsafe, and that AI use may need to be disclosed.

Researchers should treat external AI assistants as third-party processing services that require a deliberate data-flow and contractual assessment before confidential or personal data are submitted. Whether a vendor legally acts as a processor, independent controller or in another role depends on the concrete service, purposes, contractual terms and applicable law. As a practical rule, unpublished manuscripts, sensitive datasets, peer-review materials, grant proposals, industry-funded work and protected intellectual property should be used only with tools and configurations approved for those data.

IT and cybersecurity teams should expand their threat models to include AI-specific risks. Traditional controls such as authentication, network security, and endpoint protection remain necessary but do not address LLM-specific issues. Additional controls should include prompt-injection testing, detection of sensitive data in prompts and uploaded files, enforcement of access control in retrieval-augmented systems, monitoring of AI tool usage, vendor assessment, abuse detection, secure logging, isolation of AI tools from high-risk systems, and human approval for sensitive actions.

The central proposal of this article is that academic institutions should treat AI assistants as security- and privacy-sensitive socio-technical systems rather than as productivity or learning tools. Policy without architecture is insufficient: a university may publish AI guidelines, but if users continue uploading sensitive data to uncontrolled public tools, the risk remains unmanaged. Architecture without literacy is also insufficient: a secure AI gateway helps, but students and staff still need to understand privacy, hallucination, prompt injection, and academic-integrity risks. And detection without impact limitation is insufficient: prompt-injection filters are useful, but the system must also apply least privilege, human approval, access control, and monitoring, because prompt injection cannot be assumed to be fully eliminated. The six layers of the proposed framework are designed to be adopted together, and it is their combination that allows academic institutions to support responsible AI adoption while reducing cybersecurity, privacy, and governance risks.

6. Conclusion

AI assistants based on large language models are becoming part of everyday academic life. They support students, teachers, researchers, and administrators with writing, summarisation, translation, coding, explanation, and information retrieval. Their use in academic institutions nevertheless creates cybersecurity and privacy risks that go far beyond academic integrity.

The article has shown that the risks of AI assistants in universities can be organised into four major groups: data-related risks, model-related risks, application and integration risks, and human and governance risks. The classification is intentionally institution-centred rather than a duplicate of OWASP: it maps technical vulnerabilities and model limitations onto academic assets, workflows and accountability. Current OWASP 2025 categories — including prompt injection, sensitive information disclosure, improper output handling, excessive agency, system-prompt leakage, vector and embedding weaknesses and misinformation — are therefore treated as inputs to, rather than substitutes for, the proposed university risk model (OWASP Foundation, 2025).

A key finding is that AI assistants should not be treated only as educational tools. In academic institutions they are security- and privacy-sensitive socio-technical systems: they process data, influence academic work, support decisions, and may interact with institutional infrastructure. Universities therefore need more than general advice about responsible AI use; they need a structured institutional response.

The proposed Academic AI Security and Privacy Governance Framework addresses this need through six layers: governance and policy; data classification and privacy; secure AI architecture; prompt and output security; human oversight and AI literacy; and monitoring, audit, and continuous improvement. The framework integrates higher-education AI governance, technical LLM security, privacy protection, and institutional risk management.

The central conclusion is that safe AI adoption in academic institutions requires balance. Universities should neither ignore AI assistants nor rely on prohibition alone; equally, they should not allow uncontrolled use of public AI systems for sensitive academic work. A risk-based approach is required, in which public and low-risk educational content may be suitable for AI-assisted processing while personal data, confidential research, examination materials, and institutional records require strict controls.

Three implications follow for governance and regulatory practice, and they are the reason the analysis belongs to the study of law and digital technologies rather than to information security alone. First, the institutional AI policy is emerging as the operative regulatory instrument in this field. International guidance and general data-protection law set the objectives; what determines whether student data actually reaches a third-party model on a given Tuesday is a university's acceptable-use rule, its approved-tool list, and the configuration of its gateway. Regulators and ministries that wish to influence outcomes should therefore attend to the quality and enforceability of these subordinate instruments, and not only to the adequacy of the primary norms. Second, accountability requires auditability, and auditability requires design. A university cannot demonstrate compliance, respond to a subject access request, or investigate an incident if AI-assisted actions leave no record; the sixth

layer of the framework is thus a legal requirement expressed as a technical one, and it should be treated as such in procurement and in vendor contracts. Third, the residual character of prompt injection has a governance consequence that is easily missed. Where a class of attack cannot be eliminated, the institution's obligation shifts from prevention to the limitation of consequences — least privilege, human confirmation of high-impact actions, and a decision not to deploy where the residual risk is intolerable. For universities in jurisdictions that are aligning their data-protection and digital regulation with European standards, including Ukraine, the practical task is to build these three commitments into institutional rules now, while AI assistants are still being adopted, rather than to retrofit them after the first serious incident. Sustainable governance of academic AI is, on this view, less a matter of new legal norms than of institutional capacity to apply the norms that already exist.

Funding

This research received no external funding.

Conflicts of Interest

The author declares no conflicts of interest.

Data Availability

No new datasets were generated or analysed for this conceptual review. The study is based on publicly available academic literature, regulatory documents and technical guidance cited in the References.

Ethics Statement

This study is based on the analysis of publicly available academic publications, policy documents, regulatory guidance, and technical frameworks. It does not involve human participants, personal data processing, interviews, surveys, or experiments. Formal ethics committee approval was therefore not required.

Declaration of Generative AI Use

During the preparation of this manuscript, the author used the local LLM gpt-oss-20b for English-language editing, grammar checking, and improvement of wording. The author reviewed, edited, and verified all outputs, and retains full responsibility for the manuscript's intellectual content, analysis, conceptual framework design, and evaluation of the literature.

References

An, Y., Yu, J. H., & James, S. (2025). Investigating the higher education institutions' guidelines and policies regarding the use of generative AI in teaching, learning, research, and administration. International Journal of Educational Technology in Higher Education, 22. https://doi.org/10.1186/s41239-025-00507-3

Autio, C., Schwartz, R., Dunietz, J., Jain, S., Stanley, M., Tabassi, E., Hall, P., & Roberts, K. (2024). Artificial intelligence risk management framework: Generative artificial intelligence profile (NIST AI 600-1). National Institute of Standards and Technology. https://doi.org/10.6028/NIST.AI.600-1

Bittle, K., & El-Gayar, O. (2025). Generative AI and academic integrity in higher education: A systematic review and research agenda. Information, 16(4), Article 296. https://doi.org/10.3390/info16040296

Borodiyenko, O., Drach, I., Bazeliuk, N., Petroye, O., Reheilo, I., Bazeliuk, O., & Slobodianiuk, O. (2025). Opportunities and risks of using AI-based applications in research: The case of Ukrainian universities. Information Technologies and Learning Tools, 105(1), 125–143. https://doi.org/10.33407/itlt.v105i1.5794

Chang, V., Ansari, Y., & Arami, M. (2024). ChatGPT in higher education: A risk management approach to academic integrity, critical thinking, and workforce readiness. In Proceedings of the 6th International Conference on Finance, Economics, Management and IT Business. https://doi.org/10.5220/0012764100003717

Dahabiyeh, L., Taha, N., Thneibat, M., & Bhat, M. A. (2026). Privacy awareness in generative AI: The case of ChatGPT. Interactive Technology and Smart Education, 23(1), 25–48. https://doi.org/10.1108/ITSE-01-2025-0009

Das, B. C., Amini, M. H., & Wu, Y. (2025). Security and privacy challenges of large language models: A survey. ACM Computing Surveys, 57(6), Article 152, 1–39. https://doi.org/10.1145/3712001

European Commission, Directorate-General for Research and Innovation. (2026). Living guidelines on the responsible use of generative AI in research (3rd ed.). European Commission. https://research-and-innovation.ec.europa.eu/news/all-research-and-innovation-news/updated-era-living-guidelines-responsible-use-generative-ai-research-2026-05-08_en

European Data Protection Board. (2024). Opinion 28/2024 on certain data protection aspects related to the processing of personal data in the context of AI models. https://www.edpb.europa.eu/our-work-tools/our-documents/opinion-board-art-64/opinion-282024-certain-data-protection-aspects_en

European Data Protection Board. (2025). AI privacy risks & mitigations: Large language models (LLMs). https://www.edpb.europa.eu/our-work-tools/our-documents/support-pool-experts-projects/ai-privacy-risks-mitigations-large_en

Miao, F., & Cukurova, M. (2024). AI competency framework for teachers. UNESCO. https://www.unesco.org/en/articles/ai-competency-framework-teachers

Miao, F., & Holmes, W. (2023). Guidance for generative AI in education and research. UNESCO. https://www.unesco.org/en/articles/guidance-generative-ai-education-and-research

Miranda, M., Ruzzetti, E. S., Santilli, A., Zanzotto, F. M., Bratières, S., & Rodolà, E. (2025). Preserving privacy in large language models: A survey on current threats and solutions. Transactions on Machine Learning Research. https://arxiv.org/abs/2408.05212

Moorhouse, B. L., Yeo, M. A., & Wan, Y. (2023). Generative AI tools and assessment: Guidelines of the world's top-ranking universities. Computers and Education Open, 5, Article 100151. https://doi.org/10.1016/j.caeo.2023.100151

Muliarevych, O. (2024). Enhancing system security: LLM-driven defense against prompt injection vulnerabilities. In 2024 IEEE 17th International Conference on Advanced Trends in Radioelectronics, Telecommunications and Computer Engineering (TCSET) (pp. 420–423). IEEE. https://doi.org/10.1109/TCSET64720.2024.10755823

National Cyber Security Centre. (2025a). Impact of AI on cyber threat from now to 2027. https://www.ncsc.gov.uk/report/impact-ai-cyber-threat-now-2027

National Cyber Security Centre. (2025b). Prompt injection is not SQL injection: It may be worse. https://www.ncsc.gov.uk/blog-post/prompt-injection-is-not-sql-injection

Neel, S., & Chang, P. (2024). Privacy issues in large language models: A survey. arXiv. https://doi.org/10.48550/arXiv.2312.06717

Novelli, C., Casolari, F., Hacker, P., Spedicato, G., & Floridi, L. (2024). Generative AI in EU law: Liability, privacy, intellectual property, and cybersecurity. Computer Law & Security Review, 55, Article 106066. https://doi.org/10.1016/j.clsr.2024.106066

OWASP Foundation. (2025). OWASP Top 10 for large language model applications. https://owasp.org/www-project-top-10-for-large-language-model-applications/

Pikhart, M., & Al-Obaydi, L. H. (2025). Reporting the potential risk of using AI in higher education: Subjective perspectives of educators. Computers in Human Behavior Reports, 18, Article 100693. https://doi.org/10.1016/j.chbr.2025.100693

Temper, M., Tjoa, S., & David, L. (2025). Higher Education Act for AI (HEAT-AI): A framework to regulate the usage of AI in higher education institutions. Frontiers in Education, 10, Article 1505370. https://doi.org/10.3389/feduc.2025.1505370

Wilson, T. D. (2025). The development of policies on generative artificial intelligence in UK universities. IFLA Journal, 51(3), 722–734. https://doi.org/10.1177/03400352251333796

Wu, C., Zhang, H., & Carroll, J. M. (2024). AI governance in higher education: Case studies of guidance at Big Ten universities. Future Internet, 16(10), Article 354. https://doi.org/10.3390/fi16100354

Xu, X. S., Liu, J., Zheng, R., Lei, V. N.-L., & An, Q. (2025). Learners' perception of data privacy when using AI language models: Reflective diary analysis of undergraduates in China. Acta Psychologica, 260, Article 105491. https://doi.org/10.1016/j.actpsy.2025.105491

Xue, Y., Chinapah, V., & Zhu, C. (2025). A comparative analysis of AI privacy concerns in higher education: News coverage in China and Western countries. Education Sciences, 15(6), Article 650. https://doi.org/10.3390/educsci15060650

Yao, Y., Duan, J., Xu, K., Cai, Y., Sun, Z., & Zhang, Y. (2024). A survey on large language model security and privacy: The good, the bad, and the ugly. High-Confidence Computing, 4(2), Article 100211. https://doi.org/10.1016/j.hcc.2024.100211

Pedagogical Framework For Training Social Workers As Mediators In Civil Proceedings: A Trauma-Informed And Digitally Responsible Approach

Kateryna Dmytrenko
"Kharkiv Humanitarian-Pedagogical Academy"
Kharkiv Regional Council
Kharkiv, Ukraine
ORCID iD: 0000-0002-4880-8274
dmitrenko.katia@gmail.com

Abstract.
The integration of mediation into civil justice in Ukraine raises an educational problem that cannot be resolved by legal regulation alone: institutions must prepare practitioners who can conduct a structured, confidential and neutral process while working with conflict, stress, digital communication and professional boundaries. This conceptual article develops a pedagogical framework for preparing social work students for a later professional pathway into mediation. The study combines doctrinal analysis of the Law of Ukraine „On Mediation", analysis of the national higher-education standard for Social Work, European mediation-training guidance, and a targeted synthesis of literature on mediation education, trauma-informed social work and online dispute resolution. No survey, experiment, interview or other human-participant research is reported. The proposed framework contains five competency domains: legal-procedural literacy; neutral facilitative communication; trauma-informed process management; self-regulation and professional resilience; and digital mediation and data ethics. A two-level implementation model is proposed: degree-embedded preparatory learning within social work education, followed by statutory basic mediator training that meets the requirements of Ukrainian law. The framework emphasises role differentiation because social workers' helping and advocacy functions do not automatically coincide with the mediator's duty of neutrality and party self-determination. It also treats digital competence as a professional and governance requirement, encompassing confidentiality, platform security, informed consent, accessibility and responsible use of AI-assisted tools. The article argues that sustainable mediation reform depends on educational capacity, quality assurance and ethically governed digital practice as much as on the existence of mediation legislation.

Keywords: *mediation; civil justice; social work education; trauma-informed pedagogy; digital mediation; professional competence*

1.Introduction

Mediation has become an increasingly important component of contemporary civil justice because it offers parties a structured procedure for resolving disputes without transferring control over the outcome to a third-party decision-maker. In Ukraine, the Law of Ukraine „On Mediation" defines mediation as a voluntary, confidential and structured out-of-court procedure and establishes the principles of mediator neutrality, independence and impartiality, party self-determination and equality. The Law also establishes a professional threshold: a person may act as a mediator after completing basic mediator training, and that

88

basic programme must comprise at least 90 hours, including at least 45 hours of practical training (Law of Ukraine „On Mediation", 2021). These requirements are significant for higher education because they make mediator competence an educational as well as a legal issue. The existence of statutory training requirements does not, by itself, determine which prior professional backgrounds are best suited to mediation. Social work is relevant because its educational standards and professional traditions develop adjacent competences: communication, analysis of social and psychological processes, work with vulnerable persons, ethical decision-making, cooperation with clients and other professionals, use of information and communication technologies, and the capacity to resolve complex problems. The Ukrainian bachelor-level standard for Social Work includes legal knowledge, information and communication technology skills, ethical conduct, work with clients on the basis of trust, analysis of interpersonal processes, and the use of methods for resolving conflicts and difficult life circumstances (Ministry of Education and Science of Ukraine, 2019). These competences create a plausible foundation for subsequent mediator training.

At the same time, the relationship between social work and mediation must not be overstated. A social work degree does not itself confer mediator status under Ukrainian law, and the professional role of a social worker may include assistance, advocacy, case management or protection of a vulnerable client. Mediation, by contrast, requires the mediator to avoid deciding the dispute, advising the parties on the merits of the outcome, or representing one side. The educational challenge is therefore not to present social workers as mediators by default, but to identify which social-work competences are transferable, which require adaptation, and which specifically mediator competencies must be developed through dedicated training. This challenge is particularly important in an environment shaped by prolonged social stress and rapid digitalisation. Civil disputes may involve persons affected by displacement, loss, family disruption, housing insecurity, debt or other difficult life circumstances. A mediator needs sufficient trauma awareness to maintain procedural safety without converting mediation into therapy or presuming that every participant is traumatised. In parallel, mediation is increasingly prepared, communicated and sometimes conducted through digital platforms. Online interaction changes the practical meaning of confidentiality, informed consent, identity verification, accessibility and professional boundaries (Barsky, 2016; Katsh & Rabinovich-Einy, 2017). Accordingly, mediator preparation requires a competence model that combines legal, communicative, psychosocial and digital dimensions.

The aim of this article is to develop a conceptually grounded pedagogical framework for preparing future social workers for professional mediation in civil disputes. The article addresses three questions: (1) which competences required by mediation are already adjacent to the learning outcomes of social work education; (2) which competence gaps require dedicated mediator training; and (3) how trauma-informed and digitally responsible practice can be integrated into a coherent educational pathway. The contribution is a competency-mapping and curriculum-design model rather than an empirical evaluation of a programme. This distinction is essential: the framework is proposed for subsequent testing and implementation, not presented as an intervention whose effectiveness has already been statistically demonstrated.

2. Conceptual And Regulatory Foundations

2.1 Mediation competence in civil justice

Mediation differs from adjudication because the mediator manages a process rather than determines the parties' substantive rights. Moore (2014) describes mediation as a structured form of third-party intervention that supports negotiation and decision-making by the parties. In the Ukrainian regulatory model, this process orientation is reinforced by the principles of voluntariness, confidentiality, neutrality, independence, impartiality, self-determination and equality (Law of Ukraine „On Mediation", 2021). The mediator therefore requires legal literacy sufficient to understand the permissible scope of the role, procedural competence to organise the mediation, and communicative competence to facilitate negotiation without taking ownership of the decision.

The European framework points in the same direction. Directive 2008/52/EC addresses mediation in civil and commercial matters and links the development of mediation to a predictable legal framework and quality of mediation services (European Parliament & Council of the European Union, 2008). The Council of Europe's CEPEJ guidelines on designing and monitoring mediation training schemes further emphasise structured training, practical skills development and quality monitoring (European Commission for the Efficiency of Justice [CEPEJ], 2019). Taken together, these sources support a competency-based approach: mediator preparation should be defined not only by attendance or course titles but by observable learning outcomes and the ability to apply them in realistic situations.

2.2 Social work as an adjacent professional foundation

Social work education offers a strong adjacent foundation because it combines legal, psychosocial, communicative and ethical dimensions. Payne (2020) emphasises the holistic character of social work practice, while Barsky (2017) treats conflict-resolution skills as central to helping professions. The Ukrainian higher-education standard likewise requires graduates to understand the legal basis of social work, analyse social and psychological processes, interact with clients and professional groups, act ethically, use information and communication technologies, and apply methods for resolving difficult situations (Ministry of Education and Science of Ukraine, 2019). These outcomes overlap substantially with the knowledge and skills needed for mediation.

The overlap, however, contains an important professional-boundary problem. Social workers may be trained to protect clients' interests, mobilise resources, advocate for services or recommend interventions. A mediator must instead protect the integrity of the process and the parties' capacity for self-determination. Ukrainian law expressly prevents a mediator from combining the mediator role with another participant role in the same dispute and from advising the parties on the substantive decision they should make (Law of Ukraine „On Mediation", 2021). Consequently, training social workers for mediation must include role differentiation: when entering the mediator role, the practitioner must shift from helping through substantive assistance to helping through neutral facilitation.

This role transition is one reason why it is insufficient simply to add a short lecture on

90

mediation to an existing social work course. Students require repeated practice in reframing, active listening, open questioning, agenda construction, managing imbalance, summarising interests, supporting option generation and maintaining neutrality under pressure. They also need opportunities to identify when a matter is unsuitable for mediation, when specialist legal or psychological advice should be recommended, and when the process should be paused or terminated. The core pedagogical task is therefore conversion of adjacent social-work competence into mediator-specific professional behaviour.

2.3 Trauma-informed pedagogy without therapeutic overreach

Trauma-informed social work is built around safety, trust, collaboration, choice and empowerment rather than around assuming pathology or requiring disclosure of traumatic experiences (Levenson, 2017). In social work education, Carello and Butler (2015) argue that trauma-informed educational practice should reduce unnecessary re-traumatisation and create learning conditions in which difficult material can be addressed without sacrificing academic rigour. These principles are useful for mediation training because conflict situations may activate fear, anger, shame or physiological stress responses that interfere with communication and decision-making.

For mediator education, trauma-informed practice should be translated into process competence rather than therapeutic intervention. A mediator is not required to diagnose trauma and should not treat mediation as psychotherapy. Instead, the mediator should be able to recognise signs that participation is becoming unsafe or ineffective, explain the structure of the process transparently, offer appropriate breaks, use predictable communication, avoid coercive pressure, support party choice, and refer participants to specialist assistance where necessary. This boundary protects both the parties and the mediator's professional role.

The same logic applies to the mediator's own well-being. Repeated exposure to high-conflict narratives can produce emotional strain, while a mediator who loses self-regulation may become directive, defensive or avoidant. Grant and Kinman (2014) therefore provide a useful basis for treating resilience, reflective practice and professional self-care as competence-related rather than purely personal matters. In a training programme, self-regulation can be developed through structured debriefing, reflective logs, supervision, peer feedback and explicit strategies for managing cognitive and emotional load.

2.4 Digital mediation as a professional and governance issue

Digitalisation affects both the delivery of mediation and the design of mediator education. Online dispute resolution can increase accessibility and reduce geographic barriers, but it also changes the architecture of communication and the distribution of risk (Katsh & Rabinovich-Einy, 2017). Mediators working online must understand not only how to operate a videoconferencing platform but also how the platform affects confidentiality, privacy, party autonomy, power balance and the quality of interaction.

Barsky (2016) identifies informed consent, privacy and confidentiality, neutrality, fair-

91

ness and professional boundaries as ethical issues in technology-assisted mediation. For educational purposes, these concerns translate into concrete learning outcomes: students should know how to establish rules on recording, select an appropriate communication channel, confirm who is physically present with each participant, respond to connection failures, protect documents shared during the session, and recognise when digital exclusion or lack of privacy makes online mediation inappropriate. Where personal data are processed in EU-linked or cross-border contexts, the data-protection principles reflected in Regulation (EU) 2016/679 also provide a relevant benchmark for data minimisation, purpose limitation and security (European Parliament & Council of the European Union, 2016).

Digital competence also changes mediator training itself. Walsh (2019) shows that mediation education depends heavily on experiential learning and role-play and discusses how these activities can be redesigned for online environments. This is directly relevant to social work programmes because virtual simulations can provide repeated practice without exposing real clients or real case data. The appropriate pedagogical principle is therefore not maximal technologisation but purposeful use of technology: digital tools should increase practice opportunities, reflection and accessibility while preserving confidentiality, human oversight and ethical control.

3. Materials And Methods

This article uses a qualitative conceptual design combining doctrinal analysis, targeted literature synthesis, competency mapping and pedagogical modelling. It does not employ a mixed-methods design and does not report an experiment, survey, interview study or statistical evaluation. This methodological choice reflects the available evidence and the purpose of the paper: to construct a theoretically and normatively grounded framework that can later be tested empirically.

3.1 Normative and policy analysis

The normative component focused on documents that define either mediator qualification or the educational competences relevant to the proposed pathway. The principal Ukrainian sources were the Law of Ukraine „On Mediation" and the bachelor-level Standard of Higher Education in speciality 231 „Social Work". For comparative and quality-assurance purposes, the analysis also considered Directive 2008/52/EC and the CEPEJ Guidelines on Designing and Monitoring Mediation Training Schemes. The documents were read for requirements concerning mediator status, training duration, practical skills, neutrality, confidentiality, party self-determination, ethical conduct, professional competence and education quality.

3.2 Targeted literature synthesis

The literature component synthesised works already central to the author's topic—mediation process, social work theory, conflict resolution, trauma-informed education and resilience—and supplemented them with sources specifically addressing digital mediation

92

and mediator training. The review is targeted and conceptual rather than systematic; it does not claim exhaustive database coverage or PRISMA compliance. Sources were selected for their direct relevance to the competence domains required to construct the pedagogical framework.

3.3 Competency mapping and conceptual modelling

The analysis proceeded in three steps. First, mediator-specific requirements were extracted from law and mediation-training guidance. Second, these requirements were compared with adjacent competences contained in social work education and the professional literature. Third, areas of overlap and deficit were translated into learning outcomes, teaching methods and assessment evidence. The resulting model was then organised as a two-level educational pathway: preparatory competence development within a social work degree programme and dedicated statutory mediator training.

3.4 Research boundaries and ethics

No human participants were recruited, no student questionnaire was administered, no pedagogical experiment was conducted, and no numerical outcomes are presented. Consequently, no claims are made about the measured effectiveness of the proposed framework. Statements about likely educational value are conceptual propositions derived from the cited literature and normative analysis. Because the study uses publicly available legislation, policy documents and published literature and does not process personal data, formal human-subject ethics approval was not required for the work reported in this article. Empirical validation remains a task for subsequent research.

4. Results: A Competency-Based Pedagogical Framework

4.1 Regulatory and educational competency map

The comparison shows that social work education supplies several relevant foundations but does not replace mediator-specific preparation. The clearest overlap concerns communication, ethics, legal literacy, work with complex social situations and use of digital technologies. The clearest gaps concern the legal boundaries of the mediator role, disciplined neutrality, structured mediation procedure, mediation-specific confidentiality, party self-determination, and performance assessment through realistic mediation practice.

Table 1. Regulatory and educational foundations for the proposed mediator-training pathway

Source / domain	Requirement or existing competence	Identified educational implication	Status in the proposed pathway
Law of Ukraine "On Mediation"	Mediator status requires basic training of at least 90 hours, including at least 45 hours of practical training.	A social work degree may prepare students for mediation but cannot be treated as a substitute for the statutory training requirement.	Dedicated mediator training

93

Source / domain	Requirement or existing competence	Identified educational implication	Status in the proposed pathway
Principles of mediation under Ukrainian law	Voluntariness, confidentiality, neutrality, independence, impartiality, party self-determination and equality.	Students need role-boundary training and observable practice in neutral facilitation rather than advice-giving.	Mediator-specific core
Higher Education Standard: Social Work	Legal literacy, communication, ICT skills, ethical conduct, client interaction, analysis of social--psychological processes and conflict-related problem solving.	These competences provide an adjacent foundation that can be mapped to mediator learning outcomes.	Degree-embedded preparation
CEPEJ mediation-training guidance	Training should combine structured content, practical skills development and monitoring of learning quality.	Role-play, simulation, feedback and competency assessment should be central, not optional extras.	Quality assurance
Digital mediation / ODR literature	Technology affects confidentiality, informed consent, fairness, accessibility and professional boundaries.	Digital mediation ethics and data governance should be taught as professional competence.	Cross-cutting competence

4.2 Five competency domains

On the basis of this mapping, the framework is organised into five domains. They are intentionally formulated as learning outcomes rather than as course titles, because the same outcome may be developed across lectures, seminars, simulation, supervised practice and reflective work. The model also separates competence from confidence: students should not be judged primarily by self-reported readiness but by evidence that they can perform mediation-relevant actions consistently and ethically.

Table 2.Competency matrix for preparing social work students for professional mediation

Competency domain	Learning outcomes	Pedagogical methods	Evidence of attainment
1. Legal-procedural literacy	Explain the legal status and limits of mediation; distinguish mediation from legal advice, representation and adjudication; identify when specialist advice or termination is required.	Case-based lectures; analysis of the Law on Mediation; process maps; short legal problem scenarios.	Scenario-based test; process plan; reasoned response to boundary cases.
2. Neutral facilitative communication	Use active listening, reframing, open questions, summarising and agenda--setting; maintain neutrality; support party self-determination without directing the outcome.	Demonstration; paired exercises; role-play; observed simulation; peer and trainer feedback.	Behaviourally anchored simulation rubric; reflective commentary on interventions.
3. Trauma-informed process management	Recognise signs of distress without diagnosing; create predictable and psychologically safer process conditions; use breaks, choice and referral appropriately.	Trauma-informed case analysis; simulation with stress cues; debriefing; referral-mapping exercises.	Response to a complex scenario; explanation of safety and referral decisions.
4. Self-regulation and professional resilience	Monitor personal stress responses; maintain professional boundaries; use supervision and recovery strategies; recognise secondary stress risks.	Reflective logs; supervision; guided debrief; workload and trigger mapping; peer consultation.	Reflective portfolio; supervision plan; self-regulation strategy linked to observed practice.

94

Competency domain	Learning outcomes	Pedagogical methods	Evidence of attainment
5. Digital mediation and data ethics	Conduct secure and accessible online mediation; manage recording, identity, documents and confidentiality; evaluate digital-platform and AI-assisted tool risks.	Online role-play; platform--risk checklist; synthetic-case document sharing; data--protection exercises.	Digital-session protocol; security/privacy checklist; observed online simulation.

4.3 Learning sequence: from adjacent competence to mediator performance

The five domains should be taught through a staged sequence rather than as unrelated modules. The first stage is orientation and role differentiation. Students analyse the legal status of mediation and compare the mediator role with familiar social-work roles such as counsellor, advocate, case manager and service coordinator. The purpose is to prevent a common transfer error: assuming that helpfulness always means offering advice or recommending an outcome.

The second stage is isolated skills practice. Students rehearse specific interventions—listening, reframing, summarising, asking open questions, identifying interests, setting an agenda and responding to emotional escalation—before combining them in a full simulation. Short exercises make it easier to identify the mechanism of a skill and to provide focused feedback. This reflects the experiential character of mediator training highlighted in CEPEJ guidance and in mediator-training literature (CEPEJ, 2019; Walsh, 2019).

The third stage is integrated simulation. Students work with fictitious civil-dispute scenarios that combine legal ambiguity, strong emotions, unequal communication styles and digital-process complications. The simulation should require process decisions rather than a predetermined settlement. For example, a scenario may require the student to decide whether to pause the session, hold separate meetings, recommend independent legal advice, change the communication channel or terminate mediation because the conditions for voluntary participation are no longer present. The fourth stage is reflective assessment. Students review selected interventions, identify where their own assumptions influenced the process, explain how they protected neutrality and confidentiality, and formulate a development plan. Reflection is not a substitute for performance assessment; it is evidence of the capacity to learn from performance. The final assessment should therefore combine observed behaviour with reasoned self-analysis.

4.4 Pedagogical conditions for trauma-informed and digitally responsible simulation

Simulation is valuable only when its educational environment is itself ethically designed. Trauma-informed pedagogy suggests that students should receive advance information about the nature of difficult scenarios, understand that simulation is a learning exercise rather than a test of personal emotional disclosure, and have structured debriefing after high-conflict role-play (Carello & Butler, 2015). Students should not be required to reproduce personal traumatic experiences in order to demonstrate competence.

95

Digital simulation should use synthetic case materials and institutionally approved platforms. Recording should be limited to what is necessary for learning and should be governed by clear access and retention rules. Where automated transcription, generative AI or other AI-assisted functions are available, they should be treated as optional tools whose outputs require verification. Sensitive or identifiable client information should not be used to train students on public AI services. These controls make digital literacy part of professional ethics rather than merely technical convenience.

5. Practical Implementation In Social Work Education

5.1 A two-level educational pathway

The proposed framework is best implemented as a two-level pathway. Level One is embedded in the social work degree and prepares students through relevant learning outcomes, electives and simulations. Its purpose is orientation and competence development, not automatic professional certification as a mediator. Level Two is a dedicated basic mediator-training programme compliant with the Law of Ukraine „On Mediation", including the legally required volume and practical component. Where a higher-education institution acts as an authorised subject of educational activity and designs a programme meeting the statutory requirements, the two levels may be organisationally connected; however, the present article does not claim that any specific existing programme at the author's institution already satisfies or certifies the statutory mediator-training requirement.

This distinction resolves an important regulatory ambiguity in the earlier formulation of the topic. The educational value of social work is not that it creates a privileged or automatic route into mediation, but that it supplies a professional foundation from which mediation-specific competence can be developed efficiently. The framework therefore supports curriculum articulation: universities can identify which outcomes are already addressed in the social work programme and reserve dedicated mediation training for the competences that require specialised instruction and assessed practice.

5.2 Suggested instructional formats

A practical curriculum may combine five instructional formats. First, case-based seminars can connect mediation principles with civil-dispute contexts and professional-boundary questions. Second, micro-skills laboratories can isolate communication techniques before full simulations. Third, structured role-play can reproduce the temporal and relational complexity of mediation. Fourth, digital simulations can train online process management, data handling and accessibility. Fifth, supervision and reflective portfolios can connect performance feedback with professional self-regulation. Moodle or another learning-management system can support preparatory materials, submission of reflective work and controlled access to synthetic case files; videoconferencing platforms can support online role-play; and immersive technologies may be used where available, but they are not necessary for the framework to function.

Civil-dispute scenarios should be selected for educational value rather than sensationa-

lism. Suitable examples include consumer-service disputes, neighbour disputes, contractual disagreements, housing-related conflicts, inheritance communication problems or conflicts involving ongoing relationships. Scenarios should provide enough legal context to require boundary awareness but should not encourage students to practise unauthorised legal advice. The assessment question is how well the student manages the mediation process, not whether the student independently identifies the legally correct outcome.

5.3 Assessment and quality assurance

Assessment should rely on observable criteria. A simulation rubric may include opening and explanation of the process, neutrality of language, listening and questioning, management of participation, recognition of confidentiality issues, response to distress, support for party self-determination, digital-process control and quality of closure. Behaviourally anchored descriptors are preferable to global labels such as „good communication" because they provide clearer evidence for students, trainers and quality-assurance bodies.

Quality assurance also requires trainer competence and calibration. A programme that integrates law, social work, trauma-informed practice and digital mediation is inherently interdisciplinary. Legal specialists can clarify the limits of the mediator role; experienced mediators can assess process performance; social work educators can address client interaction, ethics and vulnerability; and psychologists or trauma-informed practitioners can support the design of safe educational scenarios without turning the mediation course into clinical training. Regular moderation of assessment decisions can reduce inconsistency among trainers.

5.4 Digital governance requirements

When mediator training is delivered digitally, the institution itself becomes responsible for modelling the practices it expects students to use professionally. Course design should therefore specify approved platforms, access permissions, recording rules, retention periods, procedures for sharing case materials and protocols for responding to accidental disclosure. Students should be taught to ask not only „Can this tool be used?" but also „What information will it process, who can access it, how long will it be retained, and what happens if the technology fails?" This turns digital competence into a governance habit.

The same principle applies to AI-assisted tools. Generative systems may be useful for creating synthetic role-play prompts, language support or practice questions, but they should not be treated as autonomous mediators or authoritative sources of legal advice. When such tools are used in education, students should be trained to verify outputs, avoid uploading identifiable or confidential information, and understand that responsibility remains with the human practitioner and institution. This is especially important in mediation because confidentiality and trust are not peripheral requirements but structural conditions of the process.

6. Discussion

The central theoretical implication of the proposed framework is that the relationship between social work and mediation is best understood through competence transfer rather than professional substitution. Social work provides a strong base in communication, ethics, psychosocial understanding and work with complex life circumstances, but mediation adds a distinct process role with distinct legal and ethical limits.

Framing the relationship this way avoids two opposite errors: treating social workers as automatically qualified mediators, and ignoring the substantial professional assets that social work education can contribute to mediator preparation.

A second implication concerns trauma-informed practice. The framework does not equate conflict with trauma, nor does it ask mediators to diagnose psychological conditions. Its purpose is procedural: mediation should be organised so that parties can participate voluntarily, understand what is happening, retain meaningful choice and communicate without unnecessary escalation or re-traumatisation.

This is consistent with trauma-informed social work principles while preserving the boundary between mediation and therapy (Levenson, 2017). In the Ukrainian context, where many citizens and professionals live with the consequences of prolonged war, this form of preparedness is particularly relevant, but it should remain individualised rather than assumption-driven.

A third implication concerns resilience. Earlier versions of the manuscript treated resilience largely as an individual health-preserving technology. The conceptual revision places it within professional capacity. A mediator who cannot recognise overload, seek supervision or regulate their own responses may compromise neutrality and process quality. Resilience is therefore connected to competence and quality assurance rather than to personal wellness alone.

This framing is more compatible with professional education because it links self-care to accountable practice.

The fourth implication concerns digitalisation. Online mediation is not simply face-to-face mediation transferred to a screen. Technology changes who can participate, what information is visible, how confidentiality can be breached, and how the mediator observes power and distress. A digitally responsible mediator therefore needs procedural and ethical judgement about technology, not merely operating skills. Barsky (2016) and the broader online-dispute-resolution literature show why issues such as privacy, informed consent, fairness and access must be integrated into professional training rather than delegated entirely to IT staff.

These findings also connect the article with sustainable governance. Mediation reform is sustainable only if institutions can reproduce competent practitioners, monitor training quality and adapt professional standards to digital conditions. A law may authorise mediation, but weak educational capacity can leave the reform under-implemented or unevenly implemented.

Conversely, a competence-based training pathway can translate legal principles into repeatable professional practice. In this sense, mediator education is part of justice-system

infrastructure: it links legislation, higher education, professional standards and digital governance.

The framework has limitations. It is a conceptual model based on normative documents and selected literature rather than a systematic review or empirical evaluation. It does not compare curricula across a representative sample of Ukrainian higher-education institutions, and it does not measure student learning, mediator performance, burnout or dispute outcomes. It also does not establish that social work graduates perform better as mediators than graduates of other disciplines.

These questions require subsequent research using transparent sampling, validated instruments, ethics procedures and observable outcome measures. A future pilot study could evaluate competency change before and after a defined training module, but such data should be collected prospectively rather than reconstructed retrospectively.

7. Conclusions

The preparation of social workers for a professional pathway into mediation should be built on a clear distinction between adjacent competence and mediator qualification. Social work education develops many capacities relevant to mediation, including legal and ethical awareness, communication, analysis of social and psychological processes, work with vulnerable persons and digital literacy. These capacities create a strong foundation, but they do not replace the dedicated basic mediator training required by Ukrainian law.

The framework proposed in this article organises mediator preparation around five domains: legal-procedural literacy; neutral facilitative communication; trauma-informed process management; self-regulation and professional resilience; and digital mediation and data ethics. The model recommends a staged sequence from role differentiation and micro-skills practice to integrated simulation and reflective assessment. It also proposes a two-level institutional design in which social work programmes develop preparatory competences and statutory mediator training provides the specialised, assessed practical preparation required for professional practice.

The conceptual contribution lies in linking three regulatory and educational layers that are often treated separately: mediation law, social work education and digitally mediated professional practice. Trauma-informed principles are translated into procedural safeguards rather than therapeutic claims, while digital competence is treated as an issue of confidentiality, consent, accessibility and institutional governance. This makes the framework suitable for further curriculum development without relying on unsupported claims of already-proven effectiveness.

Further research should empirically test the framework through prospectively designed studies. Priority directions include validation of behaviourally anchored assessment rubrics, comparison of face-to-face and online simulation, investigation of how role-boundary training affects neutrality, and longitudinal study of professional resilience among newly trained mediators. Such research would allow the proposed model to move from a conceptual framework to an evidence-informed component of mediator education and sustainable justice governance.

Funding

This research received no external funding.

Conflicts of Interest

The author declares no conflicts of interest.

Data Availability

No new datasets were generated or analysed in this conceptual study. The analysis is based on publicly available legal and policy documents and published literature cited in the References.

Ethics Statement

The study did not involve human participants, surveys, interviews, experiments, or the processing of personal data; therefore, human-subject ethics approval was not required for the work reported in this article.

References

Barsky, A. E. (2016). The ethics of app-assisted family mediation. Conflict Resolution Quarterly, 34(1), 31–42. https://doi.org/10.1002/crq.21168

Barsky, A. E. (2017). Conflict resolution for the helping professions (3rd ed.). Oxford University Press.

Carello, J., & Butler, L. D. (2015). Practicing what we teach: Trauma-informed educational practice. Journal of Teaching in Social Work, 35(3), 262–278. https://doi.org/10.1080/08841233.2015.1030059

Cole, S. F., O'Brien, J. G., Gadd, M. G., Ristuccia, J., Wallace, D. L., & Gregory, M. (2013). Helping traumatized children learn: Creating and advocating for trauma-sensitive schools. Massachusetts Advocates for Children.

European Commission for the Efficiency of Justice. (2019). Guidelines on designing and monitoring mediation training schemes (CEPEJ(2019)8). Council of Europe. https://rm.coe.int/guidelines-on-designing-and--monitoring-mediation-training-schemes-en/1680ac4908

European Parliament & Council of the European Union. (2008). Directive 2008/52/EC of 21 May 2008 on certain aspects of mediation in civil and commercial matters. Official Journal of the European Union, L 136, 3–8. https://eur-lex.europa.eu/eli/dir/2008/52/oj

European Parliament & Council of the European Union. (2016). Regulation (EU) 2016/679 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 (General Data Protection Regulation). Official Journal of the European Union, L 119, 1–88. https://eur-lex.europa.eu/eli/reg/2016/679/oj

Grant, L., & Kinman, G. (2014). Developing resilience for social work practice. Palgrave Macmillan.

Katsh, E., & Rabinovich-Einy, O. (2017). Digital justice: Technology and the Internet of disputes. Oxford University Press.

Law of Ukraine "On Mediation" [Zakon Ukrainy "Pro mediatsiiu"] of November 16, 2021, No. 1875-IX. (2021). Vidomosti Verkhovnoi Rady Ukrainy, (7), Art. 51. https://zakon.rada.gov.ua/laws/show/1875-20#Text

Levenson, J. (2017). Trauma-informed social work practice. Social Work, 62(2), 105–113. https://doi.org/10.1093/sw/swx001

Livingstone, S., & Third, A. (2017). Children and young people's rights in the digital age: An emerging agenda. New Media & Society, 19(5), 657–670. https://doi.org/10.1177/1461444816686318

Ministry of Education and Science of Ukraine. (2019). Standard of higher education for speciality 231 "Social Work" for the first (bachelor's) level of higher education (Order No. 557, April 24, 2019). https://mon.gov.ua/npa/pro-zatverdzhennya-standartu-vishoyi-osviti-za-specialnistyu-231-socialna-robota-dlya-pershogo-bakalavrskogo-rivnya-vishoyi-osviti

Moore, C. W. (2014). The mediation process: Practical strategies for resolving conflict (4th ed.). Jossey-Bass.

Payne, M. (2020). Modern social work theory (5th ed.). Oxford University Press.

Sourdin, T. (2020). Alternative dispute resolution (4th ed.). Thomson Reuters.

van der Kolk, B. A. (2014). The body keeps the score: Brain, mind, and body in the healing of trauma. Viking.

Walsh, S. (2019). Setting out across the sea of monsters: Bringing learning design into mediator training. Conflict Resolution Quarterly, 37(1), 79–94. https://doi.org/10.1002/crq.21255

Yotka, Y. M. (2026). Digital technologies in the formation of communicative and methodological competence of future vocal teachers: A conceptual framework for higher art education. ESS Conference Series Social Science and Humanities, 1(1). https://doi.org/10.54658/esscssh.2026.1.1.07

Digital Technologies In The Formation Of Communicative And Methodological Competence Of Future Vocal Teachers: A Conceptual Framework For Higher Art Education

Yaroslav M. Yotka
Department of Vocal and Choral Mastery
Faculty of Pedagogy, Psychology, Social Work and Arts
Nizhyn Mykola Gogol State University
Nizhyn, Ukraine
ORCID iD: 0000-0002-6885-6687
yotka.yaroslav@ndu.edu.ua

Abstract.
Digital technologies are becoming embedded in higher music education, yet their pedagogical value in vocal teacher preparation depends on how they are integrated into professional competence rather than on technological novelty itself. This conceptual study develops a framework for the formation of communicative and methodological competence of future vocal teachers in digitally enriched higher art education. The study uses structured conceptual analysis of research on vocal pedagogy, digital and AI-supported music education, teacher digital competence, and human-centred AI guidance. It distinguishes communicative competence as a combination of cognitive, verbal, non-verbal, emotional-dialogic and digital interaction capacities, and methodological competence as a combination of theoretical, procedural, diagnostic, reflective, technological and ethical capacities. Recent evidence suggests that digital tools can support feedback, reflection, practice design and teacher technological-pedagogical knowledge, while not consistently outperforming conventional instruction in musical performance outcomes. On this basis, the article proposes a six-block conceptual model linking professional aims, pedagogical principles, competence content, digitally mediated practice, reflective assessment and governance conditions. The model treats AI literacy, data stewardship, equitable access, vocal health and preservation of teacher judgement as conditions of responsible digitalisation. The contribution lies in integrating communication, methodology and digital governance into one framework for pre-service vocal teacher education. The model is conceptual and requires empirical validation through competence rubrics, longitudinal observation and controlled comparison of digitally supported and conventional training practices.

Keywords: *vocal pedagogy; teacher competence; digital music education; artificial intelligence; reflective practice; higher art educationy.*

1.Introduction

Digital transformation has become a structural feature of higher education rather than a temporary response to emergency remote teaching. In music and art education, however, the consequences of digitalisation are unusually complex because learning depends not only on access to information but also on embodied demonstration, auditory discrimination, artistic interpretation, interpersonal trust and repeated guided practice. Vocal pedagogy is especially sensitive to this tension. The voice is an internal instrument whose functioning cannot be observed directly by the learner, while many aspects of singing are experienced through

bodily sensation, acoustic feedback and teacher-guided interpretation. Digital technologies can broaden the means through which these processes are represented and discussed, but they can also encourage excessive visualisation, fragmented feedback or unwarranted confidence in automated analysis.

The professional preparation of future vocal teachers therefore requires more than the acquisition of isolated digital skills. A teacher must be able to decide when a digital tool serves a vocal objective, how its output should be interpreted, what information should remain under human judgement, and how technology changes the communicative relationship between teacher and student. In this context, communicative competence concerns the teacher's capacity to establish pedagogically and artistically meaningful interaction, while methodological competence concerns the capacity to design, diagnose, adapt, assess and improve the learning process. Digital competence intersects with both: it changes the media through which communication occurs and expands the repertoire of methodological actions available to the teacher.

Recent scholarship provides growing evidence for the educational relevance of digital and AI-supported music tools. Systematic reviews identify personalised practice, timely feedback, interactive learning and digital materials as recurrent affordances of AI in music education (Zhang et al., 2024; Wang et al., 2025). Research focused on sight-singing and aural training similarly reports benefits from adaptive and interactive technologies, while noting continuing problems of access, teacher preparation and algorithmic transparency (Chen & Lin, 2026). In vocal education specifically, spectrum-based approaches have been discussed as a way of making selected acoustic features more visible to learners (Du & Idris, 2025), and an experimental study of pre-service teachers found that AI-assisted feedback combined with audio comparison and reflective journaling improved metacognitive outcomes, although it did not demonstrate a superior group-by-time effect for singing performance itself (Li et al., 2025). This distinction is important: current evidence supports the pedagogical usefulness of digital feedback and reflection more clearly than it supports claims that AI can replace expert vocal instruction.

At the same time, research on pre-service music teachers shows that competence development depends on pedagogical design rather than on access to generative AI alone. Li, Chai, and Wang (2025) found that a structured design-with-AI intervention enhanced pre-service music teachers' self-perceived GenAI-related technological pedagogical content knowledge (TPACK) and encouraged critical evaluation of generated outputs. At the policy level, UNESCO's AI Competency Framework for Teachers emphasises a human-centred mindset, AI ethics, AI foundations, AI pedagogy and professional learning, and explicitly connects teacher competence with human agency, sustainability and enabling institutional conditions (Miao & Cukurova, 2024). These findings suggest that digital competence should not be treated as an additional software skill but as a component of professional judgement.

The remaining gap lies in the connection between this emerging digital evidence and the specific professional architecture of vocal teacher education. Existing studies often analyse particular technologies, performance outcomes or general music-teacher digital competence. Less attention is given to how digital practices simultaneously reshape two core capacities of a future vocal teacher: the ability to communicate complex embodied vocal

phenomena and the ability to make methodologically justified pedagogical decisions. The present article addresses this gap by developing a conceptual framework in which digital technologies function as mediators of communication, diagnosis, reflection and learning design rather than as autonomous determinants of educational quality.

The question also has a sustainable-governance dimension. Higher education institutions must decide which tools are approved, how student voice recordings are stored and reused, how unequal access to equipment is addressed, how teachers are trained, and how responsibility is allocated when AI-generated feedback is inaccurate. Sustainable digitalisation in art education therefore means the capacity to maintain pedagogical quality, human agency, equity and accountability while technologies change. In this sense, institutional governance is not external to competence formation: it defines the conditions under which digital competence can be exercised responsibly.

2. Research Aim, Questions And Method

The aim of the article is to develop a conceptually grounded model for forming the communicative and methodological competence of future vocal teachers through digital technologies in higher art education. The study addresses four questions: (1) Which components of communicative and methodological competence are specifically affected by digitalisation? (2) Which digitally mediated practices have a plausible or evidence-supported role in competence formation? (3) What conditions are required to prevent technology from displacing artistic judgement, vocal health and teacher responsibility? and (4) How can these elements be integrated into a coherent framework suitable for curriculum design and subsequent empirical testing?

Methodologically, the article uses structured conceptual analysis and pedagogical modelling. It draws on four bodies of material: scholarship on communicative and methodological competence in vocal and music teacher education; peer-reviewed studies and systematic reviews on digital and AI-supported music learning; empirical studies of feedback, reflection and teacher AI/TPACK development; and authoritative guidance on human-centred and ethical AI in education. The review is integrative rather than systematic: it does not claim exhaustive database coverage, calculate pooled effects or apply PRISMA screening procedures. Sources are used to clarify concepts, identify convergent pedagogical mechanisms and delimit claims that cannot yet be supported by evidence.

The analytical procedure consisted of four steps. First, the professional functions of a vocal teacher were grouped around communication and methodological decision-making. Second, digital practices were mapped to those functions according to their educational role rather than their brand or technical novelty. Third, the potential benefits of each practice were paired with limiting conditions such as validity of feedback, privacy, access and preservation of human judgement. Fourth, these relationships were synthesised into a conceptual model and an implementation matrix. No survey, experiment, interview or observation was conducted for the present study; therefore, statements about competence development are theoretical propositions informed by prior research, not original measured outcomes.

3. Competence Architecture Of The Future Vocal Teacher

3.1. Communicative competence in digitally mediated vocal pedagogy

Communicative competence in vocal pedagogy may be defined as the integrated capacity to organise clear, ethical, emotionally sensitive and artistically meaningful interaction with a learner. Its specificity follows from the nature of vocal instruction. Teachers frequently need to translate invisible physiological and acoustic processes into language, demonstration, metaphor, gesture and sound. Explanations of breath coordination, resonance, registration, diction or timbral balance cannot be reduced to terminology alone; they require attention to what the learner hears, feels and understands.

For conceptual purposes, five interrelated components can be distinguished. The cognitive-verbal component includes specialised vocabulary and the ability to explain it in accessible form. The demonstrative-non-verbal component includes vocal modelling, gesture, posture and visual cues. The emotional-dialogic component includes empathy, psychological safety, questioning and listening to the student's subjective sensations. The artistic-interpretive component concerns communication of style, phrasing, character and meaning. The digital-communicative component concerns asynchronous comments, annotated recordings, online lesson etiquette, multimodal explanations and the critical use of AI-mediated dialogue.

Digitalisation changes communicative competence by increasing the number of representational channels available to the teacher. A student may receive an audio comparison, a marked score, a short video demonstration, a spectrogram, written comments and reflective prompts. Such multimodality can make feedback more persistent and reviewable. Yet more channels do not automatically produce better communication. When feedback is excessively technical, contradictory or decontextualised, the learner may attend to visible metrics rather than musical intention or bodily sensation. Communicative competence therefore includes the ability to select the minimum useful representation and to translate digital evidence back into an intelligible vocal task.

3.2. Methodological competence as professional decision-making

Methodological competence is the capacity to design, conduct, evaluate and improve vocal learning through reasoned pedagogical decisions. It transforms teaching from the imitation of inherited practices into reflective professional action. The future vocal teacher must be able to formulate objectives, select repertoire, construct exercises, sequence tasks, distinguish technical from musical or psychological difficulties, monitor progress and adapt teaching to the learner's vocal development.

Six components are especially relevant. The theoretical component covers voice science, acoustics, repertoire, style and pedagogy. The procedural-design component concerns lesson planning and sequencing. The diagnostic component concerns identification of the most plausible source of a difficulty and the limits of the teacher's competence. The adaptive component concerns modifying tasks for individual voices and learning conditions. The reflective-assessment component concerns evidence-based evaluation of both student pro-

gress and the teacher's own choices. The technological-ethical component concerns selecting digital tools, interpreting their outputs, protecting learner data and recognising when a technological intervention is methodologically unnecessary.

Digital tools can support methodological competence only when the student teacher must justify their use. Creating a vocalise in notation software is methodologically meaningful when range, tessitura, vowel, rhythm and progression of difficulty are linked to a defined learning objective. Analysing a recording is meaningful when the observed acoustic feature is connected cautiously to audible performance and a pedagogical response. Asking a generative AI system to produce lesson ideas is meaningful when the student evaluates, rejects and revises those ideas using domain knowledge. The methodological task is therefore not tool operation but reasoned selection, interpretation and adaptation.

3.3. Digital competence as a cross-cutting professional condition

The framework proposed here does not treat digital competence as a third independent competence alongside communication and methodology. Instead, it functions as a cross-cutting condition that modifies both. This position is consistent with contemporary teacher-AI frameworks that place AI use within pedagogy, ethics, professional learning and human-centred decision-making rather than within a narrow category of software proficiency (Miao & Cukurova, 2024). For future vocal teachers, digital competence comprises tool literacy, AI literacy, data literacy, critical evaluation of automated output, online communication, copyright awareness, privacy and basic information-security behaviour. Its quality is demonstrated not by the number of platforms a student can use but by the quality of professional decisions made with and about those platforms.

4. Evidence-Informed Digital Practices And Their Pedagogical Boundaries

A useful way to organise digital technologies in vocal teacher education is by educational function. This avoids rapid obsolescence caused by listing particular commercial products and focuses instead on what the technology enables the learner or teacher to do. Systematic reviews in music education distinguish practice, theory/literacy, creativity and feedback functions, while also warning that the evidence base remains heterogeneous and methodologically uneven (Liu et al., 2025; Zhang et al., 2024). For vocal teacher preparation, six functional groups are especially relevant: notation and resource design; recording and video feedback; acoustic visualisation; generative AI and conversational support; blended learning and digital portfolios; and collaborative/creative media production.

Table 1. Functional classification of digital practices in pre-service vocal teacher education

Functional group	Typical uses	Potential competence contribution	Pedagogical boundary / condition
Notation and resource design	Notation software, digital scores, accompaniment and transposition tools	Designing exercises and explaining musical tasks; adapting repertoire to range and learning goals	The student teacher must justify pedagogical purpose, range, tessitura and progression; notation should not substitute for listening.
Recording and video feedback	Audio/video capture, annotation, comparison and portfolio tools	Persistent feedback, self-observation, peer dialogue and reflective assessment	Recording can increase self-consciousness; assessment criteria and psychologically safe feedback are required.
Acoustic visualisation	Pitch tracking, spectrum and other voice-analysis tools	Supporting diagnostic questioning and multimodal explanation of selected acoustic features	Visual metrics are proxies, not artistic verdicts; inaccurate interpretation can encourage unhealthy or mechanically optimised singing.
Generative AI	LLM-based dialogue, planning support, prompts, rubrics and resource drafting	Supporting reflective questions, alternative lesson ideas and critical pedagogical design	Outputs require verification; teacher judgement, copyright, privacy and bias must remain explicit learning objectives.
Blended learning and portfolios	LMS, video conferencing, e-portfolios and reflective journals	Organising independent preparation, asynchronous communication and longitudinal evidence of growth	Unequal access, platform overload and poor audio quality can reduce educational value.
Collaborative and creative digital production	Shared media, simple editing, presentation and content-creation tools	Developing communication, presentation, creativity and public-facing professional literacy	Production quality should remain subordinate to musical and pedagogical aims; permissions are required for identifiable recordings.

4.1. Feedback, reflection and metacognition

Feedback and reflection provide the strongest conceptual bridge between communicative and methodological competence. Digital recording allows the learner to revisit an event that would otherwise disappear after performance. Annotation and comparison can make feedback more specific, while reflective journals can require the student to explain what changed, why it changed and what should happen next. Importantly, recent experimental evidence in vocal training supports a cautious rather than triumphalist interpretation. Li et al. (2025) found that AI-assisted feedback, audio comparison and reflective writing produced stronger metacognitive development, but the intervention did not show a superior interaction effect for singing performance. This suggests that digitally supported reflection may strengthen the learner's capacity to monitor and regulate practice even when measurable performance advantages are less clear.

For teacher education, this distinction is productive. A future vocal teacher should not be trained to believe that a tool ‚improves singing' by itself. The student should instead learn to use recordings and automated feedback as evidence for professional reasoning: identify a problem, compare sources of evidence, formulate a hypothesis, select an intervention and evaluate the result. Such a cycle directly links communicative feedback to methodological decision-making.

4.2. Generative AI and the formation of pedagogical judgement

Generative AI deserves separate treatment because it produces language, suggestions and instructional materials in a form that resembles professional reasoning. Its educational risk is therefore epistemic as well as technical: fluent output may conceal weak domain understanding. Research with pre-service music teachers indicates that structured design tasks can turn this weakness into a learning opportunity when students are required to critique and revise AI-generated materials rather than accept them as finished products (Li, Chai, & Wang, 2025). In such tasks, competence is demonstrated through evaluation: Is the suggested exercise vocally safe? Is the repertoire appropriate? Does the explanation use terminology accurately? Is the feedback artistically meaningful? What evidence supports the recommendation?

A human-centred approach also requires explicit limits. UNESCO guidance emphasises human agency, ethical validation, data privacy and pedagogical appropriateness in educational AI (Miao & Holmes, 2023; Miao & Cukurova, 2024). In vocal education this means that generative AI should not be positioned as an autonomous assessor of artistic quality, a substitute for specialist diagnosis or a decision-maker about vocal health. Its legitimate educational roles are narrower: generating alternatives, supporting reflection, drafting low-stakes resources and creating material that students can critically evaluate.

4.3. Acoustic analysis and embodied knowledge

Spectrum and pitch-analysis tools can help students connect listening with selected measurable properties of sound. Du and Idris (2025) identify spectrum-based pedagogy as a developing approach in vocal music education, and Zhang (2026) reports the use of mobile and wearable technologies in vocal training. These studies expand the available evidence base, but the pedagogical interpretation remains crucial. Acoustic representations do not display ‚correct singing' in a complete sense. They isolate measurable features from a complex embodied and artistic event. A future teacher should therefore be taught to triangulate: listen, observe, ask about bodily sensation, consider musical context and use visual data only where it answers a defined pedagogical question.

5. Conceptual Model Of Competence Formation

On the basis of the preceding analysis, the article proposes a six-block model of competence formation. The model is cyclical rather than linear: practice generates evidence, evidence supports reflection, reflection modifies methodological decisions, and those decisions reshape communication in the next learning episode. Digital technologies enter the cycle only where they perform a defined educational function. Governance conditions surround the cycle because access, privacy, institutional rules and teacher capacity determine whether the same technology becomes pedagogically useful or problematic.

Table 2. Conceptual model for communicative and methodological competence formation through digital technologies

Block	Core content	Observable educational result
1. Target block	Formation of communicative clarity, methodological judgement and responsible digital-pedagogical readiness	Students can explain why technology is used and identify what should remain under human judgement.
2. Principle block	Student-centredness, artistic integrity, vocal health, human agency, evidence-informed practice, equity and ethics	Digital choices are evaluated against pedagogical and human criteria, not novelty.
3. Content block	Vocal pedagogy, methodology, communication, assessment, digital/AI literacy and data stewardship	Professional knowledge is integrated across artistic, pedagogical and technological domains.
4. Practice block	Exercise design, recording analysis, video feedback, AI critique, online teaching episodes, peer assessment and e-portfolios	Students practise professional decisions in authentic or simulated pedagogical situations.
5. Reflective-assessment block	Rubrics, self-explanation, peer/teacher feedback and portfolio evidence	Students make their reasoning visible and revise decisions on the basis of evidence.
6. Governance block	Approved tools, access, consent, data retention, staff support, escalation of health/safeguarding concerns	Technology use remains accountable, equitable and sustainable at institutional level.

The novelty of the model lies not in introducing an additional list of digital tools, but in relocating technology within the competence cycle. The same platform can contribute to competence or weaken it depending on the task. For example, generative AI used to produce a ready-made lesson plan with no evaluation may reduce methodological reasoning, whereas the same system used to generate three contrasting plans that students must diagnose, critique and redesign can make reasoning explicit. Likewise, a spectrogram used as an aesthetic score can distort vocal learning, while a spectrogram used to test a carefully formulated acoustic hypothesis can strengthen diagnostic thinking.

6. Governance Conditions For Sustainable Digital Vocal Teacher Education

The institutional dimension is essential because individual teacher competence cannot compensate indefinitely for poor governance. Sustainable digitalisation requires arrangements that preserve educational continuity, equity, accountability and human agency as tools and vendors change. This is particularly important in art education, where commercially available applications may be adopted informally before institutions establish rules for recordings, AI services or student consent.

6.1. Human agency and professional responsibility

The first governance principle is that technology should extend, not transfer, professional responsibility. The teacher remains accountable for pedagogical decisions, and students should learn that automated output is advisory evidence rather than authority. This principle aligns with UNESCO's teacher AI competency framework, which places a human-centred mindset and ethics before technical application (Miao & Cukurova, 2024). In practical terms, programmes should identify decisions that require human review: repertoire selection where vocal health is implicated, feedback on possible dysfunction, high-stakes assessment, safeguarding issues and any decision based on sensitive personal information.

6.2. Voice recordings, privacy and data stewardship

Vocal teacher education routinely generates identifiable audio and video recordings. Once recordings are uploaded to cloud platforms, AI services or shared portfolios, their educational use becomes a data-stewardship issue. Institutions should define who may record, the purpose of recording, where files are stored, who may access them, how long they are retained and whether they may be reused for teaching or AI-supported analysis. Consent should be meaningful and linked to a specific educational purpose. Student teachers should also learn to minimise data disclosure: a recording or document should not be uploaded to an external AI service merely because doing so is technically possible.

6.3. Equity, access and the digital divide

The second sustainability condition is equitable access. High-quality microphones, stable broadband, current devices and paid software are unevenly distributed. Systematic reviews in music education repeatedly identify access and teacher preparation as constraints on digital implementation (Chen & Lin, 2026; Liu et al., 2025). Consequently, programmes should avoid designing mandatory learning outcomes around tools that only some students can obtain. Institutional licences, shared equipment, low-bandwidth alternatives and equivalent non-digital routes are governance mechanisms that protect equal participation.

6.4. Capacity building and tool lifecycle

A third condition is institutional capacity. Digital sustainability is weakened when a course depends on one enthusiastic teacher or one rapidly changing platform. Teacher educators require continuing professional development in AI literacy, data protection and domain-specific digital pedagogy. Tools should be reviewed periodically for educational relevance, accessibility, data practices and continuity. This shifts the question from ‚Which app should we use?' to ‚Which educational function must the programme support, and what is the safest and most sustainable way to support it?' Such governance reduces technological overload and makes curricula more resilient to platform change.

7. Curriculum Implementation And Assessment

The conceptual model can be implemented without creating a separate technology course. A stronger approach is to embed digitally mediated tasks within existing vocal pedagogy, methodology and teaching-practice modules. The developmental sequence should move from controlled use to critical design and, finally, to justified independent selection. This mirrors the progression from acquiring foundational AI competence to deepening and creating pedagogical applications described in international teacher-competency guidance (Miao & Cukurova, 2024).

Table 3. Suggested curriculum sequence and assessment evidence

Stage	Learning activity	Competence focus	Assessment evidence
Stage 1: Guided literacy	Introduction to recording, notation, LMS and AI principles; privacy and ethical scenarios	Identify tool function; distinguish data from interpretation; recognise unsafe or unnecessary uses	Short critique; terminology quiz; privacy/ethics case response
Stage 2: Structured application	Design a vocal exercise; annotate a recording; compare human and AI feedback	Connect a digital action to a vocal objective; explain limitations and adaptations	Rubric-scored teaching artefact plus reflective rationale
Stage 3: Pedagogical design	Plan a blended teaching episode using selected tools and alternatives	Integrate communication, methodology and access considerations	Microteaching, peer review and revision
Stage 4: Reflective practice	Build an evidence-based e-portfolio across several teaching episodes	Evaluate changes in teaching decisions and feedback quality over time	Portfolio defence and self-assessment
Stage 5: Independent professional judgement	Select or reject digital tools for a complex learner scenario	Demonstrate justified, ethical and sustainable decision-making	Case-based oral defence using a competence rubric

Assessment should prioritise reasoning rather than the polished appearance of digital products. A student who produces an attractive video but cannot explain the pedagogical purpose, limitations or data implications has not demonstrated methodological competence. Conversely, a student who rejects an AI tool because the feedback is unreliable for the specific vocal problem may demonstrate a higher level of digital-pedagogical judgement than a student who uses the tool extensively. Suggested rubric dimensions include clarity of pedagogical objective, quality of vocal-methodological reasoning, communication and feedback, critical interpretation of digital evidence, ethical/data awareness, accessibility and reflective revision.

8. Challenges, Limitations And Research Agenda

Four challenges remain central. First, technological overload can fragment attention and shift lesson time from listening and embodied learning to interface management. Second, algorithmic and measurement limitations can create false precision, particularly when complex artistic outcomes are reduced to pitch, frequency or automated text feedback. Third, unequal access can reproduce rather than reduce educational inequality. Fourth, AI and cloud-based services can externalise data and decision processes beyond the direct control of the teacher or institution. These challenges do not justify rejecting digital technologies, but they require selective adoption and explicit governance.

The present study also has clear limitations. It is conceptual and does not test the proposed model with a cohort of future vocal teachers. The literature base is interdisciplinary and heterogeneous, and findings from general music education, elementary music or teacher-AI studies cannot be transferred automatically to one-to-one vocal pedagogy. Several recent studies come from particular national and institutional contexts, so cultural and curricular transfer requires caution. The article therefore avoids quantitative claims about the magnitude of competence improvement and treats the proposed relationships as hypotheses for empirical validation.

Future research should proceed in three directions. The first is measurement: validated

rubrics are needed for communicative, methodological and digital-pedagogical competence in vocal teaching. The second is comparative intervention research: studies should distinguish outcomes such as metacognition, teaching judgement, vocal performance, learner autonomy and feedback quality rather than assuming that all improve together. The third is longitudinal and governance-oriented research: it should examine whether digitally enriched training changes graduates' actual teaching practices, how institutional rules affect adoption, and whether access, privacy and technology costs create differential outcomes across student groups.

9. Conclusions

Digital technologies can make a substantive contribution to the professional preparation of future vocal teachers, but their value is conditional. The central educational problem is not the acquisition of individual applications; it is the formation of professional judgement capable of integrating artistic goals, vocal health, communication, methodology and digital evidence. Communicative competence enables the future teacher to explain, demonstrate, listen, give feedback and sustain artistic dialogue across face-to-face and digital environments. Methodological competence enables the teacher to design, diagnose, adapt, assess and revise teaching. Digital competence modifies both by adding new media, new forms of evidence and new ethical responsibilities.

The conceptual model developed in this article integrates these capacities through six blocks: target, principles, content, practice, reflective assessment and governance. The model positions recording, acoustic analysis, generative AI, digital portfolios and blended-learning environments as pedagogical mediators rather than autonomous sources of educational quality. Recent empirical studies support this restrained interpretation: digitally and AI-supported practices can strengthen reflection, metacognition and teacher technological-pedagogical knowledge, while evidence for superior musical performance outcomes is more context-dependent. The appropriate educational response is therefore neither technological enthusiasm nor rejection, but structured critical use.

The scientific contribution of the article is the integration of communicative and methodological competence with digital-pedagogical judgement and institutional governance in a single framework specific to vocal teacher education. Its practical significance lies in a curriculum logic that can be implemented through existing pedagogy and teaching-practice modules and assessed through observable reasoning, feedback, design and reflective evidence. Sustainable digitalisation of higher art education requires more than competent individuals: institutions must also provide equitable access, data stewardship, approved and reviewable tools, teacher development and clear preservation of human responsibility. Empirical validation of the model is the next necessary step.

Funding

This research received no external funding.

Conflicts of Interest

The author declares no conflicts of interest.

Data Availability

No original datasets were generated or analysed in this conceptual study. The article is based on published scholarly and policy sources cited in the reference list.

Ethics Statement

The study did not involve human participants, personal data collection or experimental procedures; institutional ethics approval was therefore not required for the present conceptual analysis.

References

Chen, Z.-L., & Lin, H. (2026). AI and digital technologies in sight-singing and aural training: A systematic review of innovations in higher music education. European Journal of Education, 61(1), e70502. https://doi.org/10.1111/ejed.70502

Du, E., & Idris, M. O. (2025). Breaking the sound barrier: Spectrum-based pedagogies in modern vocal music education. Jurnal Cakrawala Pendidikan, 44(3), 523–538. https://doi.org/10.21831/cp.v44i3.84011

Gao, Y. (2025). Digital tools in instrumental and vocal pedagogy: A pre- and post-pandemic analysis at the university level. Journal of Education and Educational Research, 15(3), 35–39. https://doi.org/10.54097/zbck7a58

Li, H., Chai, C. S., & Wang, X. (2025). Promoting pre-service music teachers' TPACK with generative AI: An intervention through designing with AI. Computers and Education: Artificial Intelligence, 9, 100525. https://doi.org/10.1016/j.caeai.2025.100525

Li, W., Cui, X., Manoharan, P., Dai, L., Liu, K., & Huang, L. (2025). AI-assisted feedback and reflection in vocal music training: Effects on metacognition and singing performance. Frontiers in Psychology, 16, 1598867. https://doi.org/10.3389/fpsyg.2025.1598867

Liu, Y., Tran, V. C., Kiss, B., Oo, T. Z., Szabó, N., & Józsa, K. (2025). The use and effectiveness of digital tools in elementary music education: A systematic review. Music & Science, 8. https://doi.org/10.1177/20592043251363338

Miao, F., & Cukurova, M. (2024). AI competency framework for teachers. UNESCO. https://unesdoc.unesco.org/ark:/48223/pf0000391104

Miao, F., & Holmes, W. (2023). Guidance for generative AI in education and research. UNESCO. https://unesdoc.unesco.org/ark:/48223/pf0000386693

Shumska, L., Chyncheva, L., Dorokhina, L., Homenko, A., & Yotka, Y. (2024). Innovative vocal technologies in the educational choir of a higher education institution: A competency-based approach. Multidisciplinary Reviews, 7, Article 2024spe044. https://doi.org/10.31893/multirev.2024spe044

Wang, Y., Karim, A. A., & Kamsin, I. F. (2025). The use of AI in music teaching in higher education: A systematic literature review. International Journal of Learning, Teaching and Educational Research, 24(11), 39–72.

https://doi.org/10.26803/ijlter.24.11.3
Yotka, Y. (2023). Vocal-pedagogical activity: Theoretical aspect. Pedahohika Formuvannia Tvorchoi Osobystosti u Vyshchii i Zahalnoosvitnii Shkolakh [Pedagogy of the Formation of a Creative Personality in Higher and General Education Schools], 88, 118–123. https://doi.org/10.32840/1992-5786.2023.88.21
Yotka, Y. (2024a). Formation of communicative competence of future vocal disciplines teachers. Journal of International Legal Communication, 14(3), 40–50. https://doi.org/10.32612/uw.27201643.2024.14.3.pp.40-50
Yotka, Y. M. (2024b). Formuvannia metodychnoi kompetentnosti maibutnikh vykladachiv vokalnykh dystsyplin yak determinanta uspishnoi pedahohichnoi diialnosti [Formation of methodological competence of future vocal teachers as a determinant of successful pedagogical practice]. Naukovi Zapysky. Seriia: Psykholoho-Pedahohichni Nauky [Scientific Notes. Series: Psychological and Pedagogical Sciences], 3, 99–107. https://doi.org/10.31654/2663-4902-2024-PP-3-99-107
Zhang, L. (2026). ICT training with wearable devices to enhance emotional communication and musicality in vocal education. Scientific Reports, 16, Article 15382. https://doi.org/10.1038/s41598-026-46822-1
Zhang, Y., Beh, W. F., Zhang, C., & Pi, S. (2024). Transforming music education through artificial intelligence: A systematic literature review on enhancing music teaching and learning. International Journal of Interactive Mobile Technologies, 18(18), 76–93. https://doi.org/10.3991/ijim.v18i18.50545

Greening Tools In Transport And Logistics Operations: A Policy-Instrument Classification And Governance Assessment

Maryna V. Halkevych
Department of Business and Tourism Management
Izmail University of Humanities
Izmail, Odesa Oblast, Ukraine
ORCID iD: 0000-0002-4786-4856
marinchik.vladi@gmail.com

Tetiana A. Voichenko
Department of Logistics
State University "Kyiv Aviation Institute"
Kyiv, Ukraine
ORCID iD: 0000-0002-0109-4622
larino101266@gmail.com

Tetiana K. Metil
Department of Business and Tourism Management
Izmail University of Humanities
Izmail, Odesa Oblast, Ukraine
ORCID iD: 0000-0002-4553-4343
tatanametil@gmail.com

Abstract.

The decarbonisation of transport and logistics is not only a technological challenge but also a problem of policy design, investment sequencing, institutional capacity, and corporate implementation. This article develops a five-part classification of greening tools used in transport and logistics operations and interprets them as a coordinated policy-instrument portfolio. The framework distinguishes legal and regulatory instruments, technical and technological solutions, economic instruments, organisational-managerial tools, and informational-analytical mechanisms. The study uses a structured integrative review of the literature cited in the manuscript, comparative analysis of European Union and Ukrainian regulatory sources, and qualitative evidence synthesis. It deliberately avoids pooled effect-size estimates because the underlying studies use heterogeneous units, baselines, technologies, and system boundaries. The analysis shows that the five instrument families are complementary: regulation establishes minimum requirements, economic instruments alter investment incentives, infrastructure and technology enable compliance, organisational measures improve operational efficiency, and information systems make performance measurable and auditable. For Ukraine, the central challenge is to combine EU-alignment obligations with wartime resilience and reconstruction priorities. The article therefore proposes a governance sequence based on measurement, regulatory alignment, infrastructure planning, targeted finance, implementation, and verification. The contribution is a transparent classification and decision framework rather than a claim that a single universal emissions-reduction percentage can be assigned to an integrated portfolio.

Keywords: *green logistics; transport decarbonisation; policy instruments; environmental regulation; sustainable governance; Ukraine.*

1. Introduction

Transport and logistics sit at the intersection of economic connectivity and climate policy. Freight movement supports trade, industrial production, food security, e-commerce, and post-crisis recovery, but it also depends heavily on energy-intensive vehicles, terminals, warehouses, and supporting infrastructure. The resulting policy problem is therefore two-sided: governments and firms must preserve the reliability and affordability of logistics while progressively reducing its environmental burden. In this setting, greening cannot be reduced to the purchase of cleaner vehicles. It requires a coordinated set of rules, incentives, infrastructure investments, management practices, and information systems.

The concept of green logistics has developed as part of the broader literature on green supply chain management. Early work emphasised the integration of environmental considerations into procurement, production, distribution, reverse flows, and end-of-life management (Srivastava, 2007). Subsequent research has shown that environmental performance is shaped by institutional pressure, managerial commitment, collaboration, operational design, and technological capability rather than by a single intervention (Sarkis et al., 2011; Zhu et al., 2013; Centobelli et al., 2017). This makes classification important: policy makers and managers need to understand not only what tools exist, but what function each tool performs and how tools interact.

For the European Union, the governance architecture for transport decarbonisation has become more concrete. Revised CO2 standards for new heavy-duty vehicles set fleet-wide reduction targets relative to the 2019 baseline of 45% from 2030, 65% from 2035, and 90% from 2040 for the relevant vehicle groups (European Parliament and Council of the European Union, 2024). Regulation (EU) 2023/1804 on alternative fuels infrastructure establishes mandatory deployment requirements for recharging and refuelling infrastructure and places particular emphasis on the progressive coverage of the trans-European transport network. A separate emissions trading system for buildings, road transport and additional sectors (ETS2) is also part of the policy mix; it regulates fuel suppliers upstream and is scheduled to become fully operational in 2028 (European Commission, 2026a). These measures illustrate a central point of this article: technology adoption is conditioned by the surrounding regulatory and infrastructure environment.

For Ukraine, the same issue is intensified by the simultaneous demands of European integration, wartime resilience, and reconstruction. Ukraine completed the bilateral screening process with the European Union in 2025 and continues to align national law and administrative capacity with the EU acquis (European Commission, 2025). At the same time, transport and energy infrastructure remain among the sectors most affected by the war and among the largest areas of reconstruction need (European Commission, 2026b). The policy challenge is therefore not to copy isolated European instruments, but to sequence legal approximation, investment, financing, infrastructure renewal, and verification in a way that remains feasible under severe fiscal and security constraints.

This article addresses three research problems. First, existing green-logistics literature uses overlapping classifications, which makes it difficult to distinguish policy instruments from the operational objects on which they act. Second, environmental-effectiveness claims

are often transferred across technologies and contexts even though studies use different baselines, functional units, time horizons, and system boundaries. Third, the Ukrainian context requires an explicit governance interpretation that connects corporate greening with accession-driven regulatory change and reconstruction policy.

The aim is to develop a transparent classification of greening tools in transport and logistics operations and to assess their role within a coordinated governance framework. The objectives are: (1) to distinguish five principal instrument families; (2) to clarify the mechanism through which each family can influence environmental performance; (3) to update the EU and Ukrainian regulatory context; (4) to identify the limits of quantitative comparison across heterogeneous evidence; and (5) to formulate a practical sequencing framework for Ukraine. The article does not claim to provide a meta-analysis or a universal pooled emissions-reduction estimate.

2. Literature Review

2.1. Green supply chain management and logistics decarbonisation

Green supply chain management provides the broad theoretical foundation for analysing transport and logistics greening. Srivastava (2007) framed the field as the integration of environmental thinking into supply-chain management across product design, sourcing, manufacturing, delivery, and end-of-life management. Sarkis et al. (2011) and Zhu et al. (2013) further emphasised that organisational and institutional pressures shape the adoption of green practices. This literature is important because it explains why the environmental performance of logistics is not determined solely by vehicle technology: supplier relationships, management systems, regulation, and information all influence implementation.

Environmental measures in transport and logistics can be grouped by the part of the system they seek to change. Technical interventions include vehicle electrification, alternative powertrains, energy-efficient buildings, and charging or refuelling infrastructure. Operational interventions include routing, consolidation, load-factor improvement, modal choice, and reverse logistics. Governance interventions include standards, taxes, subsidies, carbon pricing, public procurement, disclosure, and environmental management systems. The analytical difficulty is that these categories operate at different levels and are therefore not directly comparable in a single effect-size table.

2.2. Technology and infrastructure

The literature on freight technology shows substantial decarbonisation potential from electrification, but the practical result depends on route characteristics, payload, vehicle duty cycle, charging availability, electricity generation, and capital cost. Liimatainen et al. (2019), for example, demonstrate that the feasibility of electric trucks varies markedly across freight tasks. The implication is that a percentage taken from one vehicle class or electricity mix cannot be transferred automatically to another.

Infrastructure is equally important. Alternative-fuel vehicles create little system-level value if the necessary charging or refuelling network is absent or unreliable. Regulation (EU) 2023/1804 reflects this complementarity by setting infrastructure deployment

requirements alongside vehicle decarbonisation policy. In warehouse operations, studies such as Meneghetti and Monti (2015) illustrate the potential of energy-aware facility design, but the magnitude of savings depends on warehouse type, climate, refrigeration demand, automation, and baseline technology. Such evidence supports the direction of greening, not a universal percentage applicable to every logistics facility.

2.3. Organisational and digital tools

Operational efficiency remains one of the most accessible routes to lower emissions intensity. Better vehicle utilisation, freight consolidation, route design, and modal optimisation can reduce unnecessary vehicle-kilometres and energy use. Piecyk and McKinnon (2010) show that the carbon footprint of road freight is sensitive to logistics parameters such as vehicle utilisation and operational efficiency. Digital transport management systems can support these decisions, but digitalisation should be treated as an enabling capability rather than an emissions-reduction measure in itself.

Recent work on digital technologies and sustainable supply chains reinforces this distinction. Winkelmann et al. (2024) discuss how digital tools can support resilience and sustainability through improved information, coordination, and decision-making. The actual environmental outcome, however, depends on the operational decision that follows from the information. A routing algorithm has no direct climate value if it is not integrated into dispatching practice; a carbon dashboard has limited value if no management target or investment decision is linked to it.

2.4. Economic, informational, and institutional drivers

Institutional research consistently identifies regulation, customer requirements, competitive pressure, and managerial commitment as drivers of environmental practice (Zhu et al., 2013; Chatzoudes et al., 2024). Economic instruments change the relative cost of high- and low-emission choices, while informational instruments make performance visible to regulators, investors, customers, and managers. Rao and Holt (2005) connect green supply-chain practices with competitiveness and economic performance, although the relationship is context-dependent and should not be read as proof that every environmental investment generates a short payback period.

Carbon accounting, environmental management systems, sustainability reporting, and audit mechanisms are especially important from a governance perspective. They do not necessarily reduce emissions directly, but they establish baselines, define accountability, and allow policy makers or investors to assess whether operational claims are credible. This evidentiary function is essential in a field where effect estimates can otherwise be detached from their original scope and reused as if they were universally comparable.

2.5. Ukrainian context and research gap

Ukrainian scholarship has examined the ecologisation of logistics systems and the relationship between economic, environmental, and social goals (Velychko & Velychko, 2023). The Ukrainian context nevertheless differs from stable-market settings in three respects:

war-related infrastructure damage, constrained access to long-term capital, and rapid regulatory approximation associated with EU accession. These conditions increase the importance of sequencing and institutional capacity.

The remaining gap is therefore not simply a shortage of lists of green technologies. What is needed is an analytical framework that separates types of instruments, specifies their governance role, and avoids false precision when the underlying evidence is heterogeneous. The present study addresses that gap by combining a five-part typology with an evidence hierarchy and a governance sequence for implementation.

3. Materials And Methods

The study uses a structured integrative review and comparative regulatory analysis. It is conceptual and evidence-synthetic rather than experimental. The source base consists of the peer-reviewed works cited in the manuscript on green logistics, green supply chain management, transport technology, circular supply chains, and institutional drivers, supplemented by authoritative legal and policy sources required to update the regulatory context through 2026. No primary survey, company questionnaire, field experiment, or proprietary emissions dataset was used.

The review process was organised around three analytical questions: what greening instrument is being described; through what mechanism can it influence emissions or environmental performance; and what kind of evidence supports the claimed effect? Sources were coded into five instrument families: legal and regulatory; technical and technological; economic; organisational-managerial; and informational-analytical. The categories are functional rather than mutually exclusive. For example, an electric truck is a technical instrument, while the subsidy that lowers its purchase cost is an economic instrument and the charging-network obligation that makes its operation feasible is a regulatory-infrastructure measure.

The regulatory analysis compares current EU transport-decarbonisation instruments with the policy and institutional challenges relevant to Ukraine. Particular attention is given to the revised heavy-duty vehicle CO2 standards, alternative-fuels infrastructure regulation, ETS2, Ukraine-EU regulatory alignment, and Ukraine's National Renewable Energy Action Plan to 2030. The analysis does not assume that EU measures are automatically transferable; instead, it asks which administrative, financial, and infrastructure capacities are required for implementation.

The article deliberately does not present a PRISMA flow diagram, a pooled effect estimate, or a standardised cross-study gCO2e/tkm meta-analysis. The cited evidence differs in functional units, system boundaries, baselines, technologies, geographic contexts, and time horizons. Combining such values into a single range would create a level of statistical comparability that the source base does not support. Numerical values are retained only where they are directly traceable to authoritative legal targets or clearly scoped source-specific evidence.

The principal limitation is therefore also a design choice: this study evaluates the role, complementarity, and governance relevance of instruments rather than estimating a causal

average treatment effect. Corporate sustainability disclosures are treated as illustrative evidence of organisational practice and not as independently verified sector-wide performance data. This distinction is particularly important for Ukraine, where wartime conditions constrain data availability and comparability.

4. Results And Discussion

4.1. A five-category classification of greening instruments

The synthesis supports a five-category classification. The categories are best interpreted as parts of an instrument portfolio rather than as competing alternatives. Each category addresses a different implementation problem: authority, technology, incentives, operations, or information.

Table 1. Five-category classification of greening tools and their governance function

Category	Representative instruments	Primary mechanism	Governance function
Legal and regulatory	Vehicle emission and CO2 standards; environmental assessment; access rules; procurement requirements; carbon-market rules	Defines mandatory or permitted behaviour	Creates minimum standards and enforceable obligations
Technical and technological	Battery-electric and fuel-cell vehicles; charging and refuelling infrastructure; efficient warehouses; low-carbon energy systems	Changes the physical emissions profile of assets	Provides the technical means to comply with policy goals
Economic	Taxes and charges; grants; purchase incentives; concessional finance; carbon pricing; green bonds	Changes relative costs and investment returns	Makes cleaner investment more or less financially attractive
Organisational--managerial	TMS/WMS; consolidation; load-factor improvement; modal shift; reverse logistics; ISO 14001 systems	Changes how assets and flows are managed	Reduces avoidable activity and embeds continuous improvement
Informational-analytical	GHG accounting; carbon audits; ESG reporting; eco-labelling; digital traceability; performance dashboards	Makes impacts measurable and visible	Supports accountability, verification, and policy learning

The classification clarifies an important conceptual distinction. Technical and organisational measures are the objects through which emissions can be reduced operationally, while legal, economic, and informational instruments often shape whether those measures are adopted. A regulator may set a CO2 standard, create a fiscal incentive, and require disclosure; the firm then responds through fleet, route, warehouse, or energy decisions. The categories therefore operate at different causal levels.

This distinction also explains why an effectiveness table that assigns one percentage range to each category can be misleading. A legal standard does not have a stable direct percentage effect independent of enforcement and technology response. Similarly, an information instrument can be decisive for accountability without reducing one tonne of CO2 by itself. The meaningful unit of analysis is therefore the instrument mix and the implementation pathway.

4.2. The EU regulatory architecture as an instrument mix

The European Union provides a clear example of coordinated instrument design. Regulation (EU) 2024/1610 revised the CO2 performance standards for new heavy-duty vehicles. For the relevant vehicle groups, the fleet-wide targets require reductions of 45% from 2030, 65% from 2035, and 90% from 2040 relative to the 2019 baseline. These are manufacturer fleet targets, not direct claims about the life-cycle emissions of every individual truck. This legal distinction matters when translating EU targets into operational or corporate indicators.

Regulation (EU) 2023/1804 addresses a complementary bottleneck: alternative-fuels infrastructure. It establishes mandatory national targets and common requirements for publicly accessible recharging and refuelling infrastructure and provides for progressive heavy-duty vehicle infrastructure coverage along the TEN-T network. The policy logic is complementary: vehicle standards create demand for cleaner powertrains, while infrastructure rules reduce the risk that insufficient charging or refuelling capacity prevents adoption.

ETS2 adds an economic signal. The system covers emissions from fuels supplied to buildings, road transport, and additional sectors, with regulated fuel suppliers rather than end users responsible for monitoring and surrendering allowances. According to the European Commission's current implementation information, ETS2 is to become fully operational in 2028 (European Commission, 2026a). The important governance point is that carbon pricing does not replace standards or infrastructure policy; it changes the economics within which firms respond to them.

Together, these measures illustrate the logic of an instrument portfolio: standards define the trajectory, infrastructure regulation removes physical bottlenecks, carbon pricing changes operating incentives, and reporting obligations enable verification. The framework developed here uses this logic as a reference point for analysing Ukraine, while recognising that administrative and fiscal capacity differs significantly.

4.3. Ukraine: regulatory alignment, reconstruction, and implementation capacity

Ukraine's transport greening agenda is increasingly connected to EU accession rather than only to the Association Agreement. The European Commission reported the completion of bilateral screening in 2025, creating a technical basis for continued alignment with the acquis. Transport policy and environment and climate change are separate negotiation chapters, but in practice decarbonising logistics requires interaction between both: vehicle rules, infrastructure planning, energy policy, environmental enforcement, statistics, and investment governance.

The domestic policy framework also continues to evolve. In August 2024, the Cabinet of Ministers approved the National Renewable Energy Action Plan for the period to 2030. This is more relevant to the current energy-transition context than the obsolete 2021-2025 formulation previously used in some policy discussions. For logistics, renewable-energy policy matters because the climate value and operating resilience of electrified transport depend increasingly on the electricity system, storage, and grid capacity.

Wartime damage adds a further governance layer. The 2026 update of the joint recovery and reconstruction needs assessment identifies transport and energy among the most heavily affected sectors and shows that transport reconstruction needs remain exceptionally high (European Commission, 2026b). Reconstruction therefore creates both a constraint and a sequencing opportunity: infrastructure that must be rebuilt can be designed for future low-carbon mobility, but only if green standards, financing conditions, interoperability, and maintenance capacity are incorporated at the planning stage.

Table 2. Regulatory and policy architecture relevant to greening transport and logistics

Instrument / framework	Verified role	Implication for logistics governance
EU Regulation 2024/1610 on heavy-duty vehicle CO2 standards	Sets manufacturer fleet CO2 reduction targets for new heavy-duty vehicles: 45% from 2030, 65% from 2035, 90% from 2040 versus 2019 for relevant groups	Creates a predictable long-term technology trajectory for new fleets
EU Regulation 2023/1804 on alternative fuels infrastructure	Sets mandatory deployment requirements for alternative-fuels infrastructure, including heavy-duty vehicle charging along the TEN-T network	Links vehicle transition to infrastructure availability and interoperability
EU ETS2	Applies upstream carbon pricing to fuels used in road transport, buildings, and additional sectors; current EU implementation information points to full operation in 2028	Adds an economic signal alongside standards and infrastructure policy
Ukraine - National Renewable Energy Action Plan to 2030 (2024)	Updates national renewable-energy planning through 2030	Connects transport electrification with grid, renewable energy, and storage policy
EU accession / Ukraine Report 2025	Requires continued alignment with the transport, environment, climate, energy, and administrative acquis	Makes institutional capacity and enforcement part of the greening agenda
Recovery and reconstruction planning	Rebuilding transport and energy assets after war damage	Creates a window to integrate low-carbon standards before infrastructure is locked in

4.4. Technical and technological instruments

Technical measures have the most visible relationship with emissions because they change vehicles, energy systems, or buildings directly. Battery-electric heavy-duty vehicles can eliminate tailpipe CO2 emissions at the point of use, but life-cycle performance depends on electricity generation, battery production, vehicle utilisation, payload, and replacement cycles. Fuel-cell vehicles may provide advantages in particular long-haul applications, but their environmental performance depends heavily on hydrogen production and infrastructure. These dependencies make technology assessment scenario-specific.

The revised EU policy framework increasingly favours zero-emission powertrains while treating gaseous fossil fuels as limited or transitional options. Regulation (EU) 2023/1804 itself notes a limited long-term role for gaseous fuels in heavy-duty road transport. Accordingly, LNG should not be presented as equivalent to zero-emission technology. It may provide operational advantages in certain contexts, but investment decisions must consider methane leakage, infrastructure lock-in, and the trajectory of EU regulation.

Warehouses and terminals form a second technical domain. Energy-efficient lighting, building envelopes, heat pumps, rooftop photovoltaics, energy management, and automa-

tion can lower facility energy use. The relevant metric, however, is facility-specific energy and emissions intensity rather than a universal reduction percentage. The design principle is to establish a baseline, identify high-consumption systems, and evaluate each measure through life-cycle and operational data.

4.5. Economic instruments and finance

Economic instruments determine whether technically feasible options are investable. Taxes, carbon pricing, grants, accelerated depreciation, concessional loans, guarantees, and green bonds can alter the balance between cleaner and conventional assets. The appropriate mix depends on the policy objective. Carbon pricing rewards lower operating emissions but may be insufficient to overcome high up-front capital costs; purchase support or concessional finance can address the capital barrier; public procurement can create early demand.

For Ukraine, financial design is particularly important because war-risk premiums and damaged infrastructure shorten corporate planning horizons. A credible greening strategy must therefore connect environmental requirements with financing channels. International financial institutions and the Ukraine Investment Framework can play a role, but environmental conditionality should be designed so that it supports implementation rather than simply adding compliance costs to firms with limited capital.

4.6. Organisational-managerial instruments

Organisational measures are often less capital-intensive than fleet replacement and can be implemented incrementally. Freight consolidation, improved load factors, dynamic routing, intermodal planning, reverse-logistics integration, and maintenance management can reduce avoidable activity and improve resource use. Their effect is nevertheless highly dependent on baseline inefficiency. A company with severe empty running may obtain large gains from planning improvements; a highly optimised network will have less remaining potential.

Digital TMS and WMS platforms should therefore be evaluated through operational indicators rather than assumed emissions percentages. Useful indicators include vehicle-kilometres per shipment, empty-running share, load factor, energy use per tonne-kilometre, on-time performance, and the carbon intensity of alternative routing choices. Digitalisation becomes a greening instrument only when it changes these decisions measurably.

4.7. Informational-analytical instruments and verification

Carbon accounting and sustainability reporting are the evidence infrastructure of greening. A firm cannot manage a reduction target credibly without defining organisational boundaries, operational boundaries, a base year, data sources, and calculation methods. GHG Protocol or ISO-based systems can support this process. External assurance, where feasible, improves comparability and reduces the risk that environmental claims are based on changing boundaries or selective indicators.

Corporate disclosures can illustrate organisational commitment but should not automatically be treated as independently verified evidence of national-sector performance. For

example, Raben Group, which operates in Ukraine, reports group-level progress on emissions and sustainability targets. Such disclosure is useful evidence that formal ESG systems are being implemented in logistics, but group-level results should not be reassigned to Raben Ukraine or used as a proxy for the Ukrainian logistics sector unless country-specific data are published (Raben Group, 2025). This evidence rule is applied throughout the revised analysis.

4.8. Evidence strength and the limits of effectiveness estimates

A central result of the review is methodological: the available evidence supports directional and context-specific conclusions more strongly than universal percentage estimates. The same nominal intervention can generate different outcomes depending on vehicle duty cycle, electricity mix, facility baseline, network structure, financing, and enforcement. The appropriate question is therefore not „What percentage does this instrument always save?" but „Under what conditions, and with what evidence, can this instrument change performance?"

Table 3. Evidence hierarchy for claims about greening effectiveness

Evidence type	What it can support	What it should not be used to claim
Binding law / official regulation	Verified policy targets, scope, dates, regulated actors	Actual company-level emissions reductions
Peer-reviewed empirical study	Context-specific measured or modelled effects within stated boundaries	Universal percentages transferable to all modes and countries
Systematic or structured review	Patterns across a documented literature corpus	A pooled effect unless methods and comparable effect sizes justify meta-analysis
Corporate sustainability disclosure	Illustrative implementation, targets, and company-reported performance	Independent sector-wide evidence or country-specific performance without disaggregation
Conceptual / governance analysis	Instrument roles, causal mechanisms, sequencing, policy design	Causal impact estimates without empirical identification

This hierarchy changes the interpretation of synergy. The literature gives strong reasons to expect complementarity: vehicle electrification works better with charging infrastructure; carbon pricing works better when low-emission substitutes are available; reporting is more useful when targets and responsibilities are defined; and route optimisation has greater value when dispatch decisions can act on the data. However, the reviewed sources do not justify a universal statement that combining all five categories produces a specific 35-45% reduction. The revised framework therefore treats synergy as a governance proposition to be tested in specific implementations, not as a pooled numerical result.

The same correction applies to payback-period claims. Route optimisation or energy-efficiency projects may have short paybacks in some firms, but fleet electrification, warehouse retrofit, and infrastructure investment can require much longer horizons. Decision makers should use project-level total-cost-of-ownership analysis and scenario testing rather than generic payback numbers.

4.9. Structural barriers and a governance sequence for Ukraine

The Ukrainian context requires a sequencing framework that links environmental ambition to implementation capacity. The principal barriers identified in the literature and policy context are financial constraints, damaged and insufficient infrastructure, regulatory and administrative capacity, weak data and reporting capability, and wartime security risk. These barriers should not be assigned arbitrary criticality scores unless a documented stakeholder or multi-criteria assessment has been conducted.

Table 4. Structural barriers and governance responses for Ukraine

Barrier	Why it matters	Governance response
Finance and investment risk	High capital costs, war-risk premiums, and short planning horizons can delay fleet and infrastructure investment	Blend public guarantees, concessional finance, private capital, and transparent green eligibility criteria
Charging, grid, and terminal infrastructure	Vehicle transition is constrained if charging power, grid connections, and logistics nodes are unavailable or unreliable	Coordinate transport, energy, reconstruction, and local infrastructure planning; prioritise interoperable corridors
Regulatory and administrative capacity	EU-aligned standards require inspection, data, enforcement, procurement capability, and inter-agency coordination	Link legal approximation to implementation plans, staff capacity, digital registries, and enforcement resources
Data and competence gaps	Firms, especially SMEs, may lack emissions baselines, TCO capability, or ESG reporting expertise	Provide standard methods, training, shared tools, and technical assistance before imposing complex reporting obligations
Wartime and security risk	Assets and energy systems face disruption; firms prioritise continuity and survival	Design resilient and modular investments; integrate environmental criteria into recovery finance without undermining essential logistics

On the basis of these barriers, a six-step governance sequence is proposed. Step 1 is measurement: establish reliable activity, energy, and emissions baselines. Step 2 is regulatory alignment: identify which EU-derived standards and reporting requirements apply now and which require phased preparation. Step 3 is infrastructure coordination: align fleet policy with charging, grid, terminal, and corridor investment. Step 4 is finance: connect requirements with grants, guarantees, concessional lending, procurement, and carbon-price signals. Step 5 is implementation: deploy technical and organisational measures according to operational suitability. Step 6 is verification and learning: monitor performance, disclose results, audit material claims, and revise the instrument mix.

This sequence is deliberately iterative. Measurement can reveal that a presumed priority is not the dominant emissions source; infrastructure constraints can change technology choice; financing conditions can alter deployment speed; and monitoring can show that a measure does not perform as expected. Sustainable governance therefore requires feedback rather than a fixed one-time plan.

5. Conclusions

This study develops a five-category classification of greening tools in transport and logistics operations: legal and regulatory, technical and technological, economic, organisational-managerial, and informational-analytical. The main contribution is not a new list of technologies, but a governance interpretation of how the categories interact. Regulation de-

fines obligations, technology provides physical alternatives, economic instruments shape investment incentives, organisational tools improve the use of assets and networks, and information systems make performance measurable and accountable.

The review also identifies an important methodological limitation in effectiveness assessment. The evidence base is too heterogeneous to justify universal percentage ranges for entire instrument categories or a single pooled reduction figure for an integrated portfolio. Effect estimates depend on system boundaries, baseline conditions, functional units, technologies, and national contexts. The revised framework therefore replaces false precision with an evidence hierarchy and requires quantitative claims to remain tied to their original scope.

For Ukraine, the policy implication is that greening transport and logistics should be treated as part of accession and reconstruction governance. EU alignment is moving beyond general Association Agreement commitments toward detailed acquis implementation. At the same time, war damage creates exceptional infrastructure and financing constraints. The appropriate strategy is therefore to integrate environmental standards into reconstruction planning, coordinate transport and energy infrastructure, develop administrative capacity, and use financing instruments that make compliance feasible for firms.

The proposed six-step governance sequence - measurement, regulatory alignment, infrastructure coordination, finance, implementation, and verification - offers a practical way to translate the five-category classification into policy and corporate action. It also makes clear that no single instrument can deliver the transition independently. Standards without infrastructure may be infeasible; subsidies without measurement may be poorly targeted; technology without organisational change may underperform; and reporting without accountability may become symbolic.

Future research should test the framework empirically using comparable company or corridor-level data. Priority designs include longitudinal studies of freight fleets, matched comparisons of logistics operators adopting different instrument mixes, total-cost-of-ownership analysis under Ukrainian energy and financing conditions, and evaluation of reconstruction projects that incorporate low-carbon transport requirements from the outset. Such work could eventually support quantitative estimates of interaction effects, but those estimates should be produced from documented data rather than assumed in advance.

Funding

This research received no external funding.

Conflicts of Interest

The authors declare no conflicts of interest.

Data Availability

No new dataset was generated for this conceptual and regulatory analysis. The study relies on the cited academic literature, public legal acts, and publicly available policy documents.

Ethics Statement

The study did not involve human participants, personal data collection or experimental procedures; therefore, research ethics approval was not required.

References

Cabinet of Ministers of Ukraine. (2024, August 13). National Renewable Energy Action Plan for the period up to 2030 and action plan for its implementation (Order No. 761-r). https://zakon.rada.gov.ua/laws/show/761-2024-%D1%80

Centobelli, P., Cerchione, R., & Esposito, E. (2017). Environmental sustainability in the service industry of transportation and logistics service providers: Systematic literature review and research directions. Transportation Research Part D: Transport and Environment, 53, 454-470. https://doi.org/10.1016/j.trd.2017.04.032

Chatzoudes, D., Kadlubek, M., & Maditinos, D. (2024). Green logistics practices: The antecedents and effects for supply chain management in the modern era. Equilibrium. Quarterly Journal of Economics and Economic Policy, 19(3), 991-1034. https://doi.org/10.24136/eq.2864

Dekker, R., Bloemhof, J., & Mallidis, I. (2012). Operations research for green logistics: An overview of aspects, issues, contributions and challenges. European Journal of Operational Research, 219(3), 671-679. https://doi.org/10.1016/j.ejor.2011.11.010

Dey, A., LaGuardia, P., & Srinivasan, M. (2011). Building sustainability in logistics operations: A research agenda. Management Research Review, 34(11), 1237-1259. https://doi.org/10.1108/01409171111178774

European Commission. (2025). Ukraine Report 2025. Directorate-General for Enlargement and Eastern Neighbourhood. https://enlargement.ec.europa.eu/ukraine-report-2025_en

European Commission. (2026a). ETS2: Buildings, road transport and additional sectors. Directorate-General for Climate Action. https://climate.ec.europa.eu/eu-action/carbon-markets/ets2-buildings-road-transport-and-additional-sectors_en

European Commission. (2026b, February 23). Updated Ukraine Recovery and Reconstruction Needs Assessment released. Directorate-General for Enlargement and Eastern Neighbourhood. https://enlargement.ec.europa.eu/news/updated-ukraine-recovery-and-reconstruction-needs-assessment-released-2026-02-23_en

European Parliament and Council of the European Union. (2023). Regulation (EU) 2023/1804 of 13 September 2023 on the deployment of alternative fuels infrastructure and repealing Directive 2014/94/EU. Official Journal of the European Union, L 234, 1-47. https://eur-lex.europa.eu/eli/reg/2023/1804/oj

European Parliament and Council of the European Union. (2024). Regulation (EU) 2024/1610 of 14 May 2024 amending Regulation (EU) 2019/1242 as regards strengthening the CO2 emission performance standards for new heavy-duty vehicles. Official Journal of the European Union. https://eur-lex.europa.eu/eli/reg/2024/1610/oj

Farooque, M., Zhang, A., Thürer, M., Qu, T., & Huisingh, D. (2019). Circular supply chain management: A definition and structured literature review. Journal of Cleaner Production, 228, 882-900. https://doi.org/10.1016/j.jclepro.2019.04.303

Geissdoerfer, M., Savaget, P., Bocken, N. M. P., & Hultink, E. J. (2017). The circular economy: A new sustainability paradigm? Journal of Cleaner Production, 143, 757-768. https://doi.org/10.1016/j.jclepro.2016.12.048

Genovese, A., Acquaye, A. A., Figueroa, A., & Koh, S. C. L. (2017). Sustainable supply chain management and the transition towards a circular economy: Evidence and some applications. Omega, 66, 344-357. https://doi.org/10.1016/j.omega.2015.05.015

Intergovernmental Panel on Climate Change. (2022). Climate change 2022: Mitigation of climate change. Cambridge University Press. https://doi.org/10.1017/9781009157926

International Energy Agency. (2023). Global EV Outlook 2023: Catching up with climate ambitions. IEA. https://www.iea.org/reports/global-ev-outlook-2023

Liimatainen, H., van Vliet, O., & Aplyn, D. (2019). The potential of electric trucks: An international commodity-level analysis. Applied Energy, 236, 804-814. https://doi.org/10.1016/j.apenergy.2018.12.017

McKinnon, A., Browne, M., Whiteing, A., & Piecyk, M. (2015). Green logistics: Improving the environmental sustainability of logistics (3rd ed.). Kogan Page.

Meneghetti, A., & Monti, L. (2015). Greening the food supply chain: An optimisation model for sustainable design of refrigerated automated warehouses. International Journal of Production Research, 53(21), 6567-6587. https://doi.org/10.1080/00207543.2014.985449

Piecyk, M. I., & McKinnon, A. C. (2010). Forecasting the carbon footprint of road freight transport in 2020. International Journal of Production Economics, 128(1), 31-42. https://doi.org/10.1016/j.ijpe.2009.08.027

Raben Group. (2025). Sustainability Report 2024. https://ukraine.raben-group.com/en/about-us/sustainability

Rao, P., & Holt, D. (2005). Do green supply chains lead to competitiveness and economic performance? International Journal of Operations & Production Management, 25(9), 898-916. https://doi.org/10.1108/01443570510613956

Sarkis, J., Zhu, Q., & Lai, K. H. (2011). An organizational theoretic review of green supply chain management literature. International Journal of Production Economics, 130(1), 1-15. https://doi.org/10.1016/j.ijpe.2010.11.010

Srivastava, S. K. (2007). Green supply-chain management: A state-of-the-art literature review. International Journal of Management Reviews, 9(1), 53-80. https://doi.org/10.1111/j.1468-2370.2007.00202.x

Velychko, O., & Velychko, L. (2023). Conceptual model of ecologisation of logistics systems in the context of sustainable development. Agricultural and Resource Economics, 9(2), 241-258. https://doi.org/10.51599/are.2023.09.02.12

Winkelmann, S., Guennoun, R., Möller, F., Schoormann, T., & van der Valk, H. (2024). Back to a resilient future: Digital technologies for a sustainable supply chain. Information Systems and e-Business Management, 22, 315-350. https://doi.org/10.1007/s10257-024-00677-z

Zhu, Q., Sarkis, J., & Lai, K. H. (2013). Institutional-based antecedents and performance outcomes of internal and external green supply chain management practices. Journal of Purchasing and Supply Management, 19(2), 106-117. https://doi.org/10.1016/j.pursup.2012.12.001

Architectural Imagery In Children's Books Circulating In Kazakhstan: Cultural Memory, Place Identity, And Implications For Cultural Sustainability

Nazerke Zhambylkyzy Toktassynova
Kazakh Leading Academy of Architecture and Civil Engineering
Almaty, Kazakhstan
artandcookie6@gmail.com

Abstract.
This study examines how the built environment is represented in illustrated children's books circulating in Kazakhstan and how recurring architectural images may function as carriers of cultural memory, place identity, and cultural sustainability. The purposive corpus comprises 42 illustrated publications from the late twentieth and early twenty-first centuries, including Kazakhstan-produced titles and translated or international books present in the local reading repertoire. The analysis combines Mallan's approach to visual narrative with Assmann's concept of cultural memory, Nora's concept of lieux de mémoire, and place-based interpretation. A nine-parameter visual coding scheme was applied to composition, human–space relations, scale, visual routes, colour, realism/abstraction, narrative agency of space, schematic representation, and ecological-social context. Six recurrent architectural-environment types were identified, with three publications coded as mixed/transitional. Everyday social environments were the most frequent (12/42; 28.6%), followed by mythical-epic environments (10/42; 23.8%). Recognisable urban environments, including depictions of Astana and Almaty, linked civic landmarks with belonging and place recognition, while functional-ecological environments foregrounded relationships among infrastructure, nature, and people. The study proposes the interpretive concept of a "visualised place of memory" to describe the way architectural landmarks and spatial narratives can mediate cultural meanings in children's books. The findings are relevant to heritage education, graphic-design pedagogy, children's publishing, and place-based cultural policy, but they do not establish how children actually interpret these images; reception studies are therefore required.
Keywords: *architectural imagery; children's book illustration; cultural memory; place identity; cultural sustainability; Kazakhstan.*

1.Introduction

Globalisation, urban standardisation, and the rapid circulation of transnational visual media make the representation of place an increasingly important issue in children's culture. Illustrated books do more than accompany verbal narratives: they organise space, establish relations between people and their surroundings, and repeatedly expose young readers to visual models of home, city, landscape, monument, infrastructure, and heritage. In this sense, architecture in children's illustration can operate as a visual mediator between everyday experience and wider cultural narratives.

Research on contemporary children's literature in Kazakhstan has increasingly addres-

sed identity, imagined community, and the relationship between national and world literature (Frieß, 2025; Seisenbiyeva et al., 2024). International scholarship has also shown that picturebooks and illustrated nonfiction can organise knowledge through the interaction of text, image, layout, and spatial representation (Campagnaro, 2021; Farrar et al., 2024; Shimek, 2019). What remains less developed is a systematic account of the architectural environment itself: not simply which buildings appear, but how scale, colour, composition, routes, interiors, landmarks, and environmental systems are used to construct meaning.

The source manuscript initially described the material as "Kazakhstani children's book illustration". The corpus, however, includes both Kazakhstan-produced publications and translated or international titles. The present revision therefore uses the more precise formulation "children's books circulating in Kazakhstan". This distinction matters methodologically: the study analyses a reading repertoire available within Kazakhstan rather than claiming that all 42 publications were produced by Kazakhstani illustrators. When specifically Kazakhstani visual tendencies are discussed below, the argument is restricted to clearly local titles and settings.

The topic is also relevant to cultural sustainability. UNESCO's Culture|2030 framework treats cultural heritage, education, knowledge and skills, and sustainable places as interconnected dimensions of sustainable development (UNESCO, 2019). The MONDIACULT 2022 Declaration similarly frames culture as a public good and as a contributor to resilience, social cohesion, and sustainable development (UNESCO, 2022). Children's illustration is not itself a governance mechanism, and this article does not evaluate cultural policy. It can, however, provide evidence about which spatial and heritage images are made visible to children and how those images are organised. Such evidence can inform heritage education, publishing policy, library curation, and place-based cultural programmes.

The aim of this article is to identify and categorise recurring images of the architectural environment in a corpus of 42 illustrated children's publications circulating in Kazakhstan and to examine the visual mechanisms through which these images communicate cultural meanings and a sense of place.

Research questions

- What types of architectural environment predominate in the analysed corpus?
- Through which visual techniques—especially scale, colour, composition, spatial routes, and narrative positioning—are cultural meanings and place identity communicated?
- What implications can the identified patterns have for cultural sustainability, heritage education, and visual-design pedagogy?

The contribution is interpretive rather than causal. The study identifies visual patterns and proposes a typology, but it does not test how children receive, remember, or emotionally respond to the images. Claims about educational or cultural effects are therefore framed as plausible functions and implications to be examined in future reception research.

2. Theoretical Framework

2.1. Cultural memory, place, and architectural representation

Assmann (2011) conceptualises cultural memory as a socially organised form of remembrance sustained through texts, symbols, rituals, and material forms. Nora's (1984–1992) concept of lieux de mémoire draws attention to sites and symbolic entities in which collective memory becomes concentrated. Although Nora developed the concept in relation to historically and institutionally recognised sites of memory, it is useful here as an interpretive lens for understanding repeated visual representations of landmarks, domestic forms, and mythic spaces in children's books.

Relph (1976) distinguishes meaningful place from placelessness by emphasising lived attachment, familiarity, and identity. Architectural illustration can participate in this process symbolically: a yurt, a skyline, a square, a bridge, or a domestic interior may condense multiple associations into a recognisable spatial sign. Chukova's (2020) analysis of monuments and national identity in Macedonia and post-Soviet Central Asian republics further demonstrates that architecture and monumental imagery can be mobilised within broader narratives of collective identity. The present study does not equate children's books with state memory policy; rather, it asks whether recurring illustrated places act as small-scale visual carriers of cultural remembrance.

2.2. Visual narrative and meaning-making in children's books

Mallan (2008) shows how picturebooks can imagine identity, community, and historical memory through the interaction of visual and narrative devices. This study follows that orientation by analysing not only what is depicted but how it is depicted: whether the viewer encounters an open panorama or a compressed frame, whether a building dominates or supports the human figure, whether colour indicates security or estrangement, and whether routes invite movement through space.

Recent work on visual literacy reinforces the need to treat images as structured meaning-making systems rather than decorative supplements. Farrar et al. (2024) synthesise research on visual literacy and children's reading, while Eckhoff (2025) demonstrates the value of critical content analysis for revealing how professional and material environments are represented in children's literature. Studies of architecture and nonfiction picturebooks similarly show that illustrated spatial environments can support observation, comparison, and spatial reasoning (Campagnaro, 2021; Luigini, 2019; Schmiedeknecht et al., 2023). Olver's (2025) ecocritical analysis is relevant to the functional-ecological category identified below because it highlights how illustrated activities can position human and non-human systems in relation to one another.

2.3. Cultural sustainability and heritage education

The concept of cultural sustainability extends the analysis beyond preservation of individual monuments. It concerns the continued capacity of communities to transmit, reinterpret, and use cultural meanings across generations. In the UNESCO Culture|2030 framework, heritage, education, participation, and sustainable places are treated as interconnected policy

domains (UNESCO, 2019). From this perspective, children's books can be examined as part of the wider cultural ecosystem through which place-based knowledge is reproduced. The article therefore treats architectural illustration as a cultural-educational resource whose governance relevance lies in visibility, representation, and access rather than in direct regulatory power.

3. Materials And Methods

3.1. Research design and corpus

The study uses qualitative visual content analysis supported by descriptive frequency counts. The empirical corpus comprises 42 illustrated children's publications from the late twentieth and early twenty-first centuries that were selected because architectural or spatial imagery is materially present in the narrative or informational content. The corpus includes folk tales, everyday-life stories, city-oriented books, environmental nonfiction, architecture-related publications, and picturebooks. It also includes both Kazakhstan-produced titles and translated or international titles available in the local reading repertoire.

The sampling strategy is purposive rather than statistically representative. The study therefore does not estimate the prevalence of particular architectural images in all children's publishing in Kazakhstan. Instead, it constructs an analytically diverse corpus capable of supporting a typology of recurrent spatial representations. The titles included in the corpus are listed in Appendix A

. Edition-level bibliographic metadata were not consistently recorded in the source manuscript; this limits historical comparison and should be strengthened in future corpus construction.

3.2. Coding framework

A nine-parameter coding scheme was developed from the source manuscript's adaptation of Mallan's visual-narrative approach and from the research questions. Each publication was read as a visual-spatial unit, with attention to recurrent settings rather than isolated single illustrations. The coding dimensions are summarised in Table 1.

Table 1. Coding dimensions

Parameter	Analytical focus	Examples of coded features
Spatial composition	Overall spatial organisation	Panorama; vertical composition; fragment; map-like view
Human–space relation	Position of characters in relation to the environment	Active exploration; containment; suppression; support
Scale and proportion	Relative size and hierarchy of elements	Realistic scale; symbolic enlargement; hierarchical scale
Visual routes	Directions structuring movement through space	Roads; paths; boundaries; axes; gaze lines
Colour scheme	Use of colour to organise affect or spatial zones	Warm/cool palette; contrast; symbolic colour; zoning
Realism / abstraction	Degree of visual stylisation	Realistic; semi-realistic; schematic; symbolic

Parameter	Analytical focus	Examples of coded features
Narrative agency of space	Whether the environment functions as background or narrative actor	Passive setting; obstacle; guide; destination; memory cue
Infographic representation	Use of explanatory graphic systems	Labels; diagrams; cross-sections; arrows
Ecological-social context	Relationship between built, natural, technological, and social systems	Infrastructure; climate; household practices; public space

For the descriptive distribution, each publication was assigned to one predominant architectural-environment type when that type accounted for more than half of the publication's relevant spatial imagery. Where no single type met that threshold, the publication was coded as mixed/transitional. The original study was conducted by a single researcher, and no formal inter-rater reliability statistic was calculated. This is an important limitation because category boundaries—especially between recognisable urban, cultural-exploratory, and everyday social environments—depend on interpretive judgement.

4. Results

4.1. Typology of architectural environments

The analysis identified six recurrent architectural-environment types. The labels below refine the wording of the source manuscript for clarity while preserving its underlying categories. Table 2 summarises the defining visual cues, representative titles, and interpretive cultural function. Representative titles illustrate salient examples and should not be read as the exclusive category assignment for every secondary setting within a book.

Table 2. Summary of defining visual characteristics, typical names, and interpretive cultural functions

Type	Representative titles	Visual cues	Interpretive cultural function
1. Dominant / constraining urban environment	The Grey City; So How Do I Tell the Truth Now?	Monochrome or cool palette; strong verticals; buildings larger than people; compressed perspectives; limited sky	Makes the built environment visible as a problem or pressure; may invite critical reflection on monotonous or alienating urban space.
2. Functional–ecological system	Everyone Needs Water!; Waste Paper: Why Are the Trees Withering?; Qadam; A Great Book of Snow and Ice	Diagrams; cross-sections; flow lines; hazard/safety colour coding; people shown within a process	Connects infrastructure, natural systems, resources, and everyday human action; supports an environmental-systems reading of space.
3. Cultural and exploratory environment	A Trip to Italy; Look at that Building!; A Trip to Almaty; The Kingdom of Books; The World: Questions and Answers	Open vistas; warm/bright palette; legible scale; movement and exploration through settings	Frames architecture as an object of discovery, learning, cultural encounter, and spatial orientation.
4. Recognisable civic urban environment	Salem, Astana!; Salem, Almaty!; A Trip to Almaty; Astana Coloring Book; Legends of a Magical Land: Atameken	Landmarks; bridges; squares; routes; signage; stylised iconic features; vibrant palette	Links landmark recognition with urban belonging and place identity; can function as a visual introduction to civic space.

Type	Representative titles	Visual cues	Interpretive cultural function
5. Mythical–epic architectural environment	Eer Tostik; Ancient Kazakhstan; Kazakh fairy-tale collections; Aladdin; Cinderella	Yurt, palace, fortress, sacred or heroic site; hierarchical composition; ornament; symbolic scale; paths of trial	Connects architecture to myth, historical imagination, traditional symbols, and intergenerational cultural memory.
6. Everyday social environment	My Name Is Kozha; Connie Helps Her Mother; Brother; It's Time for Bed; Miras and Diaz; Miras and Dimash	Realistic or semi-realistic interiors; familiar scale; warm local colours; home, school, playground, market	Normalises everyday spatial practices and relationships; represents family and social life through familiar settings.

4.2. Descriptive distribution

The predominant-type distribution is shown in Table 3. Percentages are reported to one decimal place to avoid the rounding distortion present in the source version. The everyday social environment is the largest category (28.6%), followed by the mythical–epic environment (23.8%). Together these two types account for slightly more than half of the corpus. The recognisable urban environment accounts for 14.3%, while cultural-exploratory and functional-ecological settings are less frequent. Only 4.8% of the corpus was assigned to the constraining urban type. Three publications (7.1%) were coded as mixed/transitional because no single environment exceeded the 50% threshold.

Table 3. The predominant-type distribution

Coding outcome	Books (n)	Share of corpus
Everyday social environment	12	28.6%
Mythical–epic architectural environment	10	23.8%
Recognisable civic urban environment	6	14.3%
Cultural and exploratory environment	5	11.9%
Functional–ecological system	4	9.5%
Dominant / constraining urban environment	2	4.8%
Mixed / transitional	3	7.1%

The low frequency of the constraining urban type should not be interpreted as proof of a general "humanistic orientation" of children's publishing, as stated in the source manuscript. The sample is purposive and relatively small. A more defensible interpretation is that explicitly oppressive or alienating urban imagery is uncommon within this particular corpus, while familiar social space and mythic-historical space are more prominent.

4.3. Representative visual mechanisms

Several recurrent mechanisms illustrate how the typology operates. In The Grey City, large-scale buildings, grey and cool tones, and the diminished child figure create a visual relation of spatial pressure. The environment is not neutral background; it structures the emotional reading of the scene. By contrast, functional-ecological books such as Everyone Needs Water!, A Great Book of Snow and Ice, and Qadam use diagrams, process sequences, and cause-and-effect relations to connect built systems with climate, resources, and every-

day behaviour. This mode is compatible with the ecological questions identified in recent ecocritical work on children's activity and informational books (Olver, 2025).

Recognisable civic urban imagery is especially visible in Salem, Astana!, Salem, Almaty!, A Trip to Almaty, and the Astana Coloring Book. Panoramic views, routes through the city, and landmark buildings such as Baiterek and Khan Shatyr make the city readable through a small number of iconic spatial cues. In the colouring-book format, the reader is also invited to participate visually by supplying colour. These examples suggest a mechanism of place recognition rather than demonstrating a measured effect on civic identity.

Mythical-epic settings use a different spatial logic. In Eer Tostik, the steppe, underworld, heavenly realm, yurt, and palace are organised as a hierarchy of narrative worlds. In Kazakh fairy-tale collections, the yurt, palace, fortress, and caravanserai operate as compact visual signs of historical or mythic space. Everyday social environments, by contrast, depend on recognisable scale, warm colour, and functional zoning of domestic, school, market, and play spaces. Across these types, the architectural environment can act as a narrative participant by constraining, guiding, sheltering, or orienting characters.

5. Discussion

5.1. Architectural imagery as cultural memory

The corpus demonstrates that children's spatial imagery is heterogeneous rather than organised around a single national visual code. Traditional and mythic forms coexist with contemporary urban landmarks, environmental systems, international fairy-tale architecture, and ordinary domestic settings. This coexistence is important because cultural memory is not transmitted only through officially monumental heritage. It is also reproduced through familiar interiors, routes, repeated symbols, and narrative settings that connect personal experience with wider cultural references (Assmann, 2011; Nora, 1984–1992).

Within clearly Kazakhstan-specific titles, recognisable representations of Astana and Almaty can be interpreted as emerging visual places of memory: images that condense civic recognition, narrative movement, and cultural identification. The concept proposed here —"visualised place of memory"—does not claim that every illustrated landmark becomes a collective memory site. Rather, it describes a representational mechanism through which a built form is repeatedly simplified, stylised, and embedded in a narrative so that it becomes available as a memory cue. This proposition requires testing through longitudinal and reception-based research.

5.2. Scale, colour, route, and narrative agency

Four mechanisms recur across the typology. First, relations of scale organise power: oversized buildings can diminish the human figure, while familiar scale can make space appear inhabitable. Second, colour creates affective and symbolic zoning: cool monochrome palettes are associated in the analysed examples with distance or constraint, while warm palettes frequently accompany domestic security and exploration. Third, compositional routes—roads, paths, bridges, panoramic viewpoints, and sequences—structure how readers are invited to move mentally through the depicted environment. Fourth, narrative agency

determines whether architecture merely frames action or becomes part of the problem, destination, memory cue, or learning process.

These mechanisms correspond with research that treats picturebooks as multimodal systems in which meaning is generated through the interaction of verbal and visual structures (Campagnaro, 2021; Farrar et al., 2024; Shimek, 2019). The present contribution is to focus that multimodal analysis on architectural space and to differentiate recurring spatial functions across a Kazakhstan-based reading corpus.

5.3. "Nomadic minimalism" and ethno-futurist synthesis as provisional analytical labels

The source manuscript proposed the terms "nomadic minimalism" and "ethno-futurism" to describe local visual tendencies. These terms are retained here only as provisional analytical labels, not as established art-historical categories. In Eer Tostik and Ancient Kazakhstan, certain architectural forms are reduced to geometric outlines and ornamental details; the yurt, for example, may be represented through a small set of recognisable lines and circular forms. "Nomadic minimalism" is used here to describe this economy of visual coding. In Salem, Astana! and Never Satisfied with Art, traditional ornament and culturally familiar motifs are combined with modern or futuristic urban forms; the term "ethno-futurist synthesis" is used to describe that juxtaposition.

These tendencies should not be generalised to all Kazakhstani illustration without a larger, production-based corpus. They are best understood as hypotheses generated from specific local titles. Their significance lies in the possibility that cultural continuity is communicated through transformation rather than through literal replication of historical architecture. Frieß (2025) similarly shows that contemporary children's literature in Kazakhstan can negotiate identity through open and imaginative forms, while Seisenbiyeva et al. (2024) position children's literature within broader processes of national-cultural representation.

5.4. Implications for cultural sustainability and governance

The results have a limited but meaningful connection to sustainable governance. Sustainable cultural governance concerns not only the protection of monuments but also the institutions and educational practices through which cultural knowledge, diversity, and place-based meanings are maintained and reinterpreted. UNESCO's Culture|2030 Indicators explicitly connect heritage with education, knowledge, participation, and sustainable places (UNESCO, 2019). In that context, the typology developed here can function as a diagnostic tool for reviewing the visual environments presented in children's publishing and educational materials.

Four practical implications follow. First, heritage-education programmes can use recognisable civic landmarks and mythic-historical forms as prompts for discussing how cities and cultural identities change over time. Second, publishers and illustrators can use the coding framework to assess whether a book presents children only with monumental and touristic images or also with everyday, ecological, and socially inclusive spaces. Third, graphic-design education can use the typology to connect visual composition with cultural responsibility, asking how scale, colour, routes, and symbols shape the imagined relationship between the

child and the built environment. Fourth, public libraries, museums, and local cultural programmes can use children's illustration as a supplementary medium for place-based learning.

These are governance implications rather than measured outcomes. The study does not show that any particular image produces pride, environmental responsibility, or social cohesion. A policy or educational programme should therefore treat the typology as an analytical and design resource, not as evidence of causal effects on children.

Table 4. Finding and Potential

Finding	Potential cultural-governance use	Required safeguard
Recognisable civic landmarks	Heritage education; city orientation; place-based cultural programmes	Avoid reducing urban identity to a small set of iconic monuments; include diverse neighbourhoods and everyday spaces.
Mythical–epic environments	Intergenerational heritage communication; folklore-based learning	Avoid presenting a single essentialised version of national identity; contextualise traditions historically.
Functional–ecological systems	Education for sustainable development; infrastructure and resource literacy	Verify scientific accuracy and distinguish environmental explanation from symbolic interpretation.
Everyday social environments	Inclusive design education; discussion of home, school, market, and public space	Consider social diversity, accessibility, gender, disability, and different family or community experiences.
Visual coding framework	Publisher review; design pedagogy; research coding	Use as an interpretive tool; do not infer child reception without empirical evidence.

5.5. Limitations

The study has five principal limitations. First, the corpus is purposive and cannot be treated as representative of all children's publishing in Kazakhstan. Second, the corpus mixes domestically produced and translated or international titles; this is appropriate for studying the local reading repertoire but limits claims about the distinctive characteristics of Kazakhstani illustration as a production field. Third, edition-level metadata were not consistently available in the source manuscript, which restricts precise historical comparison across the late twentieth and early twenty-first centuries. Fourth, the coding was conducted by a single researcher and no inter-rater reliability measure was calculated. Fifth, the study analyses visual content rather than reader reception; it therefore cannot determine how children of different ages, genders, linguistic backgrounds, or places of residence interpret the architectural imagery. Digital picturebooks, comics, educational textbooks, and interactive media were not included.

6. Conclusion

This study developed a visual-spatial typology of architectural environments in a purposive corpus of 42 illustrated children's publications circulating in Kazakhstan. Six recurrent types were identified, together with a mixed/transitional category. Everyday social environ-

ments were most frequent (28.6%), followed by mythical–epic environments (23.8%). Recognisable civic urban environments accounted for 14.3% of the corpus, while functional-ecological representations made infrastructure and environmental processes visually explicit.

The analysis indicates that architecture can perform several narrative functions in children's illustration: it can constrain the character, organise exploration, provide cultural landmarks, connect people with ecological systems, or locate social life in familiar everyday settings. Scale, colour, routes, level of realism, and the narrative agency of space are the main visual mechanisms through which these functions are expressed.

The theoretical contribution is the proposal of the "visualised place of memory" as an interpretive concept for describing how architectural forms may become condensed visual cues of cultural memory when repeatedly stylised and embedded in narrative. The concepts of "nomadic minimalism" and "ethno-futurist synthesis" are retained as provisional labels for patterns visible in a limited group of Kazakhstan-specific titles and require validation in a larger production-based corpus.

For the purposes of the present conference issue, the practical significance lies in cultural sustainability and heritage governance. The typology can support critical review of children's publishing, heritage-education materials, library and museum programmes, and graphic-design curricula by making visible which kinds of places, infrastructures, and cultural symbols are presented to children and how they are framed. Future research should combine content analysis with empirical studies of children aged 5–9, compare clearly defined historical periods using edition-level metadata, and examine how digital and interactive media transform architectural imagery and place-based cultural memory.

Funding

This research received no external funding.

Conflicts of Interest

The author declares no conflicts of interest.

Data Availability

The titles included in the analysed corpus and the aggregate coding categories and counts are reported in this article. No separate dataset has been deposited.

Ethics Statement

This study analyses published children's books and does not involve human participants or personal data; institutional ethics approval was therefore not required.

References

Assmann, J. (2011). Cultural memory and early civilization: Writing, remembrance, and political imagination. Cambridge University Press. https://doi.org/10.1017/CBO9780511996306

Campagnaro, M. (2021). Stepping into the world of houses: Children's picturebooks on architecture. In N. Goga, S. H. Iversen, & A.-S. Teigland (Eds.), Verbal and visual strategies in nonfiction picturebooks: Theoretical and analytical approaches (pp. 202–219). Scandinavian University Press. https://doi.org/10.18261/9788215042459-2021-15

Chukova, R. (2020). Legitimizing new national identity through the monuments: The case of Macedonia and post-Soviet Central Asian republics. Revue des Études Sud-Est Européennes, 58(1–4), 353–365. https://resee.acadsudest.ro/sites/default/files/sites/default/files/articole/2020_22_Chukova.pdf

Eckhoff, A. (2025). Representation in engineering-focused children's literature: A critical content analysis. International Journal of Early Childhood, 57(2), 527–545. https://doi.org/10.1007/s13158-024-00409-x

Farrar, J., Arizpe, E., & Lees, R. (2024). Thinking and learning through images: A review of research related to visual literacy, children's reading and children's literature. Education 3-13, 52(7), 993–1005. https://doi.org/10.1080/03004279.2024.2357892

Frieß, N. (2025). Offen, tolerant, fantastisch: Imaginierte Gemeinschaften in Kasachstans zeitgenössischer Kinderliteratur. Zeitschrift für Slawistik, 70(2), 200–217. https://doi.org/10.1515/slaw-2025-0014

Luigini, A. (2019). Case, oggetti e architetti: Il disegno dell'architettura nei libri illustrati per l'infanzia. diségno, 4, 161–174. https://doi.org/10.26375/disegno.4.2019.164

Mallan, K. (2008). Imagining identity, community and historical memory in Canadian picture books. Bookbird: A Journal of International Children's Literature, 46(3), 11–19. https://doi.org/10.1353/bkb.0.0089

Nora, P. (1984–1992). Les lieux de mémoire (Vols. 1–3). Gallimard.

Olver, C. (2025). Nature's puzzles: An ecocritical theorisation of children's activity books. Children's Literature in Education, 56(4), 619–634. https://doi.org/10.1007/s10583-024-09587-7

Relph, E. (1976). Place and placelessness. Pion.

Schmiedeknecht, T., Rudd, J., & Hayward, E. (Eds.). (2023). Building children's worlds: The representation of architecture and modernity in picturebooks. Routledge.

Sebenova, B. T. (2024). Ethnocultural traditions and trends in the modern art of book illustration in Kazakhstan [Teaching aid]. Arkalyk University Press.

Seisenbiyeva, E., Mukhamadiev, D., Sametova, Z., Aitova, Z., Tulebayeva, K., & Ismagulova, N. (2024). Children's literature of Kazakhstan in the context of world literature as the basis of national identity. Journal of Ecohumanism, 3(8), 9925–9934. https://doi.org/10.62754/joe.v3i8.5605

Shimek, C. (2019). Sites of synergy: Strategies for readers navigating nonfiction picture books. The Reading Teacher, 72(4), 519–522. https://doi.org/10.1002/trtr.1754

UNESCO. (2019). Culture|2030 indicators. UNESCO. https://whc.unesco.org/en/culture-2030indicators/
UNESCO. (2022). MONDIACULT 2022 Declaration. UNESCO. https://www.unesco.org/en/mondiacult/2022

Appendix A. Corpus of 42 analysed publications

1. Aladdin. The Magic Lamp	22. Look at that Building!
2. Grandfather's Sweet Bun	23. Waste Paper: Why Are the Trees Withering?
3. Everyone Needs Water!	24. My Name Is Kozha
4. A Great Book of Snow and Ice	25. Miras and Diaz: Inesaut
5. Brother	26. Miras and Dimash
6. Magic Words: Sorry	27. The World: Questions and Answers
7. Magic Words: Thank You	28. Never Satisfied with Art
8. Ancient Kazakhstan	29. It's Time for Bed
9. Eer Tostik	30. The Adventures of Marco Polo
10. Sound and Rhythm: A Note Seeking Its Place	31. A Trip to Almaty
11. Cinderella	32. A Trip to Italy
12. The Magic Pies of Inju	33. Qadam (Step)
13. So How Do I Tell the Truth Now?	34. Salem, Almaty!
14. How to Behave in the Market	35. Salem, Astana!
15. Kazakh Fairy Tales	36. The Grey City
16. Kazakhstan Fairy Tales	37. Fairy Tales from Around the World
17. Connie Helps Her Mother	38. The Curious Garden
18. The Kingdom of Books	39. The Star Who Lost Its Sleep
19. A Collection of Fairy Tales from Kazakh and World Peoples	40. Find It in the Big Book
20. The Friendship of the Sheep and the Wolf	41. Astana Coloring Book
21. Legends of a Magical Land: Atameken	42. Jacob Is Playing Football

The Unregulated Middle: Generative AI in Foreign Language Teacher Education Between the EU AI Act and Ukrainian Law

Raisa Gladushyna
Borys Grinchenko Kyiv Metropolitan University
Kyiv, Ukraine
ORCID iD: 0000-0002-6760-0487
gladushyna.raisa@gmail.com

Abstract.
Generative artificial intelligence entered foreign language teacher education faster than the law governing it. This article asks a narrow doctrinal question: which binding rules actually apply when a Ukrainian pre-service teacher of English uses a commercial large language model to prepare, deliver or assess instruction? It answers by reading three bodies of law against one another — the EU Artificial Intelligence Act as amended by the Digital Omnibus of July 2026, Ukraine's Law on Copyright and Related Rights of 2022, and Article 42 of Ukraine's Law on Education. Three findings follow. First, the AI Act does not designate educational artificial intelligence as high-risk by sector; Annex III lists four discrete use cases, the obligations attaching to them are deferred to December 2027, and what binds today is the literacy duty in Article 4 and the transparency duty in Article 50. Second, Ukraine's sui generis right in non-original computer-generated objects gives a teacher a proprietary position in generated teaching materials but no authorship, and the statutory notion of the lawful user of a computer program does not map cleanly onto cloud services. Third, undisclosed generative AI use cannot constitute academic plagiarism under Ukrainian law, and constitutes cheating only where an institution has designated such tools as impermissible sources. Between these layers sits an unregulated middle that statute delegates to institutional rule-making and that most Ukrainian universities have not yet occupied.
Keywords: *artificial intelligence; AI Act; academic integrity; sui generis right; teacher education; Ukraine.*

1. Introduction

A student teacher of English in Kyiv opens a commercial chatbot, asks it for a B1 reading lesson on climate change, receives a text, a glossary and six comprehension questions, edits the result for forty minutes and teaches it the following week. Nothing about this sequence is unusual. Almost every element of it is legally unsettled.

Who holds rights in the generated text? May the teacher paste a pupil's essay into the same tool to obtain feedback? If the lesson plan is later published on a departmental website without attribution to the system that produced it, has any rule been broken? If a student submits generated prose as her own coursework, which provision of Ukrainian law does that violate — and does it violate any?

The scholarly literature on generative artificial intelligence in language education has grown quickly and answers none of these questions, because it does not ask them. It asks instead about attitudes, adoption, efficacy and competence frameworks (Harakchiyska, 2025; Kasneci et al., 2023; Yan et al., 2024). Where law appears at all, it appears as background: a

gesture towards the AI Act, a mention of data protection, an appeal to institutional policy. The gesture is often inaccurate. It is now commonplace to read that the AI Act classifies artificial intelligence in education as high-risk. It does not, and the difference matters a great deal to anyone trying to work out what to do on Monday morning.

This article takes the opposite approach. It brackets the pedagogical question entirely and asks only what the applicable law provides. The jurisdictional frame is Ukraine, for two reasons. Ukrainian higher education institutions are adapting to European standards under the accession process while remaining outside the scope of most EU instruments, which makes the boundary between what applies and what merely influences unusually consequential. And Ukraine holds a statutory position on computer-generated output that few states hold: since 1 January 2023 it has recognised a sui generis right in non-original objects generated by a computer program (Law of Ukraine No. 2811-IX, Article 33). That provision was not drafted with large language models in mind, yet it now governs them, and its interaction with the academic integrity regime has not been examined.

The argument proceeds in four steps. Section 3 establishes what the AI Act does and does not do to teacher education, in the form the Act now takes after the Digital Omnibus of July 2026. Section 4 identifies which data protection regime actually binds a Ukrainian university. Section 5 works through the copyright position, which is where the Ukrainian material is most distinctive. Section 6 turns to academic integrity and shows that the copyright rule and the education rule interlock badly. Section 7 draws the strands together under the heading that gives this article its title.

The claim advanced is not that Ukrainian law is silent. It is that the binding rules are dispersed across instruments drafted for other purposes, that they leave a defined space to institutional rule-making, and that institutions have not yet legislated into it. That space is the unregulated middle, and it is where the ordinary daily use of generative artificial intelligence in teacher education actually sits.

2. Scope, Method And Sources

This is a doctrinal study. It reconstructs the applicable legal position from primary sources — regulations, statutes, and official guidance — and reads them against one another to identify the rules, the gaps and the conflicts. It makes no empirical claims. No human participants were involved, no data were collected, and no assertion is made about how teachers or students in fact behave.

Three bodies of law are analysed. The first is the EU Artificial Intelligence Act, Regulation (EU) 2024/1689, as amended by Regulation (EU) 2026/1744, together with the European Commission's draft guidelines on high-risk classification of 19 May 2026 and the Commission's ethical guidelines for educators. The second is Ukrainian copyright law, principally Law No. 2811-IX of 1 December 2022. The third is Ukraine's academic integrity regime under Article 42 of Law No. 2145-VIII on Education, read with the data protection framework of Law No. 2297-VI.

Soft-law instruments are treated as what they are. The UNESCO guidance on generative artificial intelligence (UNESCO, 2023), the UNESCO competency framework for teachers

(Miao & Cukurova, 2024), Ukraine's Roadmap and White Paper on AI regulation, and institutional codes of conduct all shape practice and none of them creates an obligation enforceable against a teacher. Where this article draws on them, it says so.

Two limits should be stated at the outset. The analysis is current to 1 September 2026; Ukraine's standalone artificial intelligence bill is expected during the fourth quarter of that year and will alter the picture. And the article addresses higher education, specifically initial teacher preparation. The Commission's ethical guidelines for educators are aimed principally at primary and secondary schooling, and are used here for the principles they articulate rather than as a source of obligation in the university setting.

3. The EU Layer: What the AI Act Does to Teacher Education

The most persistent error in the education literature is the proposition that the AI Act treats artificial intelligence in education and vocational training as high-risk. The Act does nothing of the sort. Article 6(2) makes a system high-risk if it falls within one of the categories in Annex III, and point 3 of that Annex contains four discrete entries: systems used to determine access or admission to educational institutions, or to assign persons to them; systems used to evaluate learning outcomes, including where those outcomes steer a learner's path; systems used to assess the appropriate level of education a person will receive; and systems used to monitor and detect prohibited behaviour during examinations.

Each of those is an act performed upon a learner with consequences for that learner's future. None of them describes a chatbot used by a teacher to draft a reading passage. The Annex is a list of functions, not a designation of a sector, and the distinction is not pedantic: the entire compliance apparatus of Chapter III — risk management, technical documentation, logging, human oversight, conformity assessment, registration — attaches to the four functions and to nothing else in the educational field. Manganello et al. (2025) show what compliance with point 3(b) would actually require of a university deploying automated learning-outcome assessment, and the gap between that regime and ordinary classroom use of a general-purpose assistant is not a matter of degree.

Article 6(3) narrows the category further. A system that falls within an Annex III heading is not high-risk where it performs only a narrow procedural task, improves the result of a previously completed human activity, detects decision patterns without replacing human assessment, or performs preparatory work. The Commission's draft classification guidelines of 19 May 2026 read these exceptions restrictively and switch them off entirely where the system profiles natural persons within the meaning of Article 4(4) GDPR. The guidelines also treat interconnected systems that function together as a single system, which forecloses the strategy of distributing a high-risk function across components.

The draft guidelines distinguish pedagogical support, which is often filter-eligible, from evaluative application, which is not. That line is the operative one for teacher education. Lesson preparation, materials drafting, differentiation and formative feedback sit on the pedagogical side. Summative marking, placement testing and proctoring sit on the evaluative side and carry the full regime.

Regulation (EU) 2026/1744, the Digital Omnibus on artificial intelligence, was published

on 24 July 2026 and entered into force three days later. Its principal effect is temporal: the obligations attaching to standalone Annex III systems, which were to apply from 2 August 2026, now apply from 2 December 2027, and those attaching to high-risk systems embedded in regulated products move to 2 August 2028. For a university contemplating automated assessment, that is sixteen months of additional runway. It is not an exemption, and it does not touch the classification analysis, which must be performed on the existing timetable if the eventual obligations are to be met.

What did not move matters more for present purposes. Article 4, the artificial intelligence literacy duty, has applied since 2 February 2025 and was not deferred, although the Omnibus amended its wording with effect from 27 July 2026. Providers and deployers must take measures supporting the development of literacy among staff and others operating systems on their behalf, having regard to their knowledge, experience and education, to the context of use and to the persons affected; they are not required to guarantee that any individual attains a specified level. Article 50, the transparency regime, has applied since 2 August 2026 and was likewise untouched, with a short grace period to 2 December 2026 for machine-readable marking of outputs by generative systems already on the market. The prohibitions in Article 5 have applied since 2 February 2025 and now include a further prohibition, phased to 2 December 2026, on systems whose reasonably foreseeable output is non-consensual intimate imagery or child sexual abuse material.

The shape of the obligation set for education is therefore counter-intuitive. The heavy regime, which most commentary treats as imminent, does not bite for over a year and covers a narrow band of functions. The light regime, which commentary barely mentions, binds now and covers everyone.

Article 4 addresses providers and deployers. A university that makes an artificial intelligence system available to staff or students is a deployer, and the duty is its own. It is not a duty owed by the student teacher, and it is not discharged by the student teacher having taught herself to write prompts. This inversion is worth stating plainly, because the pedagogical literature routinely locates artificial intelligence literacy in the individual educator as a matter of professional competence. As a matter of Union law it sits with the institution as a matter of compliance, and the institution must be able to evidence the measures it has taken.

Two consequences follow for initial teacher preparation. A faculty that deploys such tools in its own programmes owes the Article 4 duty to its students in their capacity as operators. And its graduates will enter schools that owe the same duty to them, which makes the content of the duty part of what they need to understand before they arrive. Neither consequence is captured by treating literacy as a curricular aspiration.

One prohibition applies squarely to the classroom. Article 5 forbids placing on the market or using systems that infer emotions of a natural person in the workplace or in educational institutions, except where deployed for medical or safety reasons. Engagement analytics, attention monitoring and affect detection marketed for language classrooms fall within it. This is not a high-risk classification requiring documentation; it is a prohibition, and it has been in force since February 2025.

Taken together, the Union layer is narrower and sharper than the literature suggests. It

prohibits a small number of practices outright, imposes literacy and transparency duties on institutions now, and defers a demanding regime for four evaluative functions until the end of 2027. It says nothing whatever about a teacher drafting a lesson with a chatbot.

4. Data Protection: Which Regime Actually Binds

Writing on digitalisation in Ukrainian higher education frequently states that universities must handle data in accordance with European standards including the General Data Protection Regulation. As a statement of policy direction that is accurate. As a statement of applicable law it is not, and the imprecision has practical consequences.

Regulation (EU) 2016/679 applies under Article 3 to processing in the context of the activities of an establishment in the Union, and to processing by a controller not established in the Union where the processing relates to offering goods or services to data subjects in the Union or to monitoring their behaviour within the Union. A Kyiv university teaching Ukrainian students in Ukraine satisfies neither limb. It may fall within Article 3(2) in specific configurations — an exchange programme recruiting in Member States, a joint degree with an EU partner, an online course marketed to learners in the Union — but that is a conclusion to be reached on the facts, not a default.

The distinction matters because a university that believes itself bound by the GDPR and is not will design to a standard it cannot be held to, while overlooking the standard it can. Compliance effort is finite. Directing it at the wrong instrument is not a conservative error.

The applicable framework is Law of Ukraine No. 2297-VI on Personal Data Protection, supervised by the Parliament Commissioner for Human Rights. It is built on the same architecture as the pre-2018 European regime — lawful basis, purpose limitation, data subject rights, obligations on controllers and processors — and it is materially thinner than the GDPR in the areas that generative artificial intelligence stresses most: automated decision-making, transfers to third countries, and the accountability documentation that would evidence a lawful basis for a novel processing operation.

Alignment is a declared objective of the accession process rather than an accomplished fact, and the interim position is the operative one. Where a Ukrainian institution is not caught by Article 3(2) GDPR, its obligations are those of Law No. 2297-VI, and the gap between the two is the space in which most classroom uses of commercial language models currently sit.

The concrete question is narrow. A teacher pastes a pupil's written work into a commercial system in order to obtain feedback. Three characterisations of that act are possible and they are not equivalent.

It is a disclosure of personal data to a third party, because a pupil's essay is data relating to an identifiable person and its content may reveal a great deal more. It is a transfer outside Ukraine, because the processing occurs on the provider's infrastructure. And it may be a licensing act, because the terms of service of most consumer products reserve rights to process submitted content, sometimes including its use in model improvement.

Each characterisation attracts a different rule, and the institution rather than the individual teacher is the controller. The European Commission's revised guidelines for educa-

tors put the underlying caution plainly: uploading learner work to publicly accessible large language models creates risks for privacy, data protection and intellectual property. That instrument does not bind a Ukrainian university, and the analysis does not depend on it. It depends on whether a lawful basis exists under Law No. 2297-VI for disclosing identifiable learner work to an external processor for a purpose that was not contemplated when the work was collected. In the absence of an institutional policy, a processing agreement and a stated basis, the honest answer is that it does not.

5. Who Holds Rights In The Generated Lesson

Union copyright law contains no rule allocating rights in the output of a generative system. The originality requirement developed in the case law of the Court of Justice presupposes the author's own intellectual creation and free creative choices, which locates protection in human authorship and leaves purely machine-generated material outside it without saying what, if anything, occupies the vacated space. The Digital Single Market Directive addresses the input side through the text and data mining exceptions in Articles 3 and 4, and is silent on the output side. Member State practice diverges. There is no harmonised answer, and none is imminent.

Ukraine took a position. Law No. 2811-IX, in force since 1 January 2023, creates in Article 33 a right of a special kind — pravo osoblyvoho rodu, sui generis — in non-original objects generated by a computer program. Article 8(4) confirms that such objects fall outside copyright and are protected by that right instead. The provision predates the general availability of the systems it now governs, and it is worth setting out its terms precisely, because each element does work.

Article 33(1) defines a non-original generated object as one that differs from existing similar objects and is formed through the functioning of a computer program without the direct participation of a natural person in its formation. The second sentence draws the boundary from the other side: works created by natural persons using computer technologies are not non-original generated objects. The dividing line is therefore the presence of human creative contribution to the formation of the particular output, not the involvement of software in the process.

Article 33(2) identifies the right-holders: persons holding economic rights in, or licensing powers over, the computer program — its authors, their heirs, transferees, or lawful users of the program. Contract may vary the allocation. Article 33(3) is short and consequential: no moral rights arise from the generation of such an object. Article 33(4) sets the scope of economic rights by reference to Article 12, the general provision on exploitation. Article 33(5) makes the right arise automatically upon generation. Article 33(6) fixes the term at twenty-five years from 1 January of the year following generation. Article 33(7) subordinates the right: where the generated object results from the use of protected works or related-rights subject matter, the holder may exercise the sui generis right only subject to the rights of those whose material was used. Article 33(8) confers the exclusive right to license, and Article 33(9) permits assignment.

The first consequence is that the teacher probably does hold rights. As a lawful user of

the program she falls within the class identified in Article 33(2), and the right arises by the fact of generation without registration or formality. She is not, however, an author, and she cannot become one. Article 33(3) forecloses it. She may license and assign; she may not claim authorship, demand attribution as author, or object to distortion of the material on the moral-rights basis available under Article 11 for works. A lesson plan generated in this way is property she controls for twenty-five years and not a work she made.

The second consequence is that the distinction is fragile in practice. Most real teaching materials are not purely generated. The teacher prompts, discards, selects, reorders, rewrites and adapts. At some point along that sequence the second sentence of Article 33(1) engages and the output becomes a work created by a natural person using computer technologies, protected by copyright with the teacher as author. Ukrainian law offers no threshold and no guidance on where the point lies, and there is no case law. Two materials produced in the same afternoon may sit on opposite sides of the line with no reliable way of telling which is which.

The third consequence concerns employment. Article 14 vests economic rights in a work made in the course of employment in the employer from the moment of creation, subject to contrary agreement, and Article 15 does the same for commissioned works. Article 33 contains no equivalent provision for generated objects, and the allocation instead follows the licensing position in the program, subject to contract. Whether a lesson plan generated by a lecturer on a university-procured licence belongs to the lecturer or the university is therefore a question of the licence terms and the employment contract, not of the copyright default. Few Ukrainian universities have addressed it in either instrument.

Article 1(21) defines the lawful user of a computer program as a person lawfully possessing a lawfully made copy of it. That definition was drafted for installed software. It does not describe a person who accesses a hosted service through a browser, holds no copy, and cannot make one.

On a literal reading, a teacher using a cloud-based assistant is not a lawful user within the meaning of Article 1(21), does not fall within Article 33(2), and holds no sui generis right at all — with the consequence that the right vests, if anywhere, in the provider. On a purposive reading, the definition should be construed to cover authorised access to a service, and the teacher holds the right subject to whatever the provider's terms say. The provision has not been tested, and the terms of service of the major providers do not resolve it in the vocabulary the statute uses.

This is not a peripheral drafting point. It determines whether a Ukrainian institution can build an intellectual property policy for AI-assisted materials on the statute at all, or must construct one entirely from contract.

Article 22 permits certain uses of works without authorisation. Article 22(2)(2) allows reproduction and interactive provision of lawfully published articles, short works and extracts as illustrations in the educational process or for research, where the use has no independent economic significance and is carried out by educational or scientific bodies on their premises or through a secure electronic environment accessible exclusively to that institution's learners and teaching staff. Article 22(2)(3) permits reprographic reproduction for classes on a non-systematic basis, and Article 22(2)(14) contains the text and data

mining exception, subject to machine-readable reservation by rights-holders.

Two features of this scheme constrain generative use directly. The educational exception is expressly conditioned on the secure closed environment; a commercial chatbot is the opposite of one, so submitting third-party copyright material to it in order to generate teaching content is not covered. And Article 22(3) states that the list of permitted free uses is exhaustive. Ukrainian law contains no fair use doctrine and no residual flexibility. Where the conduct is not on the list, it requires authorisation, and Article 33(7) reinforces the point from the other direction: a generated object built on protected input carries the sui generis right only if the input rights were respected.

6. Academic Integrity: An Interlocking Failure

Article 42 of Law No. 2145-VIII on Education defines academic integrity and enumerates its violations. Part 4 lists academic plagiarism, self-plagiarism, fabrication, falsification, cheating, deception, bribery, biased assessment, and the provision of assistance or obstruction during assessment. The list is a statutory one, and disciplinary consequences under Ukrainian institutional practice are ordinarily traced to a listed head.

Two of the definitions matter here. Cheating is the performance of written work with the involvement of external sources of information other than those permitted for use, in particular during the assessment of learning outcomes. Deception is the provision of knowingly false information about one's own educational, scholarly or creative activity, and its forms are stated to include plagiarism, self-plagiarism, fabrication, falsification and cheating.

Academic plagiarism consists in presenting another person's work as one's own. The concept requires an appropriated author. Article 33(3) of the copyright law states that no moral rights arise from the generation of a non-original object, and Article 33(1) defines such an object as formed without the direct participation of a natural person. Ukrainian legislation therefore holds, in terms, that there is no author to appropriate.

The two statutes thus interlock in a way neither drafter intended. Submitting generated prose as one's own cannot be academic plagiarism, because the conduct plagiarism describes is impossible with respect to material the legal system says has no author. This is not a gap left by silence. It is a conclusion compelled by two provisions that are individually coherent and jointly awkward.

Cheating remains available, and it is the natural head. But its definition is conditional in a way that is easy to miss. The prohibited conduct is the use of external sources of information other than those permitted for use. The statute does not itself designate which sources are permitted. It presupposes that someone else has done so.

Where a university has adopted a policy stating that generative systems are not a permitted source in assessed work, undisclosed use is cheating and the statutory head is engaged. Where no such policy exists, the source has not been placed outside the permitted set, and the conduct does not answer to the definition. The same act is a disciplinary offence at one institution and unregulated at another, and the difference is not a matter of interpretation but of whether a document exists.

Deception offers no reliable fallback. It requires knowingly false information about one's

own activity. Silence is not an assertion, and it becomes one only where a duty to disclose has been created. Absent an institutional declaration requirement, a student who does not mention having used a chatbot has stated nothing false. Where such a requirement exists and is breached, deception is straightforwardly engaged — but again the operative instrument is institutional, not statutory.

The pattern in both heads is the same. Article 42 supplies the sanctionable categories and delegates the substantive content to institutional rule-making. That is a defensible legislative design; universities are closer to the practices they regulate, and a statutory list of permitted tools would date within a year. It functions only where the delegate legislates.

The delegation was made in 2017, before the technology existed. It has not been revisited, and no binding national instrument has since specified how generative artificial intelligence relates to any of the listed violations. What exists is soft law: ministerial and expert recommendations, the Ministry of Digital Transformation's Roadmap of 2023 and White Paper of 2024, a regulatory sandbox, a code of conduct, an updated terminology dictionary. These are preparatory instruments in an explicitly bottom-up strategy whose second stage — binding legislation harmonised with the AI Act — is expected to begin with a draft bill in the fourth quarter of 2026. Ukraine has also signed the Council of Europe Framework Convention on artificial intelligence.

None of that reaches the student who submitted generated coursework last week. Until an institution has adopted a policy, the statutory heads under Article 42 are either definitionally unavailable, in the case of plagiarism, or conditionally unavailable, in the case of cheating and deception.

7. The Unregulated Middle

The three preceding sections describe layers that do not meet.

Above sits the Union layer, which prohibits emotion inference in educational settings, imposes literacy and transparency duties on deployers now, and defers a demanding regime for four evaluative functions to December 2027. It is precise, it is enforceable, and — for a Ukrainian institution — it applies only as an accession trajectory and through the occasional operation of Article 3(2) GDPR.

Below sits the Ukrainian statutory layer, which allocates a proprietary right in generated output without authorship, protects personal data to a pre-2018 European standard, and enumerates academic integrity violations whose substantive content is delegated to institutions.

Between them sits everything a student teacher actually does. Drafting a reading passage. Producing a glossary. Generating comprehension questions. Adapting a text for a mixed-ability group. Obtaining feedback on a pupil's writing. Preparing a portfolio for assessment. None of this is high-risk under Annex III. None of it is prohibited under Article 5. The copyright position is governed by a provision whose central definition does not fit cloud services and whose boundary with authorship has no threshold. The integrity position depends on an institutional document that in most cases has not been written.

This is the unregulated middle. It is not a lawless space; several rules touch it at the edges.

It is a space in which the rules that touch it were drafted for other objects, and in which the instrument designed to occupy it — institutional policy — has not been issued.

Two features make it durable. The Digital Omnibus deferral means that the Union regime most likely to prompt Ukrainian institutional reform will not bite until the end of 2027, removing the nearest external deadline. And the bottom-up sequencing of Ukraine's own strategy is deliberate: soft instruments first, binding law later, with the draft bill not expected before the final quarter of 2026 and adoption necessarily later still. The middle will therefore remain open for at least two more academic years.

8. Implications

8.1. For institutions

Four items follow directly from the analysis and none requires new legislation.

An institution should specify, under Article 42 of the Law on Education, whether and in what circumstances generative systems are a permitted source in assessed work, because until it does so the statutory head of cheating cannot be engaged. It should create a disclosure requirement, because deception is otherwise unavailable and because disclosure is the only mechanism that makes the permitted-source rule administrable. It should settle the intellectual property position by contract — in the procurement licence and in the employment contract — because Article 33 provides no employment default and because its definition of the lawful user may not reach hosted services at all. And it should establish a lawful basis and a processing arrangement before learner work is disclosed to any external system, or prohibit that disclosure, because under Law No. 2297-VI the institution is the controller and the individual teacher is not in a position to supply the basis.

A fifth item follows from Union law for any institution within its reach: Article 4 requires measures supporting artificial intelligence literacy among those operating systems on the institution's behalf, and requires them to be evidenced.

8.2. For teacher education curricula

The competency frameworks that structure this field treat legal awareness as one dimension among several. The UNESCO framework for teachers places ethics of artificial intelligence alongside a human-centred mindset, foundations, pedagogy and professional development (Miao & Cukurova, 2024), and the UNESCO guidance for generative artificial intelligence in education proceeds from human agency, learner protection and institutional governance (UNESCO, 2023). Both are sound and both are soft law.

What this article's analysis adds is that the legal content required is more specific than those frameworks suggest and different in kind from ethical reasoning. A graduating teacher who understands that AI use raises questions of copyright and privacy is better prepared than one who does not, and is still not equipped to answer whether she may license the material she generated, whether her employer owns it, or whether her school's silence on permitted sources means her pupils may use a chatbot for homework. Those questions have determinate answers derivable from the instruments analysed here, and none of them appears in a competency framework.

The practical suggestion is modest. Initial teacher preparation in Ukraine could usefully include a short unit on the actual rule set — Article 42 and the delegation it makes; Article 33 and what it does and does not confer; the controller position under Law No. 2297-VI; and the shape of the AI Act as the accession trajectory brings it closer. This is a matter of a few hours, and it produces graduates who can read their own institution's policy and notice when it is absent.

9. Conclusions

This article set out to establish which binding rules govern the use of generative artificial intelligence in Ukrainian foreign language teacher education. Three conclusions emerge.

The EU Artificial Intelligence Act is narrower in the educational field than the literature reports. It designates four evaluative use cases in Annex III rather than a sector, subjects them to a filter that the Commission's 2026 draft guidelines read restrictively, and — since Regulation (EU) 2026/1744 — defers the obligations attaching to them to 2 December 2027. What binds now is the Article 4 literacy duty, addressed to institutions rather than to individual educators, the Article 50 transparency regime, and the Article 5 prohibition on emotion inference in educational settings.

Ukraine's sui generis right in non-original generated objects is a genuine statutory answer to a question most jurisdictions have left open, and it answers it in an unexpected register: property without authorship, twenty-five years, no moral rights, subordinated to the rights in any protected input, and allocated by reference to a definition of the lawful user of a computer program that was written for installed software and does not obviously reach a hosted service.

The academic integrity regime cannot be applied to undisclosed generative use without institutional action. Plagiarism is definitionally unavailable, because Ukrainian copyright law states that the material has no author. Cheating and deception are available in principle but conditional on institutional designation of permitted sources and on an institutional disclosure duty. Article 42 delegated that content in 2017 and most delegates have not exercised it.

The composite result is the unregulated middle: a space occupied daily by ordinary teaching practice, bounded by rules drafted for other purposes, and left by statute to an institutional instrument that in most cases does not exist. Sustainable governance of artificial intelligence in education will not arrive through the AI Act, whose relevant obligations are deferred and whose scope is narrow, nor through a Ukrainian bill that has not yet been introduced. It will arrive, if at all, through institutions writing the rules that national law has already asked them to write.

10. Limitations

Three limitations bound the claims made here. The analysis is doctrinal and reports what the instruments provide, not how institutions or individuals behave; whether Ukrainian universities have in fact adopted policies under Article 42, and what those policies say, is

an empirical question this article does not answer and which would repay documentary survey. The legal position is stated as at 1 September 2026 and is unstable in two respects: Ukraine's standalone artificial intelligence bill is expected in the fourth quarter of 2026, and the Commission's guidelines on high-risk classification were still in draft when this article was written. And the argument addresses Ukraine; the AI Act analysis travels to any Member State, but the copyright and integrity analysis is jurisdiction-specific, and comparison with states that have not legislated on computer-generated output would sharpen the account of what Article 33 achieves.

Funding

This research received no external funding.

Conflicts of Interest

The author declares no conflicts of interest.

Ethics Statement

This is a doctrinal legal analysis. No human participants were involved and no personal data were collected; ethical approval was therefore not required.

Data Availability

All sources analysed are publicly available and cited in full.

References

Council of Europe. (2024). Framework Convention on Artificial Intelligence and Human Rights, Democracy and the Rule of Law (CETS No. 225). Council of Europe.

Directive (EU) 2019/790 of the European Parliament and of the Council of 17 April 2019 on copyright and related rights in the Digital Single Market. Official Journal of the European Union, L 130, 92–125.

Edmett, A., Ichaporia, N., Crompton, H., & Crichton, R. (2024). Artificial intelligence and English language teaching: Preparing for the future (2nd ed.). British Council. https://doi.org/10.57884/78EA-3C69

European Commission. (2026a). Draft Commission guidelines on the classification of high-risk AI systems. https://digital-strategy.ec.europa.eu/en/library/draft-commission-guidelines-classification-high-risk-ai-systems

European Commission, Directorate-General for Education, Youth, Sport and Culture. (2026b). Guidelines on the ethical use of artificial intelligence and data in teaching and learning for educators (rev. ed.). Publications Office of the European Union. https://education.ec.europa.eu/focus-topics/digital-education/actions/plan/ethical-guidelines-for-educators-on-using-artificial-intelligence

Gill, S. S., Xu, M., Patros, P., Wu, H., Kaur, R., Kaur, K., Fuller, S., Singh, M., Arora, P., Parlikad, A. K., Stankovski, V., Abraham, A., Ghosh, S. K., Lutfiyya, H., Kanhere, S. S., Bahsoon, R., Rana, O., Dustdar, S., Sakellariou, R., … Buyya, R. (2024). Transformative effects of ChatGPT on modern education: Emerging era of AI chatbots. Internet of Things and Cyber-Physical Systems, 4, 19–23. https://doi.org/10.1016/j.iotcps.2023.06.002

Harakchiyska, T. (2025). Predictors of pre-service EFL teachers' predisposition towards AI adoption in langu-

age teaching. Education Sciences, 15(9), 1112. https://doi.org/10.3390/educsci15091112

Kasneci, E., Sessler, K., Küchemann, S., Bannert, M., Dementieva, D., Fischer, F., Gasser, U., Groh, G., Günnemann, S., Hüllermeier, E., Krusche, S., Kutyniok, G., Michaeli, T., Nerdel, C., Pfeffer, J., Poquet, O., Sailer, M., Schmidt, A., Seidel, T., … Kasneci, G. (2023). ChatGPT for good? On opportunities and challenges of large language models for education. Learning and Individual Differences, 103, 102274. https://doi.org/10.1016/j.lindif.2023.102274

Law of Ukraine No. 2145-VIII of 5 September 2017 "On Education". Vidomosti Verkhovnoi Rady Ukrainy. https://zakon.rada.gov.ua/laws/show/2145-19

Law of Ukraine No. 2297-VI of 1 June 2010 "On Personal Data Protection". Vidomosti Verkhovnoi Rady Ukrainy. https://zakon.rada.gov.ua/laws/show/2297-17

Law of Ukraine No. 2811-IX of 1 December 2022 "On Copyright and Related Rights". Vidomosti Verkhovnoi Rady Ukrainy. https://zakon.rada.gov.ua/laws/show/2811-20

Manganello, F., Nico, A., Ragusa, M., & Boccuzzi, G. (2025). Testing the applicability of a governance checklist for high-risk AI-based learning outcome assessment in Italian universities under the EU AI Act Annex III. Frontiers in Artificial Intelligence, 8, 1718613. https://doi.org/10.3389/frai.2025.1718613

Miao, F., & Cukurova, M. (2024). AI competency framework for teachers. UNESCO. https://doi.org/10.54675/ZJTE2084

Ministry of Digital Transformation of Ukraine. (2023). Roadmap for the regulation of artificial intelligence in Ukraine. https://thedigital.gov.ua

Ministry of Digital Transformation of Ukraine. (2024). White paper on artificial intelligence regulation in Ukraine. https://thedigital.gov.ua

Nazaretsky, T., Ariely, M., Cukurova, M., & Alexandron, G. (2022). Teachers' trust in AI-powered educational technology and a professional development program to improve it. British Journal of Educational Technology, 53(4), 914–931. https://doi.org/10.1111/bjet.13232

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 (General Data Protection Regulation). Official Journal of the European Union, L 119, 1–88.

Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonised rules on artificial intelligence (Artificial Intelligence Act). Official Journal of the European Union, L, 2024/1689. http://data.europa.eu/eli/reg/2024/1689/oj

Regulation (EU) 2026/1744 of the European Parliament and of the Council amending Regulation (EU) 2024/1689 (Digital Omnibus on Artificial Intelligence). Official Journal of the European Union. http://data.europa.eu/eli/reg/2026/1744/oj

Sharples, M. (2023). Towards social generative AI for education: Theory, practices and ethics. Learning: Research and Practice, 9(2), 159–167. https://doi.org/10.1080/23735082.2023.2261131

UNESCO. (2023). Guidance for generative AI in education and research. UNESCO Publishing. https://doi.org/10.54675/EWZM9535

Yan, L., Greiff, S., Teuber, Z., & Gašević, D. (2024). Promises and challenges of generative artificial intelligence for human learning. Nature Human Behaviour, 8(10), 1839–1850. https://doi.org/10.1038/s41562-024-02004-5

Dei, H. (2026). Public Governance of Cybersecurity in Higher Education Institutions: Legal and Institutional Foundations for Sustainable Digital Transformation in Ukraine. ESS Conference Series Social Science and Humanities, 1(1). https://doi.org/10.54658/esscssh.2026.1.1.11

Public Governance of Cybersecurity in Higher Education Institutions: Legal and Institutional Foundations for Sustainable Digital Transformation in Ukraine

Herasym Dei
Department of Public Administration and Project Management
State Higher Education Institution „University of Educational Management"
Kyiv, Ukraine
ORCID iD: 0009-0009-5358-3047
herasym_dei@edu.cn.ua

Abstract.
Legal and organisational structures in higher education must reconcile the sector's security with its capacity to develop sustainably. This article asks how legal rules and institutional governance can support cybersecurity as a condition of sustainable digital transformation in Ukrainian universities. A qualitative documentary and comparative policy design was applied to a purposive corpus of 30 sources (19 peer-reviewed articles, 11 official legislative, strategic and policy documents), coded against five governance dimensions: legal mandate, distribution of institutional responsibility, inter-organisational coordination, university-level arrangements, and the embedding of security requirements in long-term digital development. Ukraine has a comparatively developed national framework for information protection, cybersecurity coordination, critical-infrastructure protection and organisational resilience, but it is not translated into sector-specific requirements for higher education. National roles and coordination are established, whereas it remains only partly defined how and to whom university leaders report, how incident reporting connects to handling, what competences are required, and how resilience is planned. Comparison with selected European instruments shows partial convergence on risk-based security, accountability, information protection and coordination, but weaker sectoral articulation of professional roles, management responsibility, assurance mechanisms and links to technology strategy. The principal conclusion is institutional fragmentation rather than regulatory absence: a sectoral coordination layer is needed to connect national regulation with autonomous university governance, setting minimum standards of organisational responsibility, management accountability, competence, incident coordination, supplier-risk control and continuity planning, without creating a parallel administrative system. The study is confined to documentary evidence and does not assess the effectiveness of practice in individual universities..
Keywords: *regulatory coordination; organisational accountability; resilience planning; sectoral policy integration; management responsibility; information protection.*

1. Introduction

The growing digitalisation of higher education has made universities more reliant on cloud platforms, learning management systems, digital identity providers, and networked research infrastructures. This reliance has also increased the attack surface of higher education institutions (HEIs), which hold sensitive personal data, intellectual property, financial

information, and critical educational workflows. Recent analyses highlight the persistence of threats to the sector such as phishing, malware, credential compromise, software vulnerabilities, poor incident reporting and a low level of cybersecurity awareness (Afolalu & Tsoeu, 2025; Salam et al., 2026). Cybersecurity in universities is therefore not merely a technical infrastructure to be managed: the resilience of an institution depends as much on its governance arrangements — organisational capability, internal regulation, staff practice, and coordination between those responsible — as on the security of its critical technical infrastructure.

In this, the Ukrainian case is no exception. Under martial law, universities continue to function in the face of cyberattack, disinformation, the threat of personal data leaks, and a growing dependence on digital communication and distance education services (Chornomydz, 2025). At national level, the Cybersecurity Strategy of Ukraine identifies cyber resilience, institutional cooperation, capacity building, and a secure national cyberspace as areas of strategic importance (President of Ukraine, 2021). These priorities have not yet been translated adequately into the means by which the higher education sector itself is governed.

Current cybersecurity policy is converging on the treatment of cybersecurity as a public-governance challenge that can be addressed only through the coordinated application of informational, regulatory, financial and organisational instruments, rather than through stand-alone technical tools (Cotta & Righettini, 2026). The higher education literature, by contrast, continues to be concerned primarily with threats, vulnerabilities, awareness, and technical safeguards (Afolalu & Tsoeu, 2025; Salam et al., 2026). There is therefore a disconnect between national-level cybersecurity governance and the level of the Ukrainian university.

This study asks how legal rules and institutional governance can support cybersecurity as a medium of sustainable digital transformation in Ukrainian higher education. It is guided by three questions: how national cybersecurity priorities are realised at the level of the university; what type of institutional arrangements enhance cyber resilience; and in which areas of public governance such capacity is lacking.

The question is posed here as a legal and institutional one rather than a technical one. What is at issue is not which controls a university should deploy, but how a binding national cybersecurity regime and a statutorily autonomous university are to be connected: which obligations attach to a higher education institution as a regulated organisation, which follow instead from its own governing decisions, and through what interface the two meet. Framed in these terms, the analysis belongs to the study of law, digital technologies and sustainable governance, and it is offered as a contribution to that field.

2. Literature Review

Studies of cybersecurity in higher education are converging on the view that universities are not simply another kind of digitally intensive organisation but a distinctive security environment. Their openness, diverse user bases, decentralised decision-making, large data holdings, and reliance on interconnected academic and administrative systems make

traditional information-security paradigms difficult to apply. Bongiovanni (2019) pointed out that information security management in higher education is a field that has attracted little research attention, particularly as regards security culture, cross-institutional studies, and security economics. Subsequent reviews have broadened the evidential basis but have not substantially addressed this deficit in governance. One such review (2022) highlighted increasing academic and administrative information risk in step with greater reliance on cloud services, while Nuñez et al. (2023) classified organisational responses as institutional, technological, physical, and standards-based security measures. The strength of these analyses is that they identify operational vulnerabilities and the controls available against them; what is missing is an account of institutional security as part of, rather than distinct from, a broader public-governance regime.

The same tendency appears in research on information security frameworks. Merchan--Lima et al. (2021) found a wide variety of frameworks, implementation phases, infrastructure services, and protective mechanisms in use across higher education institutions. This shows that cybersecurity is not simply a matter of deploying individual technical controls. However, this diversity of frameworks also poses a challenge to institutional consistency: the presence of standards does not by itself determine who is responsible, how priorities are coordinated, or how compliance and accountability are ensured among multiple actors. The ISO 27000-series standards and the CIS controls are examples of frameworks used by universities (Nuñez et al., 2023), but these instruments are designed principally to define security practices, not to allocate authority in the public sector. As a result, the literature is better equipped to answer how a university information system can be protected than how responsibility for cybersecurity should be governed.

This article approaches the emergent scholarship on cyber-governance from a wider conceptual vantage point. Kuerbis and Badiei (2017) distinguish market, networked, and hierarchical governance mechanisms, and show that cybersecurity is the outcome of the interaction of these mechanisms rather than of government hierarchy alone. Correspondingly, Savaş and Karataş (2022) argue that management without stakeholder-inclusive cyber governance is insufficient, and observe that no universally accepted governance model exists. Recent evidence cements this institutional reading. Carmichael (2026), analysing Estonia through the lens of collaborative governance, demonstrates that responsibility for cybersecurity within government can shift over time, and that conceptions of cybersecurity may remain underdeveloped even in a digitally mature state. Collectively, these works challenge state-centric models, but their level of analysis remains overwhelmingly national or ecosystem-wide. They offer a useful vocabulary for analysing coordination and responsibility, but they do not specify how such arrangements should operate in a field marked by university autonomy, public regulation, academic openness and decentralised digital infrastructure.

The gap is more pronounced in the digital-transformation literature. Castro Benavides et al. (2020) found that no genuinely holistic models of digital transformation exist for the higher education context. Fernández et al. (2023) show that digital transformation involves strategic, informational, process, technological, and human change rather than technology implementation alone. Their review of university projects indicates considerable attention to the quality of education, but also questions whether such isolated projects have a place

within an overall institutional digital strategy. Farias-Gaytan et al. (2023) similarly show that research focuses overwhelmingly on digital competences and educational technologies, with some attention to broader aspects of digital literacy. The transformation literature therefore acknowledges institutional complexity, but it does not often conceptualise cybersecurity governance as a component of the digital transformation process.

This tension is further highlighted by studies of barriers. Gkrimpizi et al. (2023) identify twenty barriers, grouped into environmental, strategic, organisational, technological, people-related and cultural categories, and conclude that the technical capability of an organisation is not the only reason why digital transformation fails. Singun (2025) extends this view through nine dimensions: digital vision, leadership, organisation, resources, competence, stakeholder management, culture, academic processes and ethics. These multidimensional approaches are analytically valuable because they move beyond technological determinism. However, cybersecurity is generally treated as one element of a larger transformation agenda rather than as a cross-cutting governance condition linking institutional accountability with regulatory compliance, resilience and continuity.

A further contextual gap is found in the small body of research relating to Ukraine. Nashynets-Naumova et al. (2020) address information and cybersecurity technologies in the system of Ukrainian higher education institutions, and Kobis et al. (2024), in a comparative study of universities in Poland, Ukraine and the Czech Republic, highlight the significance of employees' views on information security and of training needs in the handling of digital resources. These papers confirm that technological protection and human capability matter in the Ukrainian case. They stop short, however, of offering a comprehensive account of the relationship between university-level practice, national cybersecurity governance arrangements, statutory obligations, institutional accountability, and the strategic dimension of higher education digitalisation.

Finally, institutional sustainability is itself related to cybersecurity. Othman (2023) connects hijackability as a factor in the survivability of higher education institutions with their ability to withstand cyberattacks, illustrating through a qualitative case study that institutions are under assault on multiple fronts and must enhance their cybersecurity governance. The single-case design, however, limits the transferability of these conclusions to other legal and institutional contexts.

The literature is thus scattered across three relatively insular areas: university-based cybersecurity management, national or ecosystem-level cyber governance, and higher education digital transformation. What has not yet emerged is a coherent analytical framework capturing the ways in which legal norms, public governance models, institutional duties, and university-level cybersecurity practices interrelate within a specific national higher education system. This divide is especially consequential for Ukraine, where digital transformation and cyber resilience must be built concurrently in a distinctive institutional and security context. The open research question is therefore not only what cybersecurity measures universities should take, but also how public governance can coordinate legal requirements, institutional capabilities, stakeholder obligations, and resilience mechanisms so that the digital transformation of higher education in Ukraine is both sustainable and secure.

3. Materials and Methods

The research was carried out in August–September 2026 as a qualitative policy analysis of legal and institutional documents governing cybersecurity in the context of Ukrainian higher education. The unit of analysis was the individual legal rule, policy instrument, institutionally mandated responsibility, or governance mechanism applicable to cybersecurity, cyber resilience, or the digital transformation of higher education institutions. The study involved no human subjects, surveys, experiments, interventions, or personal information.

The documentary evidence was treated not as a systematic-review sample but as an intentionally assembled analytical corpus. Non-random purposive sampling yielded 30 documents in two evidence groups: 19 peer-reviewed scientific publications and 11 official legal, strategic, and institutional documents. The scientific literature reviewed, produced mainly between 2019 and 2026, related to cybersecurity governance, information-security management in higher education, cyber resilience, institutional sustainability, and digital transformation. A publication was retained only where it supplied conceptual or governance resources directly applicable to the research problem.

The official-document group comprised four Ukrainian laws relating to higher education, cybersecurity, information protection, and critical infrastructure; the Cybersecurity Strategy of Ukraine; three EU legal instruments, namely the General Data Protection Regulation, the Cybersecurity Act and the NIS2 Directive; the Digital Education Action Plan 2021–2027; and two ENISA documents concerning cybersecurity competences and the current threat landscape. Only authoritative official or consolidated versions were used.

Sources were included if they were relevant to at least one of five substantive areas: cybersecurity in higher education institutions; national or institutional cybersecurity governance; legally defined cybersecurity responsibilities for public or educational organisations; the interplay between digital transformation, institutional resilience and higher education; or the legal status, governance responsibilities, institutional autonomy and organisational role of higher education institutions required to contextualise cybersecurity obligations. Duplicate publications, non-peer-reviewed opinion pieces, commercial web content, documents without clear analytical relevance, and studies confined to the technical aspects of attack detection without organisational or governance implications were excluded.

The analysis was conducted in four phases. First, the corpus was filtered through five a priori governance dimensions: legal mandate, distribution of institutional responsibility, inter-organisational coordination, university-level cybersecurity provision, and the embedding of cybersecurity in sustainable digital transformation. Sustainable digital transformation was understood as continuity, cyber resilience, secure digital infrastructure, institutional capacity, and the minimisation of deterioration in digital function under conditions of cyber risk. Second, the relevant provisions and findings were entered into a structured coding matrix recording source, level of governance, responsible actor, regulatory or organisational modality, compliance and enforcement requirements, and identified governance gap. The degree of HEI-specific regulatory specification was further categorised as direct, partial, indirect or absent, according to whether a source directly regulated higher education, addressed HEIs as a subgroup of more general regulated entities, offered only generic

rules or guiding principles applicable to HEIs, or contained no discernible sector-relevant rule. Third, the national policy framework was analysed for coherence between national strategic priorities, the sectoral legal framework, and the duties entrusted to higher education institutions. Fourth, these arrangements were compared with a selection of EU and ENISA instruments in order to identify convergence, partial harmonisation, institutional fragmentation, and residual governance challenges.

This final interpretative step linked formal legal requirements with documented institutional arrangements and aggregated recurrent relationships into a five-level governance structure comprising national, sectoral, institutional, operational, and assurance functions. Particular attention was paid to the explicit allocation of responsibility, to coordination mechanisms, to the role of universities as regulated organisations or governance actors, and to the incorporation of cybersecurity into digital-transformation policy. Because the design rests only on documentary evidence, the paper evaluates the formal governance architecture and documented institutional arrangements, not the actual performance of cybersecurity practice in individual Ukrainian universities.

4. Results

4.1. Legal mandate and the position of higher education institutions within the cybersecurity framework

The documentary coding reveals a structural asymmetry in the governance relationship. Although Ukraine has a broad general legal regime for cybersecurity and information protection, higher education does not appear within that regime as a distinct area of cybersecurity governance. The Law of Ukraine on the Basic Principles of Cybersecurity defines the national cybersecurity system and its principal public actors, establishes the mechanism for coordination, and imposes certain cybersecurity obligations on ministries and other public authorities, operators of critical infrastructure, owners or administrators of critical information infrastructure, and a number of other entities whose activities relate to national information resources, e-services, communications, information protection or cyber protection (Verkhovna Rada of Ukraine, 2017). The Cybersecurity Strategy places particular emphasis on cyber resilience, cooperation, national capacity building and the interaction of cybersecurity actors as conditions of Ukraine's existence in the digital domain (President of Ukraine, 2021).

This national mandate bears only indirectly on higher education, since no specific sectoral regime exists. Under the Law of Ukraine on Higher Education, a higher education institution is a separate legal entity possessing institutional autonomy in educational, research, organisational, economic, and personnel matters (Verkhovna Rada of Ukraine, 2014). Universities therefore have the organisational freedom to formulate internal cybersecurity policies, roles, and responsibilities, to manage their infrastructure and to allocate resources. The coding did not, however, identify in the higher education legislation analysed any sector-wide cybersecurity governance framework that would impose a common set of cyber-resilience functions on university governing bodies, define cybersecurity leadership roles, or create a standardised higher education incident-governance mechanism.

The Law of Ukraine on Protection of Information in Information and Communication Systems operates at a different regulatory level. It provides the legal framework for protecting information processed in information and communication systems, and therefore imposes obligations wherever university systems process information protected by statutory requirements (Verkhovna Rada of Ukraine, 1994). The Law of Ukraine on Critical Infrastructure introduces a resilience-focused regime covering continuity, recoverability, integrity, and the protection of critical infrastructure; its requirements become institutionally determinative for a university only where the relevant infrastructure is identified and treated under the critical-infrastructure regime, and not simply because the organisation is a higher education institution (Verkhovna Rada of Ukraine, 2021).

The results of coding these instruments against the five predefined dimensions are summarised in Table 1.

Table 1. Legal and institutional coverage of cybersecurity governance dimensions in Ukrainian higher education

Governance dimension	Documentary finding in the Ukrainian framework	Degree of HEI-specific specification	Identified governance gap
Legal mandate	Cybersecurity, information protection, cyber resilience, and critical-infrastructure protection are regulated at national level	Partial	No dedicated cybersecurity governance regime for the higher education sector
Institutional responsibility	National cybersecurity actors and broad categories of responsible entities are legally identified	Partial	University governing bodies and cybersecurity leadership functions are not standardised sector-wide
Inter-organisational coordination	National coordination and incident-response architecture exists	Partial	No uniform HEI-specific coordination channel linking universities, education authorities, and national cyber actors was identified
University-level arrangements	HEIs possess organisational autonomy and may establish internal structures and policies	Indirect	Autonomy does not itself define minimum governance roles, reporting chains, or cyber-resilience functions
Cybersecurity and digital transformation	National strategy connects cybersecurity with secure digital development	Partial	Higher education digitalisation and cybersecurity governance remain institutionally separated across the analysed legal instruments

Note. HEI = higher education institution. „Partial" means that the relevant governance element is present in the broader legal framework but is not comprehensively specified for higher education as a sector. Source. Compiled by the author on the basis of Verkhovna Rada of Ukraine (1994, 2014, 2017, 2021) and President of Ukraine (2021).

The table shows that the central weakness is not the absence of cybersecurity legislation. Instead, the relevant mechanism is the explicit sectoral translation of national cybersecurity requirements to the autonomous governance structures of universities. The distinction matters, because the scientific literature consistently describes higher education as a hetero-

geneous environment of users, distributed information systems, open academic networks, research data, and varied institutional assets (Nashynets-Naumova et al., 2020; Merchan-Lima et al., 2021; Afolalu & Tsoeu, 2025). General organisational obligations therefore do not necessarily define how responsibility is allocated within a university.

4.2. Allocation of responsibility and inter-organisational coordination

The second dimension of the coding concerned the distribution of duties. Here the Ukrainian model proved relatively well developed at national level and less well defined at university level. The Law on the Basic Principles of Cybersecurity establishes a multi-actor framework that includes, within their respective areas of competence, the State Service of Special Communication and Information Protection, the National Police, the Security Service of Ukraine, defence and intelligence bodies, the National Bank, and the Ministry of Foreign Affairs, among others. It also provides for information sharing, incident response, preventive measures, training, cybersecurity audit, and public–private collaboration within the national system (Verkhovna Rada of Ukraine, 2017). The Cybersecurity Strategy echoes this network logic, conceptualising cyber resilience as the product of interaction among cybersecurity actors rather than of protection at the level of a single organisation (President of Ukraine, 2021).

At the level of the individual HEI, however, the documentary corpus does not disclose a comparable predefined chain of responsibility running from the rectorate or governing body to an accountable cybersecurity executive, an operational cybersecurity team, data and system owners, and users. The university autonomy provided for in the higher education law permits such arrangements but does not require them as a matter of cybersecurity governance (Verkhovna Rada of Ukraine, 2014). This produces a governance arrangement in which national accountability is relatively well specified while organisational translation continues to depend on institutional decisions.

The scientific evidence makes this gap all the more salient in practice. Reviews of information security management in higher education describe competence, resources, guidance, security frameworks, and implementation strategy as dynamically related rather than as isolated elements (Merchan-Lima et al., 2021). Recent reviews also show that fragmented security arrangements, low levels of awareness, insufficient training, poor incident reporting, and technical gaps are found even among digitally mature organisations (Afolalu & Tsoeu, 2025; Salam et al., 2026). Findings relating to universities in Ukraine likewise suggest that the way employees act and are trained in security remains a factor in protecting the institution's digital assets (Kobis et al., 2024). The evidence thus suggests that cyber resilience entails not simply a legal obligation to protect systems but also a specified organisational route through which that obligation is to be discharged.

The distinction is laid bare more clearly by the European comparison. Under the GDPR, liability lies with the controller, and technical and organisational measures must be proportional to the risk of processing; security is defined as including confidentiality, integrity, availability, resilience, the capacity for restoration and the periodic evaluation of measures (European Parliament & Council of the European Union, 2016). The relevance of this model

to the present comparison is not that the GDPR supplies a comprehensive cybersecurity framework for universities, but that it ties legal accountability to demonstrable organisational action.

NIS2 strengthens this governance logic further. It imposes on entities within its scope a duty to take appropriate and proportionate cybersecurity risk-management measures, and it locates accountability at management level. Member States may provide for the Directive to apply to education institutions, in particular those carrying out critical research activities (European Parliament & Council of the European Union, 2022); that possibility does not make every university an NIS2 entity. What it does show is a regulatory route by which higher education can be brought expressly within a national framework of cyber-risk governance, rather than addressed only in general terms.

4.3. University-level cybersecurity arrangements

The third dimension concerned the governance required within the university itself. Four functional requirements recurred across the scientific and institutional corpus: strategic cybersecurity leadership, risk and compliance management, incident response, and continuous competence development. The Ukrainian legal framework supports these functions but does not combine them into a standard HEI governance model.

The ENISA European Cybersecurity Skills Framework provides a useful organisational benchmark, because it converts cybersecurity from an abstract institutional obligation into professional functions that can be identified. Its twelve cybersecurity role profiles cover cybersecurity leadership, risk, incident response, architecture, implementation, auditing, threat intelligence, and other areas (European Union Agency for Cybersecurity, 2022). The CISO-level profile in particular links organisational cybersecurity with strategy, policy, senior-management involvement, information security management systems, reporting, external collaboration, resource allocation, resilience, and capacity building. For universities, this makes visible the governance difference between employing IT staff and establishing accountable cybersecurity functions.

The Cybersecurity Act adds a second dimension to this institutional benchmark. It does not seek to mandate the governance structure of universities, but defines the role of ENISA and establishes a European cybersecurity certification framework for ICT products, services and processes, with risk-based assurance levels and a common certification approach (European Parliament & Council of the European Union, 2019). For HEIs increasingly reliant on cloud services, digital learning platforms, identity services, research infrastructure, and externally provided ICT products, this adds a supply-side governance dimension absent from a narrow perimeter-protection model.

The current threat landscape further supports this wider institutional view. Phishing was the leading intrusion vector in the EU threat landscape analysed in ENISA's 2025 threat assessment, ransomware continued to be one of the most high-impact threats, and increasing reliance on digital dependencies amplified risk across interconnected digital ecosystems (European Union Agency for Cybersecurity, 2025). These findings align with evidence at HEI level showing continuing vulnerability to phishing, malware, weak credentials, software

vulnerabilities, intellectual property risk, low levels of awareness and poor incident practice (Afolalu & Tsoeu, 2025; Salam et al., 2026). The overall conclusion is that university cybersecurity governance must address people, organisational responsibility, systems, external providers, and response capacity. No single technical department, lacking institution-wide authority, can govern all five areas on its own.

4.4. Cybersecurity as a condition of sustainable digital transformation

The fourth and fifth coding dimensions converged on the relationship between cybersecurity and digital transformation. The Digital Education Action Plan treats successful digital transformation as dependent on infrastructure, institutional strategy, leadership, organisational capability, skills, safe environments, privacy, and cooperation among education providers, institutions, technology companies, and other relevant parties (European Commission, 2020). This contrasts with a model in which security is layered on once digital systems have been chosen and implemented.

The documentary comparison accordingly revealed a sequencing problem for Ukrainian HEIs. Decentralised digital innovation is underpinned by higher education autonomy, while cybersecurity legislation establishes a national architecture of protection duties and response. The documents analysed do not, however, merge these two governance routes into a single sector-specific cycle in which digitalisation decisions give rise to cybersecurity risk management, institutional liability, skills development, incident preparedness, supplier management, and a review-based management of these activities.

This distinction is summarised by comparing the Ukrainian architecture with selected EU and ENISA instruments. Table 2 reports the comparative outcome rather than legal equivalence between the two systems.

Table 2. Comparative governance assessment of Ukrainian HEIs against selected EU and ENISA benchmarks

Governance element	Ukrainian documentary position	Selected EU/ENISA benchmark	Comparative result
Management accountability	Broad organisational and statutory responsibility; no uniform HEI cybersecurity leadership model identified	GDPR accountability; NIS2 management-level responsibility for covered entities	Partial alignment
Risk-based security	Present through information protection, cybersecurity, and critical-infrastructure regimes	Explicit risk-based technical and organisational measures in GDPR and NIS2	Substantive basis exists, but HEI operationalisation is fragmented
Incident governance	National incident-response and coordination mechanisms exist	NIS2 formalises organisational risk management and incident reporting for entities within scope	National capacity stronger than HEI-specific procedural specification
Professional cybersecurity roles	Not standardised across HEIs by higher education legislation	ECSF defines interoperable cybersecurity role profiles and competences	Clear institutionalisation gap

Governance element	Ukrainian documentary position	Selected EU/ENISA benchmark	Comparative result
Secure digitalisation	Cybersecurity and higher education digitalisation are governed through separate legal and policy streams	Digital Education Action Plan integrates strategy, leadership, secure platforms, privacy, skills, and collaboration	Partial policy convergence, weak sectoral integration
ICT assurance and supply chain	General protection obligations apply; HEI-specific procurement assurance not identified in the analysed corpus	Cybersecurity Act provides EU-level certification architecture for ICT products, services, and processes	Comparative gap in explicit HEI-oriented assurance mechanisms
Higher education sector coverage	HEIs enter cybersecurity regulation primarily through general or conditional legal categories	NIS2 allows Member States to extend scope to education institutions, especially those conducting critical research	Sectoral coverage remains less explicit in Ukraine

Note. The EU instruments are used as comparative regulatory and policy benchmarks, not as evidence that every provision applies directly to every Ukrainian HEI. NIS2 coverage of educational institutions depends on the scope established by Member States and on other conditions of the Directive. Source. Compiled by the author on the basis of European Commission (2020), European Parliament and Council of the European Union (2016, 2019, 2022), European Union Agency for Cybersecurity (2022), Verkhovna Rada of Ukraine (1994, 2014, 2017, 2021), and President of Ukraine (2021).

4.5. Integrated governance finding

The final stage of interpretation produced a five-tier governance structure arising from the relationships identified rather than from any single determinant. At the first level, national cybersecurity policy defines strategic goals, baseline requirements, coordination, and response capability. At the second, sectoral governance should convert those general aims into requirements suited to the higher education context, including through differentiated treatment of institutions whose research, information resources, or infrastructure carry elevated risk. At the third, university governing bodies need to assign responsibility, approve cybersecurity policy and risk tolerance, endorse resource requirements, and embed cyber resilience in the institution's digital strategy. At the fourth tier, operational roles include information-security management, incident response, access and identity management, data protection, infrastructure and supplier risk, awareness, and continuity. The fifth tier is a continuous assurance loop drawing on incident data, risk reassessment, audits or evaluations, capability development, and the revision of organisational policy.

The coding matrix suggests that the components of this structure do exist in Ukraine, but in different legal and institutional layers. National coordination and cybersecurity policy are relatively clear; the protection of information systems is mandated by law; critical-infrastructure legislation imposes resilience-based obligations where applicable; and higher education law grants significant organisational freedom (Verkhovna Rada of Ukraine, 1994, 2014, 2017, 2021). It is the intermediate layer connecting the national system to the internal administration of an ordinary HEI that remains loosely institutionalised.

The main finding emerging from the doctrinal comparison is therefore one of institutional fragmentation rather than of regulatory absence. Ukrainian universities operate at the intersection of higher education autonomy, the demands of national cybersecurity gover-

nance, critical-infrastructure regulation where applicable, and expanding digital infrastructure provisions. The framework analysed does not, however, bring these elements together into a unified sectoral governance model that would specify at least minimum university-level cybersecurity duties, management accountability, professional functions, coordination channels, cyber-resilience planning, and integration with institutional digital-transformation strategies.

The EU comparison suggests that these gaps in connection need not be accepted as the price of university autonomy. The European instruments selected show, on the contrary, how decentralised organisational responsibility can be combined with risk-based accountability, management oversight, competence frameworks, secure digital platforms, certification schemes, and inter-institutional coordination (European Commission, 2020; European Parliament & Council of the European Union, 2016, 2019, 2022; European Union Agency for Cybersecurity, 2022). In the Ukrainian context, the governance arrangement to be built from these models is therefore not a parallel cybersecurity bureaucracy for the higher education sub-sector, but the formal linkage of the self-governing university to the wider national cybersecurity architecture through sector-specific minimum duties, interface specifications, and cyber-resilience standards.

5. Discussion

The main contribution of this paper is to show that the governance of cybersecurity in Ukrainian higher education is not so much unregulated between national higher education and cybersecurity policy as it is differentiated across levels — national policy, subsystems of higher education governance, and university-level institutional arrangements. Ukraine now possesses legal instruments for the protection of information, the coordination of cybersecurity, the resilience of critical infrastructure, and institutional autonomy. What remains missing or underdeveloped is the intermediate, or „meso", level of governance that translates these national requirements into a consistent and intelligible set of responsibilities for higher education institutions. That distinction is crucial, because it moves the policy challenge away from creating further cybersecurity rules and towards integrating the regulatory and organisational components that already exist.

This conclusion accords in general terms with research from other countries suggesting that weak cybersecurity on university campuses is not attributable solely to deficits in technical protection. Fragmented information security management and weak institutional cooperation were identified as problems facing higher education by Bongiovanni (2019). Merchan-Lima et al. (2021) proceed along the same lines, showing that universities adopt diverse security models and approaches to infrastructure and network management, as do Imbaquingo-Esparza et al. (2022), who find that growing reliance on digital technology increases organisation-level information security risk. The findings presented here develop these insights further by identifying fragmentation not only within the organisation of security in universities but also between that organisation and the broader public-governance framework.

This deficient division of labour in responsibilities is also consistent with the emphasis

on governance rather than control advanced by Kuerbis and Badiei (2017) and Savaş and Karataş (2022). Their work conceptualises cybersecurity as an emergent effect of interaction between hierarchical, networked and organisational structures, and therefore as a responsibility that cannot be located in a single public authority. The present results suggest that this is particularly true of Ukrainian higher education. National cyber bodies can offer strategic direction and incident-response capacity, but university autonomy means that operational responsibility remains decentralised. Autonomy is thus not incompatible with stronger cybersecurity governance; on the contrary, it increases the need for clear interfaces between public and institutional decision-making.

The contrast with Carmichael's (2026) study of Estonia further substantiates this reading. Estonia provides representative evidence that even the most „mature" digital states continue to renegotiate the distribution of cybersecurity responsibilities across institutions. Although Ukraine differs radically in institutional history and securitisation context, the comparison implies that mature cyber governance depends on continually clarifying the configuration of responsibilities rather than on fixing it. For Ukrainian HEIs, the open question is therefore not what responsibility to centralise, but which responsibilities are best institutionalised at university level and which are best addressed sectorally.

Two of the paper's principal findings concern the relationship between cybersecurity and digital transformation. The Ukrainian framework analysed here addresses the two spheres through somewhat divergent policy strands. This separation runs contrary to the change literature, which conceptualises organisational strategy, leadership, digital solutions, resources, organisational infrastructure and institutional culture as convergent constructs. Castro Benavides et al. (2020) argue that digital transformation in higher education demands an institution-level approach, and Fernández et al. (2023) hold that transformation succeeds when it is approached from the technological, organisational, process and human levels. Farias-Gaytan et al. (2023) support this line by connecting digital transformation with institutional capacities and digital literacy. The present findings indicate that cybersecurity might better be viewed as a further cross-cutting aspect of this transformation than as a technical exercise carried out after digital systems have been deployed.

This understanding is confirmed, significantly, by studies of barriers to digital transformation. Gkrimpizi et al. (2023) differentiate barriers that are strategic, organisational, technological, cultural and human, and Singun (2025) highlights the relevance of leadership, resources, competences, stakeholder management, and institutional culture. The governance gaps identified in this study are precisely of that kind. A university may possess technically adequate security tools and yet remain institutionally vulnerable if its policies on accountability, competence, supplier governance, incident escalation and continuity are unclear.

The Ukrainian evidence also partially corresponds with Nashynets-Naumova et al. (2020), who identify technological and organisational solutions to information and cybersecurity problems in Ukrainian HEIs, and with Kobis et al. (2024), whose comparative evidence underlines the importance of employee practice and security training. The present analysis nevertheless shows that competence building is not sufficient on its own. The organisational benefit of training depends on whether cybersecurity roles and chains of responsibility are institutionally defined. This finding is consistent with Nuñez et al. (2023), who show the

necessity of integrating technical tools, organisational controls, standards, and institutional practice.

Finally, the relationship between cybersecurity governance and institutional resilience is consistent with Othman (2023), for whom the risk of cyberattack has consequences for the long-term viability of higher education institutions. The present study extends that conclusion: sustainability depends not only on an institution's capacity to respond to individual incidents, but also on embedding cyber resilience in the governance of digital transformation. The continued prevalence of phishing, malware, credential compromise, vulnerabilities, and human-factor risk in HEIs is documented by Afolalu and Tsoeu (2025) and Salam et al. (2026). The present findings help explain why these threats call for governance responses covering management accountability, professional competence, coordination, suppliers, continuity, and institutional learning.

The study is limited by its documentary character. It identifies formal responsibilities and governance structures but cannot determine how reliably they are carried out in individual Ukrainian universities. Future research should therefore investigate the institutional cybersecurity policies, organisational structures, incident-response procedures, staffing models, and governance practices of a range of Ukrainian HEIs. The present findings nevertheless provide a foundation for that inquiry: improving cybersecurity in Ukrainian higher education does not require a parallel regulatory framework, but a sector-specific governance layer that bridges the gap between the national cybersecurity architecture and autonomous university management, alongside sustainable digital transformation.

6. Conclusions

The research has shown that the governance of cybersecurity in Ukrainian higher education rests on a robust national legal and strategic framework, but that this framework is not yet sufficiently elaborated in a sector-specific model for HEIs. Analysis of the 30-document corpus revealed that legal obligations concerning cybersecurity, information protection, critical infrastructure, organisational autonomy, and digital maturity are dispersed across different layers of regulation and institution. The principal weakness is therefore not regulatory absence but the weak coordination between national-level cybersecurity governance and university-level responsibility.

Five aspects of governance were examined: legal mandate, institutional responsibility, inter-organisational coordination, university-level cybersecurity provision, and the integration of cybersecurity into sustainable digital transformation. The analysis indicated that, although national-level guidance is comparatively strong, there is only partial definition of what cybersecurity leadership, accountability structures, incident involvement, professional functions, and sector-wide resilience requirements should look like for higher education.

An implication for practice is that Ukraine does not need a separate parallel cybersecurity system for universities. A more adequate way forward would be to create a sectoral governance layer connecting autonomous university governance with the national cybersecurity architecture. This should include a minimum institutional duty of care, management accountability, coordination mechanisms, competence requirements, cyber-resilience plan-

ning, and the embedding of cybersecurity within digital-transformation strategies.

As documentary research, this study cannot trace how formal requirements are executed, how policies influence practice in particular universities, or how effective institutionalised practices prove in operation. Comparative studies of cybersecurity governance across different types of Ukrainian HEI should be developed to examine their internal policies, incident-response capabilities, staffing, competence, supplier-risk management, and continuity mechanisms. Empirical substantiation would move the governance logic proposed here towards a practical sectoral model for sustainable and secure digital transformation.

Two implications follow for regulatory practice, and they are the reason the analysis belongs to the study of law, digital technologies and sustainable governance rather than to information security alone. First, the instrument that will determine whether a Ukrainian university actually governs its cyber risk is not the national statute but the subordinate sectoral rule that has not yet been made. For as long as the connection between the national cybersecurity architecture and autonomous institutional governance is left to each university to devise for itself, the standard achieved will track institutional capacity rather than legal obligation. Regulators and education authorities should therefore attend to the design of that intermediate layer, and not only to the adequacy of the primary legislation. Second, sectoral coordination of this kind is a condition of sustainability and not only of security: where digitalisation decisions are taken without a defined route to responsibility, competence and continuity, the digital capacity that results is not durable. On this reading, the task facing Ukrainian higher education is less the enactment of new cybersecurity norms than the institutional translation of the norms that already exist.

Funding Statement

This research received no external funding.

Conflicts of Interest

The author declares no conflicts of interest.

Ethical Approval Statement

This study was conducted as a documentary analysis of publicly available legal, strategic, policy and scholarly sources. There were no human subjects, surveys, experiments, interventions, or personal information. Formal ethics committee approval was therefore not required.

References

Afolalu, O., & Tsoeu, M. S. (2025). Cybersecurity in higher education institutions: A systematic review of emerging trends, challenges and solutions. Future Internet, 17(12), Article 575. https://doi.org/10.3390/fi17120575

Bongiovanni, I. (2019). The least secure places in the universe? A systematic literature review on informa-

tion security management in higher education. Computers & Security, 86, 350–357. https://doi.org/10.1016/j.cose.2019.07.003

Boutemeur, J., Lella, I., Bakatsis, I., Chatzichristos, G., Foley, K., Leskinen, J., Otcenasek, J., & Ziolek, D. (2025). ENISA threat landscape 2025. European Union Agency for Cybersecurity. https://doi.org/10.2824/1946374

Carmichael, L. (2026). Crafting a cybersecurity governance ecosystem: Two decades of learning in Estonia. European Policy Analysis, 12(2), Article e70017. https://doi.org/10.1002/epa2.70017

Castro Benavides, L. M., Tamayo Arias, J. A., Arango Serna, M. D., Branch Bedoya, J. W., & Burgos, D. (2020). Digital transformation in higher education institutions: A systematic literature review. Sensors, 20(11), Article 3291. https://doi.org/10.3390/s20113291

Chornomydz, A. V. (2025). Faculty information security in higher education institutions amidst martial law: Challenges and practical guidelines. Medical Education, (2), 67–71. https://doi.org/10.11603/m.2414-5998.2025.2.15490

Cotta, B., & Righettini, M. S. (2026). Governing cybersecurity in the digital age: Mapping comprehensive policy mixes with the Nodality-Authority-Treasure-Organization lens. Review of Policy Research, 43(4), Article e70113. https://doi.org/10.1111/ropr.70113

European Commission. (2020). Digital Education Action Plan 2021–2027: Resetting education and training for the digital age (COM(2020) 624 final). https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52020DC0624

European Parliament & Council of the European Union. (2016). Regulation (EU) 2016/679 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, L 119, 1–88. https://eur-lex.europa.eu/eli/reg/2016/679/oj

European Parliament & Council of the European Union. (2019). Regulation (EU) 2019/881 of 17 April 2019 on ENISA and on information and communications technology cybersecurity certification and repealing Regulation (EU) No 526/2013 (Cybersecurity Act). Official Journal of the European Union, L 151, 15–69. https://eur-lex.europa.eu/eli/reg/2019/881/oj

European Parliament & Council of the European Union. (2022). Directive (EU) 2022/2555 of 14 December 2022 on measures for a high common level of cybersecurity across the Union, amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972, and repealing Directive (EU) 2016/1148 (NIS 2 Directive). Official Journal of the European Union, L 333, 80–152. https://eur-lex.europa.eu/eli/dir/2022/2555/oj

European Union Agency for Cybersecurity. (2022). European Cybersecurity Skills Framework (ECSF). https://doi.org/10.2824/859537

Farias-Gaytan, S., Aguaded, I., & Ramirez-Montoya, M.-S. (2023). Digital transformation and digital literacy in the context of complexity within higher education institutions: A systematic literature review. Humanities and Social Sciences Communications, 10, Article 386. https://doi.org/10.1057/s41599-023-01875-9

Fernández, A., Gómez, B., Binjaku, K., & Meçe, E. K. (2023). Digital transformation initiatives in higher education institutions: A multivocal literature review. Education and Information Technologies, 28(10), 12351–12382. https://doi.org/10.1007/s10639-022-11544-0

Gkrimpizi, T., Peristeras, V., & Magnisalis, I. (2023). Classification of barriers to digital transformation in higher education institutions: Systematic literature review. Education Sciences, 13(7), Article 746. https://doi.org/10.3390/educsci13070746

Imbaquingo-Esparza, D., Díaz, J., Ron Egas, M., Fuertes, W., & Molina, D. (2022). Information security at higher education institutions: A systematic literature review. In J. Herrera-Tapia, G. Rodriguez-Morales, E. R. Fonseca C., & S. Berrezueta-Guzman (Eds.), Information and communication technologies: 10th Ecuadorian Conference, TICEC 2022, Manta, Ecuador, October 12–14, 2022, proceedings (pp. 294–309). Springer.

https://doi.org/10.1007/978-3-031-18272-3_20
Kobis, P., Kisiołek, A., Karyy, O., Pawliczek, A., & Chmielarz, G. (2024). Selected aspects of information security in e-marketing activities of higher education institutions in Poland, Ukraine and the Czech Republic. Procedia Computer Science, 246, 4617–4626. https://doi.org/10.1016/j.procs.2024.09.326
Kuerbis, B., & Badiei, F. (2017). Mapping the cybersecurity institutional landscape. Digital Policy, Regulation and Governance, 19(6), 466–492. https://doi.org/10.1108/DPRG-05-2017-0024
Merchan-Lima, J., Astudillo-Salinas, F., Tello-Oquendo, L., Sanchez, F., Lopez-Fonseca, G., & Quiroz, D. (2021). Information security management frameworks and strategies in higher education institutions: A systematic review. Annals of Telecommunications, 76(3–4), 255–270. https://doi.org/10.1007/s12243-020-00783-2
Nashynets-Naumova, A. Y., Buriachok, V. L., Korshun, N. V., Zhyltsov, O. B., Skladannyi, P. M., & Kuzmenko, L. V. (2020). Technology for information and cyber security in higher education institutions of Ukraine. Information Technologies and Learning Tools, 77(3), 337–354. https://doi.org/10.33407/itlt.v77i3.3424
Nuñez, M., Palmer, X.-L., Potter, L., Aliac, C. J., & Velasco, L. C. (2023). ICT security tools and techniques among higher education institutions: A critical review. International Journal of Emerging Technologies in Learning, 18(15), 4–22. https://doi.org/10.3991/ijet.v18i15.40673
Othman, Z. (2023). Sustainability of higher education institutions: Case study on cyber attacks. Global Business Management Review, 15(1), 24–38. https://doi.org/10.32890/gbmr2023.15.1.2
President of Ukraine. (2021, August 26). Decree No. 447/2021 on the decision of the National Security and Defense Council of Ukraine of 14 May 2021 „On the Cybersecurity Strategy of Ukraine". https://zakon.rada.gov.ua/laws/show/447/2021
Salam, M., Abu Bakar, K. A., Abdul Ghani, A. T., & Mohd Aman, A. H. (2026). Cybersecurity in higher education institutions digitalisation: Addressing threats and vulnerabilities. SAGE Open, 16(1). https://doi.org/10.1177/21582440251413473
Savaş, S., & Karataş, S. (2022). Cyber governance studies in ensuring cybersecurity: An overview of cybersecurity governance. International Cybersecurity Law Review, 3(1), 7–34. https://doi.org/10.1365/s43439-021-00045-4
Singun, A. (2025). Unveiling the barriers to digital transformation in higher education institutions: A systematic literature review. Discover Education, 4, Article 37. https://doi.org/10.1007/s44217-025-00430-9
Verkhovna Rada of Ukraine. (1994, July 5). Law of Ukraine No. 80/94-VR on protection of information in information and communication systems [as amended]. https://zakon.rada.gov.ua/laws/show/80/94-%D0%B2%D1%80
Verkhovna Rada of Ukraine. (2014, July 1). Law of Ukraine No. 1556-VII on higher education [as amended]. https://zakon.rada.gov.ua/laws/show/1556-18
Verkhovna Rada of Ukraine. (2017, October 5). Law of Ukraine No. 2163-VIII on the basic principles of cybersecurity in Ukraine [as amended]. https://zakon.rada.gov.ua/laws/show/2163-19
Verkhovna Rada of Ukraine. (2021, November 16). Law of Ukraine No. 1882-IX on critical infrastructure [as amended]. https://zakon.rada.gov.ua/laws/show/1882-20

ABOUT THE SERIES

ESS Conference Series: Social Science and Humanities is a peer-reviewed open access proceedings series published by ESS Press (Warsaw, Poland) within the E-Science Space ecosystem. The series publishes papers presented at international conference and internship programmes organised together with partner universities and research institutions.

SUBMISSIONS

Manuscripts and proposals are accepted through the journal platform at https://csssh.ess.press. Editorial contact: info@ess.press.

FORTHCOMING EVENTS

PILC & SEITE Conference 2026 "Human-centric Leadership: Talent, Technology, and Brand Power", 23 September – 1 October 2026, Rijeka and Poreč, Croatia. Organised by PAR University of Applied Sciences (Croatia), E-Science Space (Poland) and the Center for Strategic Innovations and Progressive Development (Ukraine).

ESS Conference Series
SOCIAL SCIENCE AND HUMANITIES

Volume 1 · Issue 1 · 2026
Varna, Bulgaria
Publisher: ESS Press, Warsaw, Poland
info@ess.press · https://csssh.ess.press

Printed by ESS Press, 2026