AI-Assisted Legislative Analysis: A Framework for Identifying Terminological Inconsistencies in Information and Cybersecurity*

Olha Kovalchuk[1,*,†], Nadiya Khoma[1,†], Keteryna Verbitska[1,2,†], Anhelina Banakh[1,3,†], Roman Ivanytskyy[1,4,†] and Ludmila Babala[1,†]

[1] West Ukrainian National University, 11 Lvivska Str., Ternopil, 46009, Ukraine
[2] Ukrainian Catholic University, 17 Ilariona Svjentsits'koho Str., L'viv, 79000, Ukraine
[3] Erasmus Universiteit Rotterdam, 50 Burgemeester Oudlaan, Rotterdam, 3062 PA, Netherlands
[4] Ternopil Volodymyr Hnatiuk National Pedagogical University, 2 Maksym Kryvonos Str., Ternopil, 46027, Ukraine

Abstract

Terminological consistency of legislation constitutes a fundamental prerequisite for legal certainty, particularly within information security and cybersecurity areas that experience swift technological progress. Traditional manual legislative analysis proves insufficient in contexts of high frequency of legislative amendments. This study presents a new approach to methodology for detecting terminological inconsistencies through the application of artificial intelligence (AI), specifically the large language model (LLM) Claude Sonnet 4.5. The methodology encompasses four sequential stages: formulation of structured queries for the identification of legislative acts, AI-assisted terminology analysis, verification of results against the official legislative database of Ukraine, and comparative analysis of identified inconsistencies. The study focuses on three key terms: "information", "cybersecurity", and "cyberdefense", The results revealed five types of terminological inconsistencies: temporal discrepancy between "old" and "new" terminology, fragmentation of definitions, monopolization of definition by a single legislative act, conceptual inconsistency of related concepts, and absence of clear delineation between "cyberdefense" and "information protection." Verification through the Official Portal of the Verkhovna Rada confirmed the correctness of the AI analysis. The proposed methodology demonstrates the capacity to rapidly identify relevant legislative acts, systematize term definitions, detect structural inconsistencies, and classify types of terminological problems. The study confirms the practical value of the AI-assisted approach for legislative analysis, ensuring methodological scalability and the possibility of iterative application for monitoring the terminological consistency of legislation.

Keywords

Artificial intelligence, legislative analysis, terminological consistency, cybersecurity, large language models, natural language processing, Ukrainian legislation

1. Introduction

Artificial intelligence (AI) is transforming the legal domain, demonstrating significant achievements in solving complex legal tasks. Large language models (LLMs) have shown the ability to analyze legal texts, identify contradictions in legislation, and automate routine legal processes [1]. Contemporary AI systems can achieve accuracy comparable to expert lawyers in tasks of legal document classification and prediction of judicial decisions [2, 3]. The application of natural language processing technologies to legislative analysis enables the automation of terminological inconsistency detection, which traditionally required substantial human resources [4].

* The Third International Conference of Young Scientists on Artificial Intelligence for Sustainable Development: Intelligent Systems and Artificial Intelligence (YAISD-WS 2026:ISAI) May 7-8, 2026, Ternopil, Ukraine
1,* Corresponding author.
† These authors contributed equally.
o.kovalchuk@wunu.edu.ua (O. Kovalchuk); n.khoma@wunu.edu.ua (N. Khoma); katya.verbitska146@gmail.com (K. Verbitska); a.banakh@st.wunu.edu.ua (A. Banakh); ivanytskyiroman@tnpu.edu.ua (R. Ivanytskyy); ludaduma7@gmail.com (L. Babala);
0000-0001-6490-9633 (O. Kovalchuk); 0000-0003-2981-0296 (N. Khoma); 0009-0006-0698-9448 (K. Verbitska); 0009-0003-2995-4203 (A. Banakh); 0009-0004-1687-9539 (R. Ivanytskyy); 0000-0002-2388-270X (L. Babala)
© 2026 Copyright for this paper by its authors. Use permitted under Creative Commons License Attribution 4.0 International (CC BY 4.0).

CEUR Workshop Proceedings ceur-ws.org ISSN 1613-0073
published 2026-11-11

CEUR-WS.org/Vol-4326/short15.pdf

Terminological consistency of legislative systems constitutes a fundamental prerequisite for ensuring legal certainty and effective law enforcement [5]. In the domain of information and cybersecurity (fields characterized by rapid technological evolution), the precision and harmonization of legal terminology acquire particular significance. Ukraine faces challenges in maintaining terminological coherence within the continuously expanding legislative corpus of cybersecurity. The terminological apparatus in this domain directly affects the implementation of Sustainable Development Goal 16 (Peace, Justice and Strong Institutions), as legislative clarity constitutes the foundation for institutional effectiveness and the rule of law [6].

Cross-border evidence shows accelerated integration of AI into parliamentary work [7]. The European Union (EU) is implementing projects using AI to identify contradictions between the national legislation of member states and EU directives [8]. NIST published comprehensive framework guidance on AI applications in legal analysis, including automated contradiction detection in federal regulatory acts [9]. Singapore has introduced the Legal Technology Vision, which uses natural language processing to analyze legislative bills for terminological consistency [10]. Estonia applies AI tools for automatic verification of regulatory acts for consistency with the existing legal framework [5].

The Ukrainian language remains relatively low-resource in terms of natural language processing tools [11]. The volatility of Ukraine's legislative environment creates additional methodological challenges. During 2020–2024, more than 15 normative legal acts in the field of cybersecurity were adopted [5, 12]. Traditional manual legislative analysis proves insufficient in contexts of high frequency of legislative amendments [13]. The methodology proposed in this study offers potential for iterative application and continuous monitoring of terminological consistency

This study examines the application of the LLM Claude Sonnet 4.5 for detecting and analyzing terminological inconsistencies in Ukrainian legislation in the domain of information and cybersecurity, focusing on three terms: "information", "cybersecurity", and "cyberdefense." Through systematic AI-assisted analysis combined with verification against official legislative databases, the study demonstrates the potential and limitations of AI tools in legislative analysis.

2. Related works

Recent years have witnessed a surge in research on AI methods applied to automating legal analysis and processing legal documents. D.M. Katz et al. demonstrated that GPT-4 successfully passes the Uniform Bar Examination in the United States, achieving scores significantly exceeding the passing threshold and demonstrating marked advancement from prior model versions [1]. L. Zheng et al. developed a methodology for evaluating chat assistants based on LLMs, using the concept of 'LLM-as-a-judge', where powerful models serve as evaluators of other systems. The authors created MT-bench (a set of multi-turn questions) and Chatbot Arena (a crowdsourcing platform for comparing models), achieving over 80% agreement with human preferences [2]. I. Chalkidis et al. developed the specialized language model LEGAL-BERT for English-language legal texts, trained on legal corpora from EU legislation, UK legislation, US contracts, and court cases [14]. In [15], a multinational English-language legal corpus, LeXFiles, with a volume of over 620,000 documents from 6 legal systems (EU, India, UK, USA, Canada), and the LegalLAMA benchmark for evaluating legal knowledge of PLMs are presented. J. Savelka and K.D. Ashley demonstrated the effectiveness of large language models GPT-4 and GPT-3.5-turbo in zero-shot semantic annotation of legal texts, including judicial decisions, contractual provisions, and legislative acts, achieving results comparable to specialized legal systems [16].

The problem of multilinguality and multi-jurisdictionality in legal NLP has been actively researched in recent years. V. Niklaus et al. created MultiLegalPile, a large-scale multilingual legal corpus with a volume of 689 GB, covering 24 languages from 17 jurisdictions, and trained on it a series of RoBERTa and Longformer models that achieved new state-of-the-art on the LEXTREME benchmark [17]. Research on legal systems for low-resource languages remains limited. Thus, P.

Joshi et al. classified the world's languages by resource level (classes 0–5), assigning Ukrainian to class 3 with limited availability of labeled datasets for the legal domain [18]. H. Muradyan et al. conducted a comprehensive review of challenges and achievements in NLP with a focus on legal informatics and low-resource languages, emphasizing the slow implementation of modern technologies in the legal domain, especially for languages with limited resources [19]. D. Chaplynskyi resented the UberText 2.0 corpus, a large-scale collection of contemporary Ukrainian language with a volume of 3.274 billion tokens [20]. However, specialized resources for the legal domain of the Ukrainian language remain absent. A methodology for AI-assisted legislative analysis in scenarios involving linguistically under-resourced contexts, particularly Ukrainian, has not been developed to date. Moreover, there is a lack of empirical studies on the application of LLMs for detecting terminological inconsistencies in cybersecurity legislation. Scalable frameworks combining AI analysis with verification of results against official legislative databases have also not been developed. The current study fills these gaps through the creation and validation of a novel methodological approach for AI-assisted analysis of terminological inconsistencies in Ukrainian legislation in the domain of information and cybersecurity.

3. Methodology

The study employed a comprehensive methodological framework that combined several approaches, scholarly literature analysis, systematic evaluation of statutes, and the recommended approach of AI tools for detecting and analyzing terminological inconsistencies in Ukrainian legislation. Ukrainian legislation functions as a complex system of interconnected normative legal acts, in which terminological consistency is key to ensuring legal certainty and proper law enforcement. Inconsistencies in the terminology application and interpretation throughout various statutory documents may result in legal conflicts, erroneous interpretations, and ineffective implementation of legal norms. Traditional manual analysis of legislative terminology is a labor-intensive process requiring constant monitoring of legislative changes, which occur quite frequently in the conditions of Ukraine’s dynamic legal environment. This study utilized the LLM Claude Sonnet 4.5 (model identifier: claude-sonnet-4-5-20250929), developed by Anthropic, accessed through the web interface claude.ai. The study was conducted in February 2026.

3.1. Methodological Approach

The methodological approach consisted of four sequential stages:
Stage 1: Formulation of structured queries. A series of four structured queries was developed, each directed at performing a specific analytical task. Queries 1–3 focused on identifying legislative acts featuring descriptions of or citations to the terms "informatio", "cybersecurity", and "cyberdefense", respectively. Each query included: (a) identification of relevant legislative acts with specification of their full titles and particulars; (b) extraction of precise definitions where available; (c) contextual analysis of the term's usage; (d) indication of articles or sections containing the respective term.
Content of structured queries:
Query 1: "Analyze Ukrainian legislation and identify all legislative acts that contain a definition of the concept 'information' or where this concept is used in a key context. For each identified act, provide: the full title of the legislative act and its particulars; an exact quotation of the term's definition (if provided); the context of the term’s usage (if a definition is absent); the article/section where the definition or reference is contained. Structure the results in table format".
Query 2: "Analyze Ukrainian legislation and identify all legislative acts that contain a definition of the concept “cybersecurity" or where this concept is used in a normative context. For each identified act, provide: the full title of the legislative act and its particulars; an exact quotation of the term’s definition (if provided); the context of the term's usage (if a definition is absent); the article/section where the definition or reference is contained; the relationship with other terms (cyberdefense, information security). Structure the results in table format".

Query 3: "Analyze Ukrainian legislation and identify all legislative acts that contain a definition of the concept “cyberdefense” or where this concept is used in a normative context. For each identified act, provide: the full title of the legislative act and its particulars; an exact quotation of the term’s definition (if provided); the context of the term’s usage (if a definition is absent); the article/section where the definition or reference is contained; the relationship with the terms “cybersecurity” and “information protection”. Structure the results in table format".
Query 4: "Based on the obtained data regarding definitions of the terms “information”, “cybersecurity”, and “cyberdefense” in various legislative acts of Ukraine, conduct a comparative analysis and systematize the identified inconsistencies according to the following categories: discrepancies in definitions of one term across different laws; contradictions between definitions of interrelated terms; cases of term usage without definition; hierarchical conflicts between legislative acts; temporal discrepancies (outdated definitions). For each inconsistency, indicate: the nature of the problem and the legislative acts between which the conflict arises".
Stage 2: Analysis using AI. The queries were executed sequentially using the Claude Sonnet 4.5 model. For each term, the model processed its knowledge base to identify relevant normative legal acts of Ukraine, extract definitions, and record the context of term usage. The obtained results were structured in tabular format to ensure systematic comparison.
Stage 3: Verification. All results obtained from the analysis using AI were verified against the Official Portal of the Verkhovna Rada of Ukraine, the official database of Ukrainian legislation. Verification included: (a) confirmation of the presence of identified legislative acts; (b) verification of the correctness of definition citations; (c) verification of current versions of normative legal acts; (d) confirmation of references to specific articles and sections.
Following technical verification, the authors, with expertise in Ukrainian law, conducted a legal qualification of the identified inconsistencies [21]. Each AI-detected discrepancy was assessed for its legal significance in terms of its potential impact on legal certainty and law enforcement in the domain of information and cybersecurity. In cases where the AI-generated output did not correspond to the current wording of legislative acts as established through the Official Portal of the Verkhovna Rada of Ukraine, the relevant results were excluded from the analysis.
Stage 4: Comparative analysis. Using Query 4, a systematization of identified inconsistencies between term definitions across different legislative acts was conducted. The analysis focused on: (a) discrepancies in definitions of identical terms; (b) contradictions between definitions of interrelated terms; (c) cases of term usage without providing a definition; (d) hierarchical conflicts between legislative acts; (e) temporal discrepancies (outdated definitions).

3.2. Methodological limitations

Key restrictions in this investigation merit recognition. First, Claude does not have direct access to the complete database of Ukrainian legislation and relies on knowledge acquired during prior training, with a knowledge cutoff date of January 2026. Accordingly, the model may not contain information about the most recent legislative changes or certain normative legal acts. Second, Claude is a natural language processing tool, not a specialized legal system; its outcomes demand confirmation from subject-matter experts in jurisprudence. Third, the AI model cannot guarantee completeness of coverage, particularly in cases of terminology usage in non-standard contexts or specific formulations. In view of this, the verification stage was necessary to ensure the reliability and validity of the research results.

3.3. The proposed approach

While Section 3.1 describes the procedural implementation of the methodology as applied in the present study, this section presents the approach as a generalizable framework intended for replication and adaptation in future legislative analysis research.

This study proposes a novel methodology for identifying and analyzing terminological inconsistencies in Ukrainian legislation using an AI tool – the LLM Claude Sonnet 4.5 (Fig. 1).

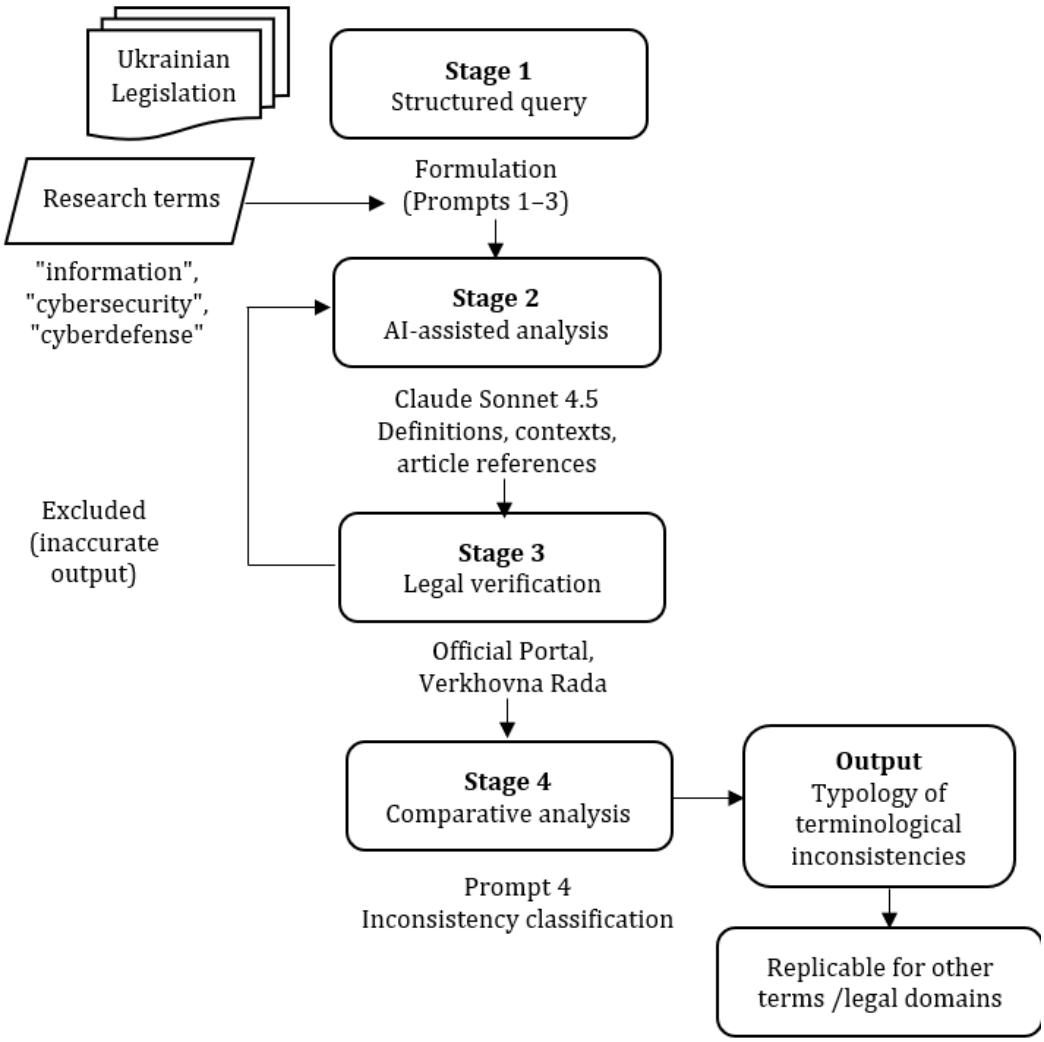


Figure 1: Flow chart of the proposed approach for identifying legislative inconsistencies using AI.

AI-assisted analysis is conducted sequentially through four structured prompts. Based on the model's knowledge base regarding Ukrainian legislation, a systematic processing of normative legal acts is performed to identify: definitions of the terms "information", "cybersecurity", and "cyberdefense"; contexts in which these terms are applied; as well as inconsistencies between definitions across different normative legal acts.

The LLM Claude Sonnet 4.5 is used to process the texts of legislative acts and extract relevant terminological information. The proposed approach enables systematic identification and classification of terminological inconsistencies across a substantial body of legislative acts, with results subject to mandatory verification against the Official Portal of the Verkhovna Rada of Ukraine. The proposed methodology represents an original combination of LLM-assisted structured querying, legal expert verification, and systematic inconsistency classification, applied for the first time to the terminological analysis of Ukrainian cybersecurity legislation as a low-resource language legal domain.

4. Results and discussion

Application of the proposed AI analysis methodology to Ukrainian legislation enabled the systematization of the terminological apparatus in the field of information and cybersecurity and revealed a number of significant inconsistencies. Using the Claude Sonnet 4.5 model, a sequential

analysis of three key terms ("information", "cybersecurity", and "cyberdefense") was conducted, which serve a fundamental function in the legal regulation of relevant social relations.

4.1. Results of identification and analysis of the term "information"

At the first stage, the model identified eight principal legislative acts of Ukraine that contain definitions or use the term "information" in a key context. The AI analysis revealed that five of these acts contain their own definitions of the term, while three legislative acts use this concept without a separate definition (Table 1).

Table 1
Identified legislative acts with a definition of the term "information"

Legislative act	Definition of the term	Article of Law	Source
Law of Ukraine "On Information"	"Information is any data and/or information that can be stored on material media or displayed in electronic form"	Article 1	[22]
Law of Ukraine "On Protection of Personal Data"	Uses the concept "information" in the context of personal data, but does not contain a separate definition. Relies on the definition from the basic law	Article 2	[23]
Law of Ukraine "On Access to Public Information"	"Information is any data and/or information that can be stored on material media or displayed in electronic form"	Article 1	[24]
Law of Ukraine "On Protection of Information in Information and Telecommunication Systems"	"Information is data or information that can be stored on material media or displayed in electronic form"	Article 1	[25]
Civil Code of Ukraine	"Information is any data and/or information that can be stored on material media or displayed in electronic form"	Article 200	[26]

Note: The presented results are based on the model's knowledge as of January 2026. For final verification, it is necessary to cross-reference these data with current versions of legislative acts on the Official Portal of the Verkhovna Rada of Ukraine.

The model identified a notable characteristic: the basic definition introduced by the Law "On Information" in 1992 was reproduced almost unchanged in other normative legal acts over nearly 30 years. Comparative analysis of the definitions enabled the systematization of four key characteristics of the legislative approach to the concept "information" (Table 2).

Table 2
Characteristics of the definition of the term "information" in Ukrainian legislation

Characteristic	Description
Unification of definition	In most legislative acts, an identical or nearly identical definition of the term "information" as "any data and/or information" is used
Dual form of existence	The definition emphasizes two forms of information existence –material (media) and electronic
Absence of substantive characterization	The definition is formal and does not reveal the substantive characteristics of information (reliability, timeliness, completeness, etc.)
Temporal stability	Despite a 30-year difference between the adoption of different laws (1992–2011), the definition remains stable

These characteristics demonstrate a high level of terminological consistency for the basic concept, which is a positive factor for law enforcement; however, the formality of the definition may create difficulties in specific contexts.

4.2. Results of identification and analysis of the term "cybersecurity"

At the second stage, the AI model identified four principal legislative acts that contain definitions or use the term "cybersecurity." Unlike the term "information", the concept "cybersecurity" has a significantly shorter normative history: it appeared in Ukrainian legislation only in 2016–2017.

Table 3
Identified legislative acts with a definition of the term "cybersecurity"

Legislative act	Presence of definition / Context of usage	Article of Law	Source
Law of Ukraine "On Basic Principles of Ensuring Cybersecurity of Ukraine"	"Cybersecurity is the protection of vital interests of individuals and citizens, society and the state during the use of cyberspace, whereby sustainable development of the information society and digital communication environment is ensured, and real and potential threats to the national security of Ukraine in cyberspace are timely detected, prevented and neutralized"	Article 1	[27]
Law of Ukraine "On National Security of Ukraine"	Does not contain a separate definition of "cybersecurity", but defines cybersecurity as a component of national security in the list of principal directions of state policy	Article 1	[28]
Cybersecurity Strategy of Ukraine	Uses the definition according to which cybersecurity encompasses issues of security in cyberspace, including the protection of critical information infrastructure	Section 1	[29]
Law of Ukraine "On Critical Infrastructure"	Uses the term "cybersecurity" without a separate definition, referring to the Law of Ukraine "On Basic Principles of Ensuring Cybersecurity of Ukraine"	Article 1	[30]

The analysis revealed that the Law of Ukraine "On Basic Principles of Ensuring Cybersecurity of Ukraine" [27] established the basic definition to which other normative acts refer. At the same time, numerous legislative documents, including resolutions of the Cabinet of Ministers of Ukraine from 2021 to 2024, use this term without a clear definition, which creates potential risks for law enforcement.

Comparative analysis enabled the identification of four key characteristics of the definition of the term "cybersecurity" (Table 4).

Table 4
Characteristics of the definition of the term "cybersecurity" in Ukrainian legislation

Characteristic	Description	Source
Dominant source of definition	The Law of Ukraine "On Basic Principles of Ensuring Cybersecurity of Ukraine" is the principal normative legal act that establishes the definition of the term "cybersecurity"	[27]

Broad approach to definition	The Law of Ukraine "On Basic Principles of Ensuring Cybersecurity of Ukraine" is the principal normative legal act that establishes the definition of the term "cybersecurity"	[27]
Absence of unification	In earlier legislative acts (before 2017), the term is absent, which creates certain terminological discrepancies between "old" and "new" legislation	[28]
Cross-sectoral character	The term is used in legislation of various sectors (national security, telecommunications, critical infrastructure), but always with reference to the basic definition	[27], [29]

4.3. Results of identification and analysis of the term "cybersecurity"

At the third stage, the model identified that the term "cyberdefense" has the narrowest normative base among the studied terms. The only comprehensive definition is contained in the Law of Ukraine "On Basic Principles of Ensuring Cybersecurity of Ukraine": "Cyberdefense is a set of organizational, organizational-technical measures aimed at ensuring cybersecurity, countering cyberattacks, and eliminating their consequences" [26].

Table 5
Identified legislative acts with definition of the term "cyberdefense"

Legislative act	Presence of definition / Context of usage	Article of Law	Source
Law of Ukraine "On Basic Principles of Ensuring Cybersecurity of Ukraine"	"Cyberdefense is a set of organizational, organizational-technical measures aimed at ensuring cybersecurity, countering cyberattacks, and eliminating their consequences"	Article 1	[27]
Law of Ukraine "On Critical Infrastructure"	Definition is absent, uses the term in the context of protection of objects	Articles 6, 11	[30]
Law of Ukraine "On Protection of Information in Information and Telecommunication Systems"	The term "cyberdefense" is absent. Instead, "information protection" is used	Article 1	[25]
Law of Ukraine "On Electronic Communications	Definition is absent, uses the term in the context of network security	Article 76	[31]

The AI analysis also revealed active use of the term "cyberdefense" in subordinate normative legal acts after 2020, particularly in the Resolution of the Cabinet of Ministers of Ukraine "On Approval of General Requirements for Cyberdefense of Critical Infrastructure Objects" [32] and the Resolution of the Cabinet of Ministers of Ukraine "Certain Issues of Critical Infrastructure Objects" [33].

Comparative analysis enabled the systematization of five key characteristics of the definition of the term "cyberdefense" (Table 6).

Table 6
Identified characteristics of the definition of the term "cyberdefense" in Ukrainian legislation

Characteristic	Description	Source
Monopoly of a single source	The single normative definition is contained in the Law "On Basic Principles of Ensuring Cybersecurity of Ukraine"; all other acts refer to it or use the term without a definition	[27]
Instrumental character	Unlike "cybersecurity" (state of protection), "cyberdefense" is defined as an active activity	[27]
Absence of clear delineation	In legislation, the concepts "cyberdefense" and "information protection" are not always clearly delineated	[27]
Threefold function	The definition encompasses the complete security cycle –prevention (ensuring), response (countering), recovery (eliminating consequences)	[27]

4.4. Systematization of identified terminological inconsistencies

At the fourth stage, using Query 4, a comparative analysis of the identified definitions was conducted, and terminological inconsistencies were systematized (Table 7).

Table 7
Typology of identified terminological inconsistencies

Type of inconsistency	Characteristic	Example	Source
Temporal discrepancy	Coexistence of "old" and "new" terminology without clear delineation of areas of application	"Information protection" (1994) vs "cyberdefense" (2017)	[25], [27]
Fragmentation of definitions	Presence of variations in definitions despite the existence of a basic definition	"Cybersecurity" is used without a definition in 3 out of 4 identified acts	[28], [30], [31]
Monopolization of definition	Single source of definition with extensive cross-sectoral use of the term	Only the Law "On Basic Principles of Ensuring Cybersecurity of Ukraine" defines "cybersecurity" and "cyberdefense"	[27]
Conceptual inconsistency	Absence of a legislatively established relationship between related concepts	The relationship between "cyberdefense" vs "information protection" is not defined	–

The most problematic proved to be the temporal discrepancy: legislative acts adopted before 2017 operate with the term "information protection", while acts after 2017 use "cyberdefense" without a clear delineation of the areas of application of these concepts or their relationship.

4.5. Quantitative and Qualitative Evaluation of the proposed methodology

All results obtained through AI analysis were verified through the Official Portal of the Verkhovna Rada of Ukraine (https://zakon.rada.gov.ua/). The verification confirmed the presence of all identified legislative acts, the correctness of extracted definitions and references to articles, and the relevance of current versions of normative legal acts as of February 2026. The proposed methodology demonstrated the ability to rapidly identify relevant legislative acts from the array of normative legal bases, systematize term definitions in tabular format, detect structural inconsistencies through comparative analysis, and classify types of terminological problems. Traditional manual analysis of a comparable volume of legislation would require significantly greater time resources, which confirms the practical value of the proposed AI-assisted approach for legislative analysis.

Verification of all 16 AI-identified legislative acts against the Official Portal of the Verkhovna Rada of Ukraine confirmed the presence of each identified act, the accuracy of extracted definitions, and the correctness of references to specific articles. No AI-generated output required exclusion due to inaccuracy, yielding a precision rate of 100% across all three analysed terms (8 acts for "information", 4 for "cybersecurity", and 4 for "cyberdefense"). This result indicates an absence of hallucinations in the AI output within the scope of the present study, though it should be interpreted in light of the methodological limitation noted in Section 3.2: the model's coverage cannot be assessed for completeness in the absence of a comprehensively annotated reference corpus of Ukrainian cybersecurity legislation, and recall therefore remains outside the scope of quantitative evaluation in this study.

5. Conclusions

The study presents an innovative framework for detecting terminological inconsistencies in Ukrainian legislation in the domain of information and cybersecurity using AI, specifically the LLM Claude Sonnet 4.5. The proposed methodology combines structured queries to the AI model with mandatory verification of results against official legislative databases, which ensures the reliability and validity of obtained conclusions in the context of a low-resource language.

Deployment of the established method to the analysis of 3 key terms ("information", "cybersecurity", and "cyberdefense") revealed five types of terminological inconsistencies in Ukrainian legislation: temporal discrepancy between "old" and "new" terminology, fragmentation of definitions, monopolization of definition by a single legislative act, conceptual inconsistency of related concepts, and absence of clear functional delineation of terms. The most critical proved to be the problem of the coexistence of the terms "information protection" and "cyberdefense" without a legislatively defined relationship. Comparative analysis demonstrated the contrast between the high terminological consistency of the basic concept "information" (stable definition over 30 years) and the significant inconsistency of newer terms "cybersecurity" and "cyberdefense".

The methodological innovation of the study lies in the development of a scalable approach to legislative analysis suitable for application in a dynamic legal environment. Structured queries can be adapted for continuous monitoring of terminological consistency without a proportional increase in resource expenditure, which is critically important in conditions of high frequency of legislative changes in Ukraine. Verification of results through the Official Portal of the Verkhovna Rada of Ukraine confirmed the correctness of the AI analysis as of February 2026, certifying the practical applicability of the proposed framework.

The practical significance of the study lies in providing systematized documentation of specific terminological inconsistencies that require legislative resolution to ensure legal certainty in the

domain of information and cybersecurity. The results can be used by legislators to develop normative legal acts on the harmonization of terminology and to implement procedures for AI-assisted verification of legislative bills for terminological consistency.
Prospects for further research include: expansion of analysis to additional terms in the cybersecurity domain; application of the methodology to other sectors of Ukrainian legislation; comparative analysis of terminological consistency with legal systems of EU countries in the context of European integration.

Acknowledgements

The authors express their sincere gratitude to the Armed Forces of Ukraine for providing security, which made our research possible.

Declaration on Generative AI

During the preparation of this work, the authors used Claude Sonnet 4.5 (model identifier: claude-sonnet-4-5-20250929) to identify legislative acts that define the terms "information", "cybersecurity", and "cyberdefense", extract terminology from Ukrainian legislation, and systematize terminological inconsistencies. All processes, including the development of structured prompts and verification procedures, are described in detail in the research methodology (Section 3). After using this tool, the authors rigorously verified all results through the Official Portal of the Verkhovna Rada of Ukraine and take full responsibility for the publication's content.

References

[1] D. M. Katz, M. J. Bommarito, S. Gao, P. Arredondo, GPT-4 passes the bar exam, Philosophical Transactions of the Royal Society A: Mathematical, Physical and Engineering Sciences 382 (2024) 20230254. doi:10.1098/rsta.2023.0254.

[2] L. Zheng, W. L. Chiang, Y. Sheng, S. Zhuang, Z. Wu, Y. Zhuang, Z. Lin, Z. Li, D. Li, E. P. Xing, H. Zhang, J. E. Gonzalez, I. Stoica, Judging LLM-as-a-Judge with MT-Bench and Chatbot Arena, in: A. Oh, T. Neumann, A. Globerson, K. Saenko, M. Hardt, S. Levine (Eds.), Advances in Neural Information Processing Systems 36, Neural Information Processing Systems Foundation, 2023. doi:10.48550/arXiv.2306.05685.

[3] O. Kovalchuk, R. Shevchuk, M. Masonkova, A. Banakh, Content Analysis of Court Decisions: A GPT-4 Based Sentence-by-Sentence Data Generation and Association Rules Mining, in: Proceedings of the I International Workshop of Young Scientists on Artificial Intelligence for Sustainable Development 2024, 2024, pp. 56–70. URL: https://ceur-ws.org/Vol-3716/paper5.pdf.

[4] V. Costa, M. Castelli, P. Coelho, A Transformer-Based Model for the Automatic Detection of Administrative Burdens in Transposed Legislative Documents, Technologies 13 (2025) 134. doi:10.3390/technologies13040134.

[5] O. Ya. Kovalchuk, Organizational and Legal Support for Digitalization of Judiciary in Ukraine, Ph.D. thesis, National University of Life and Environmental Sciences of Ukraine, Kyiv, 2025.

[6] United Nations, Transforming our world: the 2030 Agenda for Sustainable Development, Resolution A/RES/70/1, United Nations General Assembly, New York, NY, 2015. URL: https://www.refworld.org/legal/resolution/unga/2015/en/111816.

[7] V. I. Teremetskyi, O. Ya. Kovalchuk, Artificial Intelligence as a Factor in the Digital Transformation of the Justice System, Forum Prava 78 (2024) 106–115. doi:10.5281/zenodo.10870779.

[8] European Union Publications Office, EUR-Lex Strategic Plan 2022-2024: Harnessing AI for Legal Information Access, Publications Office of the European Union, Luxembourg, 2022. URL: https://eur-lex.europa.eu/content/welcome/about.html.

[9] National Institute of Standards and Technology, Artificial Intelligence Risk Management Framework (AI RMF 1.0), NIST AI 100-1, U.S. Department of Commerce, Washington, DC, 2023. URL: https://nvlpubs.nist.gov/nistpubs/ai/NIST.AI.100-1.pdf.
[10] Singapore Academy of Law, Legal Technology Vision 2030: Transforming Legal Practice through AI, Technology, Innovation and Productivity Committee Report, Singapore, 2021. URL: https://www.sal.org.sg/.
[11] O. Syvokon, M. Romanyshyn, The UNLP 2023 Shared Task on Grammatical Error Correction for Ukrainian, in: Proceedings of the Second Ukrainian Natural Language Processing Workshop (UNLP), Association for Computational Linguistics, 2023, pp. 132–137. doi:10.18653/v1/2023.unlp-1.8.
[12] Verkhovna Rada of Ukraine, Official portal. Legislation of Ukraine, 2026. URL: https://zakon.rada.gov.ua/.
[13] O. Kovalchuk, S. Banakh, M. Masonkova, K. Berezka, S. Mokhun, N. Fedchyshyn, Text Mining for the Analysis of Legal Texts, in: Proceedings of the 12th International Conference on Advanced Computer Information Technologies (ACIT), IEEE, Spišská Kapitula, Slovakia, 2022, pp. 502–505. doi:10.1109/ACIT54803.2022.9913169.
[14] I. Chalkidis, M. Fergadiotis, P. Malakasiotis, N. Aletras, I. Androutsopoulos, LEGAL-BERT: The Muppets straight out of Law School, in: Findings of the Association for Computational Linguistics: EMNLP 2020, Association for Computational Linguistics, 2020, pp. 2898–2904. doi:10.18653/v1/2020.findings-emnlp.261.
[15] I. Chalkidis, N. Garneau, C. Goanta, D. M. Katz, A. Sogaard, LeXFiles and LegalLAMA: Facilitating English Multinational Legal Language Model Development, in: Proceedings of the 61st Annual Meeting of the Association for Computational Linguistics (Volume 1: Long Papers), Association for Computational Linguistics, 2023, pp. 15513–15535. doi:10.18653/v1/2023.acl-long.865.
[16] J. Savelka, K. D. Ashley, The unreasonable effectiveness of large language models in zero-shot semantic annotation of legal texts, Frontiers in Artificial Intelligence 6 (2023) 1279794. doi:10.3389/frai.2023.1279794.
[17] J. Niklaus, V. Matoshi, M. Stürmer, I. Chalkidis, D. E. Ho, MultiLegalPile: A 689GB Multilingual Legal Corpus, in: Proceedings of the 62nd Annual Meeting of the Association for Computational Linguistics (Volume 1: Long Papers), Association for Computational Linguistics, 2024, pp. 15077–15094. doi:10.18653/v1/2024.acl-long.805.
[18] P. Joshi, S. Santy, A. Budhiraja, K. Bali, M. Choudhury, The State and Fate of Linguistic Diversity and Inclusion in the NLP World, in: Proceedings of the 58th Annual Meeting of the Association for Computational Linguistics, Association for Computational Linguistics, 2020, pp. 6282–6293. doi:10.18653/v1/2020.acl-main.560.
[19] H. Muradyan, P. Alexopoulos, C. Mourougane, A survey on challenges and advances in natural language processing with a focus on legal informatics and low-resource languages, Electronics 13 (2024) 648. doi:10.3390/electronics13030648.
[20] D. Chaplynskyi, Introducing UberText 2.0: A corpus of modern Ukrainian at scale, in: Proceedings of the Second Ukrainian Natural Language Processing Workshop (UNLP), Association for Computational Linguistics, 2023, pp. 1–10. doi:10.18653/v1/2023.unlp-1.1.
[21] Rules for drafting bills and the main requirements of legislative technique (Methodological Guidelines), October 27, 2014, Legislation of Ukraine. URL: https://zakon.rada.gov.ua/rada/show/n0002451-06#Text
[22] Law of Ukraine No. 2657-XII On Information, October 2, 1992, Legislation of Ukraine. URL: https://zakon.rada.gov.ua/laws/show/2657-12#Text.
[23] Law of Ukraine No. 2297-VI On Protection of Personal Data, June 1, 2010, Legislation of Ukraine. URL: https://zakon.rada.gov.ua/laws/show/2297-17#Text.