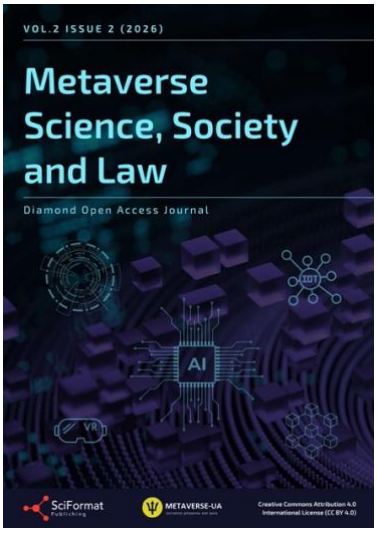


Metaverse Science, Society and Law

Vol. 2, Issue 2 (2026)

SciFormat Publishing

Publisher:
SciFormat Publishing Inc.

ISNI: 0000 0005 1449 8214
2734 17 Avenue Southwest, Calgary,
Alberta, Canada, T3E0A7

+15878858911
editorial-office@sciformat.ca

ARTICLE TITLE	CRIMINAL-LAW CHARACTERIZATION OF CYBERCRIMES COMMITTED THROUGH THE USE OF ARTIFICIAL INTELLIGENCE
DOI	https://doi.org/10.69635/mssl.2026.2.2.39
RECEIVED	21 January 2026
ACCEPTED	17 April 2026
PUBLISHED	01 May 2026
LICENSE	The article is licensed under a **Creative Commons Attribution 4.0 International License.**

© The author(s) 2026.
This article is published as open access under the Creative Commons Attribution 4.0 International License (CC BY 4.0), allowing the author to retain copyright. The CC BY 4.0 License permits the content to be copied, adapted, displayed, distributed, republished, or reused for any purpose, including adaptation and commercial use, as long as proper attribution is provided.

CRIMINAL-LAW CHARACTERIZATION OF CYBERCRIMES COMMITTED THROUGH THE USE OF ARTIFICIAL INTELLIGENCE

Viktoriya Liubavina
Candidate of Law, Associate Professor of the Department of Criminal Law and Procedure, Educational and Scientific Institute of Law, State Tax University, Ukraine
ORCID ID: 0000-0003-4715-1749

Bogdan Krymchanin
Third-Year Higher Education Student, State Tax University, Ukraine
ORCID ID: 0009-0003-4339-6658

ABSTRACT

The article examines the criminal-law characterization of cybercrimes committed through the use of artificial intelligence technologies, taking into account current trends in the digitalization of social relations and the transformation of criminal activity within the information environment. It is substantiated that the rapid development of artificial intelligence gives rise not only to new opportunities for automation, data processing, and increasing the efficiency of digital processes, but also to additional criminogenic risks associated with the use of such technologies for the commission of socially dangerous acts in cyberspace. Particular attention is paid to the fact that the use of artificial intelligence in the mechanism of cybercrime commission complicates the process of detecting, documenting, and properly assessing unlawful conduct under criminal law.

The article analyzes general approaches to understanding cybercrime as a distinct form of criminal activity that encroaches upon the security of information systems, computer networks, electronic communications, and the related social relations. Special attention is given to the impact of artificial intelligence on the modification of traditional methods of committing cybercrimes, in particular through the automation of unauthorized interference, the concealment of criminal activity, the creation of malicious software, the manipulation of information, and the imitation of human digital behavior. It is determined that, in the context of the development of intelligent technologies, particular importance attaches to the proper classification of acts, the establishment of the form of guilt, causation, and the distinction between the use of artificial intelligence as an instrument for committing a crime and cases of its lawful application.

It is concluded that the criminal-law characterization of cybercrimes committed through the use of artificial intelligence requires comprehensive scholarly analysis in view of contemporary technological challenges, law enforcement practice, and the need to improve approaches to criminal-law response to emerging forms of criminal activity.

KEYWORDS

Cybercrimes, Artificial Intelligence, Criminal-Law Characterization, Cybercrime, Classification of Criminal Offenses, Information Technologies, Cyberspace, Criminal Liability, Digital Evidence, Information Security

CITATION

Viktoriya Liubavina, Bogdan Krymchanin. (2026) Criminal-Law Characterization of Cybercrimes Committed Through the Use of Artificial Intelligence. *Metaverse Science, Society and Law*. Vol. 2, Issue 2. doi: 10.69635/mssl.2026.2.2.39

COPYRIGHT

© The author(s) 2026. This article is published as open access under the **Creative Commons Attribution 4.0 International License (CC BY 4.0)**, allowing the author to retain copyright. The CC BY 4.0 License permits the content to be copied, adapted, displayed, distributed, republished, or reused for any purpose, including adaptation and commercial use, as long as proper attribution is provided.

Introduction

Under current conditions, Ukraine's cyberspace is increasingly becoming an environment for the realization of socially dangerous encroachments, the consequences of which may affect human rights, the interests of society, the stability of the functioning of state institutions, as well as the state of the country's information security. This approach is consistent with the constitutional provisions according to which the individual, their security, and the protection of the State's information security constitute fundamental legal values and priorities [1].

This issue acquires particular relevance in view of the fact that artificial intelligence may be used as a tool for the automation of criminal activity, the acceleration of the search for vulnerabilities in information systems, the generation of malicious software code, the mass dissemination of phishing messages, the imitation of human digital behavior, and the concealment of traces of unlawful interference. At the same time, the current criminal legislation of Ukraine already contains provisions that form the basis for a criminal-law response to unlawful acts in the sphere of the use of electronic computing machines, computer networks, and telecommunications, in particular with regard to unauthorized interference, the creation and dissemination of malicious software or technical means, unauthorized actions involving information, violations of the rules for operating the relevant systems, and obstruction of their functioning through the mass distribution of electronic communications messages [2]. The problem lies not only in the existence of criminal-law prohibitions, but also in a proper understanding of how exactly the use of artificial intelligence affects the elements of a criminal offense and its classification.

The need for an in-depth scholarly analysis is further reinforced by the fact that the issue of combating cybercrime has extended beyond the limits of exclusively national legal regulation. The Law of Ukraine "On the Basic Principles of Ensuring Cybersecurity of Ukraine" directly links state policy in this sphere with the protection of human rights and freedoms, the national interests of Ukraine in cyberspace, combating cybercrime, and international cooperation with organizations engaged in such efforts [3]. At the same time, the Convention on Cybercrime forms the international legal foundation for a coordinated approach by states to combating crimes committed through the use of computer systems and networks [4]. This demonstrates that the study of the criminal-law characterization of cybercrimes committed through the use of artificial intelligence should be based both on national legal provisions and on international standards.

The issue of the criminal-law characterization of cybercrimes committed through the use of artificial intelligence, as well as the problems of their proper classification in the context of the rapid development of digital technologies, has not yet received comprehensive and independent treatment in domestic criminal-law scholarship. At the same time, certain aspects of this issue related to combating cybercrime, the criminal-law assessment of the use of emerging information technologies, the peculiarities of establishing the elements of a criminal offense, and the adaptation of criminal-law approaches to contemporary technological challenges have been addressed in the works of V. I. Antypov, O. M. Bodunova, D. I. Lopashchuk, N. A. Luhina, V. P. Liubavina, O. V. Kostenko, M. H. Maksimentsev, O. P. Milevskyi, L. V. Omelchuk, O. A. Pavliukh, N. A. Sperkach, V. V. Topchii, V. M. Tertyshnyk, and others.

Special attention should also be paid to the fact that contemporary international instruments in the field of artificial intelligence regulation already proceed from the existence of different levels of autonomy and adaptability in such systems, as well as from the need to ensure transparency, accountability, and legal control over the consequences of their use [5]. In this connection, it may be argued that, for criminal law, it is fundamentally important not merely to establish the fact that a given technology was used, but above all to determine its role in the mechanism of committing a criminal offense: as a means, instrument, element of preparation, method of concealment, or factor affecting socially dangerous consequences. For this reason, the purpose of this article is to provide a comprehensive analysis of the criminal-law characterization of cybercrimes committed through the use of artificial intelligence, with the identification of their principal legally significant features and the problems of their classification in the context of the development of advanced digital technologies.

Part 1. Theoretical and Legal Foundations of the Criminal-Law Characterization of Cybercrimes Committed through the Use of Artificial Intelligence

For a proper understanding of the criminal-law characterization of cybercrimes committed through the use of artificial intelligence, it is first necessary to clarify the content of the basic categories through which this issue is addressed. Under the current legislation of Ukraine, a cybercrime is defined as a socially dangerous culpable act committed in cyberspace and/or through its use, liability for which is provided for by the law of Ukraine on criminal liability and/or which is recognized as a crime by the international treaties of Ukraine [3]. This definition is important from a methodological perspective, as it provides grounds for considering cybercrimes not only as acts directly предусмотрені by the provisions of Chapter XVI of the Criminal Code of Ukraine, but also more broadly as criminal offenses in which cyberspace serves as the environment, means, or instrument of criminal conduct. At the same time, the international approach embedded in the Convention on Cybercrime is oriented toward the criminalization of unauthorized access, illegal interception, interference with data or systems, misuse of devices, as well as a number of related acts associated with the use of computer technologies [13].

The normative basis for the criminal-law assessment of such acts consists of the provisions of the Criminal Code of Ukraine, first and foremost the norms establishing liability for unauthorized interference with the operation of information systems, the creation and dissemination of malicious software, unlawful actions involving information, and other unlawful encroachments in the sphere of the use of electronic computing machines, computer networks, and telecommunications networks [2]. It is precisely within the framework of these elements of criminal offenses that the issue of the use of artificial intelligence as a new technological instrument for committing a crime most often arises.

In this context, artificial intelligence should be regarded not as an independent participant in criminal-law relations, but as a means of implementing a person's unlawful intent. Its use may consist in the automated search for vulnerabilities, the generation of malicious software code, the selection of methods for bypassing digital protection, the creation of false messages, or the imitation of the behavior of a real user. However, even where such systems possess a high degree of autonomy, the subject of the criminal offense under current legislation remains a natural, sane person who understands the nature of their actions and is capable of controlling them [2].

From a theoretical perspective, it is important that the use of artificial intelligence does not always alter the legal nature of the criminal offense itself, but may substantially affect the method of its commission. This means that, in most cases, artificial intelligence does not create a new and separate element of a criminal offense, but merely complicates the mechanism for carrying out already known forms of cybercriminal conduct. For that reason, in the criminal-law characterization decisive significance attaches not to the technical features of the program, but to its role in the encroachment upon social relations protected by law [3].

The object of such criminal offenses consists of social relations ensuring the confidentiality, integrity, and availability of information, the secure functioning of computer systems, and the proper circulation of electronic data. At the same time, as a result of the use of artificial intelligence, the encroachment may have broader consequences and may affect property rights, personal privacy, the information security of the State, or the continuity of the activities of institutions and organizations. Therefore, the criminal-law characterization of such acts should encompass not only the technical method of influence, but also the content of the actual or potential harm caused [1].

A specific feature of the objective element of cybercrimes committed through the use of artificial intelligence is the increase in the speed, scale, and concealment of unlawful activity. The use of intelligent systems makes it possible to automate individual stages of criminal conduct, reduce the direct involvement of a person in the performance of technical operations, and complicate the identification of the source of the attack. It is precisely this that creates additional difficulties in establishing the method of committing the criminal offense, causation, and the limits of the guilt of the specific person [2].

The subjective element of such acts is, as a rule, characterized by an intentional form of guilt, since the use of artificial intelligence for interference with information systems or for unlawful influence upon the digital environment generally has a purposeful character. At the same time, in practice, difficulties may arise in establishing the extent to which the person was aware of the possible consequences of applying intelligent algorithms. For this reason, the correct classification of such acts depends in particular on determining who initiated the use of the relevant technology, for what purpose, and within what limits they controlled its functioning [3].

In an additional theoretical dimension, it should be taken into account that the development of artificial intelligence and other digital environments does not negate the classical foundations of criminal law, but, on the contrary, highlights the need to adapt them to new forms of unlawful conduct in virtual and hybrid spaces. Scholarly literature substantiates that, in the context of digitalization, decisive significance attaches not to the formal separation of technology as an independent bearer of liability, but to the normative definition of those socially dangerous acts that may be committed through the use of digital instruments, algorithmic solutions, virtual objects, and electronic environments. For that reason, the use of artificial intelligence should be regarded as a contemporary form of technological mediation of already known criminally unlawful encroachments, one that requires clarification of approaches to their criminal-law assessment, but does not destroy the traditional structure of the elements of a criminal offense [13].

Thus, it may be asserted that the theoretical and legal foundations of the criminal-law characterization of cybercrimes committed through the use of artificial intelligence lie in the fact that such acts should be assessed through the prism of the traditional elements of a criminal offense, while taking into account the new technological methods of implementing criminal intent. In this case, artificial intelligence acts not as a subject, but as an instrument, the use of which affects the method of committing the offense, the nature of its consequences, and the complexity of its legal assessment [2].

Part 2. Peculiarities of the Classification and Problems of Criminal-Law Response to Cybercrimes Committed through the Use of Artificial Intelligence

A particular feature of the classification of cybercrimes committed through the use of artificial intelligence lies in the fact that decisive importance attaches not to the mere presence of artificial intelligence technology, but to its functional role in the mechanism of the criminal offense. If the relevant system is used for unauthorized interference with the operation of information or electronic communications systems, the legal assessment should primarily be carried out under Article 361 of the Criminal Code of Ukraine; where the issue concerns the creation or dissemination of malicious software, under Article 361-1; in the event of unlawful sale or distribution of information with restricted access, under Article 361-2; in cases of unauthorized actions by a person who has the right of access to information, under Article 362; and in the event of intentional mass dissemination of messages resulting in disruption of the functioning of systems, under Article 363-1 [2].

The complexity of classification is due to the fact that the use of artificial intelligence may conceal the actual method of committing the criminal offense, complicate the establishment of the causal link between a person's actions and the consequences, and create the false impression of an allegedly autonomous character of unlawful conduct. In this connection, in each particular case it is necessary to determine who exactly initiated the use of the intelligent system, for what purpose it was employed, what functions it performed, and whether its results were covered by the intent of the guilty person [11].

From the criminal procedural perspective, the proper classification of such acts is impossible without appropriate proof of the method of commission of the offense, the form of guilt, motive, and consequences. The Criminal Procedure Code of Ukraine requires that a judicial decision be based on objectively established circumstances confirmed by evidence, and that the judgment reflect the place, time, method of commission of the criminal offense, its consequences, the form of guilt, and motives. For this reason, in proceedings concerning cybercrimes committed through the use of artificial intelligence, particular importance attaches to the proper fixation of digital traces and to proving the real connection between the algorithmic instrument and the conduct of a specific person [6].

A separate issue is the distinction between criminally punishable use of artificial intelligence and its lawful application. This question is fundamental, since contemporary international standards in the field of artificial intelligence proceed from the need to combine innovative development with transparency, control, oversight, and responsibility for the consequences of the use of such systems. Accordingly, in law enforcement practice it is important to avoid situations in which the mere presence of an algorithmic instrument is equated with criminality without proof of the specific unlawful manner of its use [7].

In the course of classification, it should also be taken into account that a substantial part of such encroachments is carried out through electronic communications infrastructure. This means that, for proper criminal-law assessment, relevance attaches not only to the facts of interference with a system, but also to the specific features of the functioning of electronic communications networks, services, and technical channels through which the unlawful impact was carried out. Accordingly, an effective criminal-law response requires proper interaction with those entities that ensure the functioning of the relevant communications infrastructure [8].

Another complex aspect is connected with cases in which artificial intelligence is used for the unlawful collection, analysis, modification, or dissemination of information having a confidential or otherwise restricted access regime. In such a situation, the harmful consequences are not limited to technical interference with the system, but also encompass encroachments upon information rights, privacy, the data protection regime, and the security of data circulation. For this reason, the content of the harm caused must be determined more broadly than merely as a disruption of the functioning of a computer system [9].

No less important is the fact that the legal response to such acts must take into account the requirements of legislation on the protection of information in information and communication systems. If artificial intelligence is used to circumvent protective means, identify vulnerabilities, or gain access to protected data sets, this increases the social dangerousness of the act and should be taken into account in assessing the method of its commission and the nature of its consequences [10].

Legal scholarship rightly emphasizes that the development of artificial intelligence is already affecting not only the methods of committing cybercrimes, but also the mechanisms of their detection, proof, and procedural support. Hence arises the need to refine approaches to the classification of such acts, strengthen the specialization of law enforcement actors, and develop clearer criteria for distinguishing between lawful and criminally punishable uses of intelligent technologies [12]. The peculiarities of the classification of cybercrimes committed through the use of artificial intelligence lie in the need to assess not the name or technical complexity of the algorithm, but the specific nature of its use within the structure of the criminal offense. The main difficulties of criminal-law response are connected with proving human guilt, establishing causation, properly assessing digital consequences, and distinguishing criminal conduct from the lawful use of emerging technologies [11].

Conclusions

The conducted research provides grounds for asserting that the issue of the criminal-law characterization of cybercrimes committed through the use of artificial intelligence can no longer be regarded as a narrowly specialized or purely technical matter. Rather, it constitutes a complex legal phenomenon situated at the intersection of criminal law, information law, cybersecurity, and the contemporary legal regulation of digital technologies. It is precisely the development of artificial intelligence that substantially transforms the understanding of the mechanism of committing a criminal offense in cyberspace, as it makes it possible significantly to increase the speed, scale, adaptability, and concealment of unlawful activity. As a result, traditional approaches to the detection, recording, proof, and classification of cybercrimes are subjected to considerable strain and require further clarification.

It has been established that artificial intelligence, within the structure of the criminal offenses under study, should be regarded not as an independent subject of criminal-law relations, but as an instrument, means, or technological environment for the realization of human criminal intent. Despite the increasing autonomy of certain algorithmic systems, criminal-law assessment must continue to preserve its anthropocentric character. This means that what is decisive for classification is the establishment of the conduct of the specific natural person who initiated, configured, directed, or knowingly used the capabilities of artificial intelligence to achieve an unlawful result. The mere fact of using an intelligent system does not in itself create a new corpus delicti; however, it substantially affects the method of commission, the nature of the consequences, and the complexity of proving guilt.

Within the framework of the article, it is substantiated that cybercrimes committed through the use of artificial intelligence generally receive their criminal-law assessment within the scope of already existing provisions of criminal legislation, first and foremost those establishing liability for unauthorized interference with the operation of information systems, the creation and dissemination of malicious software, unlawful actions involving information, as well as other encroachments in the sphere of the use of computer networks, electronic communications, and digital data. The issue, therefore, lies not so much in the absence of legal prohibitions as in the need for their modern interpretation under conditions of a technologically complicated method of committing criminal offenses. Artificial intelligence does not abolish the classical elements of a criminal offense, but it renders their establishment considerably more difficult, especially where the method of action, causation, the extent of the person's control over the algorithm, and the limits of foreseeability of consequences are concerned.

Particular significance also attaches to the subjective element of such acts. In most cases, the use of artificial intelligence for the commission of a cybercrime is purposeful in nature and combined with an intentional form of guilt. At the same time, contemporary digital systems may operate on the basis of complex

learning models, generate variable outcomes, and function with a certain degree of technical autonomy. It is precisely this that creates difficulties for the accurate assessment of which consequences were covered by the intent of the guilty person, how foreseeable the behavior of the algorithm was, whether there was a conscious construction of a criminal mechanism, or whether a different form of mental attitude toward the consequences is involved. In view of this, the proper classification of such acts requires particularly careful establishment of the intellectual and volitional elements of guilt, as well as an analysis of the role of each participant in the creation and use of the relevant technological solution.

An important conclusion is also that the use of artificial intelligence increases the latency of cybercrimes. Automated identification of vulnerabilities, generation of false content, modification of malicious software, imitation of users' digital behavior, circumvention of protective measures, and concealment of the source of interference significantly complicate the detection of the actual method of criminal activity. For this reason, law enforcement practice is becoming increasingly dependent on the quality of work with digital evidence, the professional specialization of investigative actors, and the ability to combine technical analysis with a proper legal assessment of the established facts. In such a situation, the need to strengthen the expert and methodological support of criminal proceedings in cybercrime cases involving the use of artificial intelligence tools is beyond doubt.

In conclusion, it should be emphasized that the criminal-law characterization of cybercrimes committed through the use of artificial intelligence must be built upon a combination of the classical provisions of criminal law with a new understanding of the digital method of committing a criminal offense. This requires further doctrinal elaboration of the criteria for the classification of such acts, clarification of the role of artificial intelligence in the mechanism of criminal conduct, improvement of approaches to the assessment of guilt and consequences, and the formation of a more modern law enforcement practice. Under such conditions, the development of legislation and practice should proceed not through the mechanical creation of a large number of new norms, but through the substantive modernization of the methods of interpreting the current criminal law, the strengthening of intersectoral interaction, and due consideration of real technological risks.

REFERENCES

1. Constitution of Ukraine, No. 254k/96-VR (1996, June 28) (Ukraine) (as amended January 1, 2020). https://zakon.rada.gov.ua/laws/show/254к/96-вр#Text
2. Criminal Code of Ukraine, No. 2341-III (2001, April 5) (Ukraine) (as amended July 17, 2025). https://zakon.rada.gov.ua/laws/show/2341-14#Text
3. Criminal Procedure Code of Ukraine, No. 4651-VI (2012, April 13) (Ukraine) (as amended April 1, 2026). https://zakon.rada.gov.ua/laws/show/4651-17#Text
4. Law of Ukraine No. 2163-VIII, On the Basic Principles of Ensuring Cybersecurity of Ukraine (2017, October 5) (Ukraine) (as amended October 19, 2025). https://zakon.rada.gov.ua/laws/show/2163-19#Text
5. Law of Ukraine No. 2657-XII, On Information (1992, October 2) (Ukraine) (as amended January 20, 2026). https://zakon.rada.gov.ua/laws/show/2657-12#Text
6. Law of Ukraine No. 80/94-VR, On Protection of Information in Information and Telecommunication Systems (1994, July 5) (Ukraine) (as amended April 20, 2025). https://zakon.rada.gov.ua/laws/show/80/94-вр#Text
7. Law of Ukraine No. 1089-IX, On Electronic Communications (2020, December 16) (Ukraine) (as amended February 27, 2026). https://zakon.rada.gov.ua/laws/show/1089-20#Text
8. Council of Europe. (2001, November 23). *Convention on Cybercrime* (in force for Ukraine September 7, 2005). https://zakon.rada.gov.ua/laws/show/994_575#Text
9. European Parliament and Council of the European Union. (2024, June 13). *Regulation (EU) 2024/1689 laying down harmonised rules on artificial intelligence (Artificial Intelligence Act)*.
10. Council of Europe. (2024, September 5). *Framework Convention on Artificial Intelligence and Human Rights, Democracy and the Rule of Law* (CETS No. 225).
11. Kostenko, O. A. (Ed.). (2026). *Artificial intelligence, modern technologies and law in Ukraine: Monograph* [Electronic edition]. Phoenix.
12. Radutnyi, O. E. (2017). Criminal liability of artificial intelligence. *Information and Law, 2*(21), 124–132. https://doi.org/10.37750/2616-6798.2017.2(21).273064
13. Kostenko, O., Zhuravlov, D., Dniprov, O., & Korotiuk, O. (2023). Metaverse: Model criminal code. *Baltic Journal of Economic Studies, 9*(4), 134–147. https://doi.org/10.30525/2256-0742/2023-9-4-134-147