Proceedings of ICSPHS 2026 Symposium:Ethics, Law, and Psychology: Interdisciplinary Reconstruction of Humanities in Medicine
DOI: 10.54254/2753-7048/2026.ZJU31772

The Connection Path Between International Criminal Law Governance and Network Information Law for Transnational Cybercrimes under Data Sovereignty Conflicts

Jiayin Zhuang

Institute of Criminal Law, East China University of Political Science and Law, Shanghai, China
24040101016@ecupl.edu.cn

Abstract. The continuous deepening of digital globalization has normalized data cross-border flow. Data sovereignty, as the core extension and important component of national sovereignty in the digital era, has gained increasing strategic significance However, countries' divergent history, culture, legal traditions and development stages lead to differentiated data jurisdiction rules, which intensify cross-border data sovereignty conflicts and pose severe challenges to transnational cybercrime governance Focusing on this core background, this article, from the intersection of international criminal law governance and cyber information law, explores their logical connections in legislative concepts, rule application and implementation mechanisms, and analyzes practical pain points and key issues in transnational cybercrime governance. It further proposes targeted solutions: clarifying jurisdictional basis via rule alignment, unifying electronic evidence standards and liability boundaries, improving the international convention system through mechanism coordination, establishing a rapid information sharing and dispute resolution platform, deepening transnational law enforcement cooperation, and building a full-chain prevention system via technological empowerment, so as to boost global digital governance effectiveness.

Keywords: Data sovereignty, transnational cybercrime, International Criminal Law, network information law, legal connection

1. Introduction

Due to the emergence of digital technology, data has been able to cross geographical borders. The magnitude of cross-border data flow has increased three times the global cross-border data flow, five years after. Nonetheless, the clash between the cross-borderity of data and the sovereignty of data on claims by different states has been growing more acute. As an example, in the 2022 case in Colonial Pipeline Ransomware, the United States of America asserted investigative jurisdiction over the case under territorial jurisdiction, yet Russia, where the servers of the criminal group were situated, declined to assist with evidence offering an argument of data localization. This case throws emphasis on the limitations of the sovereignty wars to governance. Details sovereignty has also emerged a critical carrier of states in protecting digital security, and its inconsistency with the

© 2026 The Authors. This is an open access article distributed under the terms of the Creative Commons Attribution License 4.0 (https://creativecommons.org/licenses/by/4.0/).

DOI: 10.54254/2753-7048/2026.ZJU31772

regulation of the transnational cybercrimes has come into the limelight, and there is the need that co-ordinated actions be taken at the legal front. The literature addressing the topic is significantly confined to the regulation of transnational cybercrimes by international criminal law or the question of data sovereignty of network information law, as opposed to a systematic discussion of the relationship between the two areas. The need to legalize the coordination was stated by some scholars but they did not implement an analytic study on the logic and the ways of connecting the law. Moreover, the available literature lacks in empirical examination of cases, as it is not easy to present the actual dilemma in the practice.

The theme in the current paper is on the connection path between network information law and international criminal law when there exist a conflict in data sovereignty. In theory, it can fulfill the disjointed weaknesses of the study on the relationship between the two areas of law and develop an organized theoretical-grounded approach to the relationship between them. En pragmatically, it can offer certain solutions to the governance dilemmas in common scenarios, e.g., the case of data compliance conflict between Google and Russia, the case of an attack by Apple against the national time-keeping center of China, the case of Facebook data scandal, and the case of the WannaCry ransomware, which will enhance the effectiveness of the governance of transnational cybercrimes. Meanwhile, the normative analysis is assumed in this paper, which then proceeds to address the governance dilemmas, the case analysis and comparative research approaches where the connection logic is formulated, and the specific paths are suggested at the conclusion of the paper.

2. Governance dilemmas of transnational cybercrimes under data sovereignty conflicts

2.1. Manifestations of data sovereignty conflicts

Based on data sovereignty, various countries have formed a multi-jurisdictional model integrating territorial, personal and protective jurisdiction, leading to jurisdictional conflicts. The legal framework of the Geneva Conventions and their additional protocols is theoretically applicable, but their implementation has fundamentally been undermined by the unique technical and geopolitical realities of digital conflicts. For example, in the "WannaCry Ransomware Case", the virus attack affected more than 150 countries. The United Kingdom (the victim country), the United States (the technical traceability location) and North Korea (the allegedly involved location) all claimed jurisdiction, resulting in overlapping jurisdictions. In contrast, for a certain cross-border phishing website, due to its server being located in a "tax haven" and the absence of a concentrated location of victim countries, a jurisdictional vacuum emerged [1].

Conflicts in cross-border data flow rules have become a core obstacle to transnational cybercrime governance. For data flow restrictions, China's Personal Information Protection Law (PIPL) prioritizes data sovereignty, safeguarding citizens' personal information via systems like cross-border data security assessments and protection certifications. The EU's General Data Protection Regulation (GDPR) centers on data subjects' rights, emphasizing consent and rights protection while strictly limiting cross-border flows through the adequacy determination mechanism. The U.S. adopts a decentralized, industry self-regulation-based legislative model; its California Consumer Privacy Act (CCPA) grants consumers rights such as data access and deletion, featuring state-level differentiated legislation combined with long-arm jurisdiction. The differences in the concepts and models of these national rules have created a complex and dynamic relationship in the "Facebook Data Scandal", preventing the cross-border retrieval of involved data [2]. Fragmented data security and privacy rules further hinder evidence collection and law enforcement collaboration in transnational cybercrime cases.

DOI: 10.54254/2753-7048/2026.ZJU31772

There are significant differences and increasingly strict requirements for local data storage across various countries, which form a sharp contradiction with the cross-border evidence collection needs of cross-border cybercrime investigations. Many countries have implemented data local storage requirements based on considerations of data sovereignty and security, but the specific standards and applicable scopes vary significantly: Russia's "Law on Information, Information Technology and Information Protection" clearly stipulates that sensitive data involving Russian citizens must be stored on servers within Russia and prohibits unauthorized transmission to foreign countries; China's "Data Security Law" sets local storage obligations for important data and core data, and the data export of key information infrastructure operators requires strict security assessment; India's "Digital Personal Data Protection Act" requires that some sensitive personal data be stored locally and only allows cross-border transmission under specific conditions; The EU, although not mandatorily requiring full local storage, indirectly restricts data export through the adequacy recognition mechanism, and core data must ensure that the storage location complies with the privacy protection standards of the GDPR. However, cross-border cybercrime investigations often require cross-border retrieval of electronic evidence stored in different countries, and the differences and rigid constraints of these local storage requirements, as well as the rigid constraints, directly conflict with the efficiency requirements of cross-border evidence collection. The local Russian storage laws in the Colonial Pipeline Ransomware Case, the US Federal Bureau of Investigation could not directly access the interested data that was stored in Russia and had to undergo a complicated procedure of judicial assistance, and it was only after 3 months that it received crucial electronic evidence, grossly slowing down the case investigation [3].

2.2. Specific dilemmas in international criminal law governance

The established principles of the international criminal law regarding the traditional jurisdiction approaches that revolve around the place of the offense and citizenship of the accused person can hardly accommodate the dynamics of cross-border data flow. In WannaCry Case, the virus propagated automatically through a network and it is hard to define the location of crime. In addition, criminal group members were spread over a number of countries, and personal jurisdiction would not be sufficient to cover them, which resulted in confusion in determining jurisdictions. A more common case in point is the 2021 case of the Apple Vulnerability Attack on China National Timing Center which was leaked. As the investigation report published by the National Computer Virus Emergency Response Center of China states, there was a foreign hacker organization that targeted key infrastructure with cyber-attacks through a zero-day blachery in the Apple devices and stole high-precision time synchronization information, as well as core operating parameters. Here, the attack code was sent by the servers in the United States where the vulnerability exploitation tools were developed, and the victim and target of the attack was in China, and had involved several countries in the European Union. The criminal activity was inter-jurisdictional. The classical doctrine of territorial jurisdiction failed in laying a claim on the core of location of the crime. The United States claimed jurisdiction based on the "technical development location", while China claimed jurisdiction based on the "victim location" and "location of key infrastructure". The conflict in jurisdiction claims between the two sides directly led to the obstruction of initial investigation collaboration, highlighting the insufficient adaptability of traditional jurisdiction principles in cross-border cyber crimes in the field of critical infrastructure.

Restrictions imposed by data sovereignty have made cross-border evidence collection procedures cumbersome, requiring multi-level approval through mutual legal assistance treaties, with an average time consumption of more than six months. In the meantime, the standards that are used in

DOI: 10.54254/2753-7048/2026.ZJU31772

the preservation of electronic evidence across various countries differ. Indicatively, the recognition of screenshot evidence of cloud-stored data is known by the United States and the original data carriers are demanded by the European Union. In the case of Apple Hacking, law enforcement agencies in China were required to seek the logs of attacks on theirs and the communication records of the hacking group located abroad. Nonetheless, these data were stored on the cloud service systems in the USA and in the European Union. The retrieval process was nearly 8 months because of the laws concerning local data sovereignty and privacy protection. Certain important data was not received in time because of the limitations of the storage time, which influenced the effectiveness of containing those members of the attack organization who were its core.

The international movement of data has disaggregated criminal networks in multijurisdictional settings making it harder to assign responsibility to the culprits, websites and technical infrastructure suppliers. This is compounded by the blurred guidelines on determining accessories and abettors of international criminal law [4]. Using two exemplary cases, in the Facebook Data Scandal, the data was gathered in the U. S. and processed in the U. K. and applied in the election process in various other countries, forming a convoluted chain of responsibility. The 2022 Google U. S. -Russia Data Compliance Conflict Case further highlighted the dilemma of multinational companies: Google had to comply with the data localization requirements of Russia (to keep users data on its premises) at the same time as it had the obligation under the Cloud Act of the United States to disclose data stored abroad to U. S. law enforcement. The U.S. prevented the extraction of user information stored locally in Google when Russia requested the details to investigate phishing frauds due to the privacy of citizens. Balancing conflicting statutory requests, Google risked paying large fines in Russia and facing criminal responsibility in the U. S. and this forced it to block all some of its services in Russia and impeded the fraudulent investigations. These incidents reveal the compliance muddle of multinationals during data sovereignty conflicts as well as incomprehensiveness of international criminal law in the establishment of the duty of data controllers.

3. Connection logic between international criminal law and network information law

3.1. Jurisprudential logic of connection

International criminal law prevents the proliferation of crimes through the imposition of network criminal activities, and the network information law prevents criminality by controlling the exchange of data flows. The protection of cybersecurity and order is the main goal in both areas. To illustrate the point, network information law is applied to regulate data storage to ensure no weak areas exist, and international criminal law punishes the offenders when responding to the crimes of ransomware. The two areas constitute a synchronized objective of preventive and punitive action and share the same responsibility to defend cyberspace sanity.

International criminal law is preoccupied with ex post punishment in which the concern is on responsibility following the behavior of criminal acts. By contrast, the network information law focuses on ex ante prevention to minimize the breeding ground to the crimes by data security regulations. Using an example of cross-border data theft, the network information law requirements of data encryption can ensure that data is not stolen whilst the criminal law of the international law implicates the offenders that have already committed acts of stealing. The organic integration of punishment and prevention is achieved with the complementary functions of the two fields.In the "Apple attack on China's national timing center case", the rules stipulated in the Cyber Information Law regarding the encrypted storage of critical infrastructure data and the management of access rights can prevent the exploitation of vulnerabilities and data theft at the source; while international

DOI: 10.54254/2753-7048/2026.ZJU31772

criminal law can hold hackers criminally accountable for their attacks, forming a closed loop of prevention, joint punishment and deterrence.

Rules such as "data control place" and "core act place" in network information law can make up for the deficiencies in jurisdiction determination of international criminal law and provide support for it. The standards for preserving electronic evidence in network information law also provide a technical basis for the admissibility of evidence in international criminal law. For instance, the "data processor liability" clause in GDPR provides a rule reference for international criminal law to identify the criminal liability of platforms. Regarding the "Google Company's US-Russia Data Compliance Conflict Case", the rules in the Cyber Information Law regarding the cross-border data provision obligations of data controllers and the special protection of critical data can clearly define the compliance boundaries of Google as a data controller in different jurisdictions, providing a rule basis for the international criminal law to determine whether it constitutes an accomplice.

3.2. Practical basis for connection

In terms of international conventions, the Budapest Convention on Cybercrime already contains provisions regulating data-related matters. For example, Article 18 stipulates rules for cross-border collection of electronic evidence, providing a basic framework for the connection between the two legal fields. Although this convention has not fully resolved the issue of sovereignty conflicts, it has reflected the idea of coordinated governance and embodied the embryonic form of connection [5].

Meanwhile, some countries have carried out connection practices and accumulated certain experience. For example, Article 74 of China's Cybersecurity Law clearly stipulates the criminal liability clauses for cybercrimes, directly connecting network information law with criminal law. The United States' CLOUD Act allows domestic law enforcement agencies to access electronic data stored overseas, realizing the connection between data rules and criminal law enforcement. These practices have provided references for resolving jurisdictional conflicts in the "Apple Hacking Case" and for determining corporate liability in the "Google Data Compliance Case".

International organizations such as the United Nations Open-ended Working Group on Cybersecurity and the European Cybercrime Centre (EC3) have continuously promoted the coordination between data governance and transnational crime governance. The European Electronic Evidence Exchange Platform established by EC3 has realized the connection between data standards of network information law and the needs of criminal evidence, providing an ideological template for the construction of coordinated platforms. The operation mode of this platform can provide a reference for solving the cross-border evidence retrieval problem in the "Apple Hacking Case".

4. Specific connection paths between the two legal fields under data sovereignty conflicts

4.1. Connection at the rule level

To improve the compatibility of jurisdiction rules, it is necessary to clearly define the standards and priority order and set reasonable exceptions. The rules of data control and core behavior in network information law should supplement the jurisdiction principles of international criminal law and establish a jurisdiction system of "priority for general circumstances + exception for special circumstances". For ordinary cross-border network crimes, the dual dominant principle of "core criminal behavior occurrence location + key data control location" should be applied as the primary rule. These two locations are the core connection points of crime implementation and harmful

DOI: 10.54254/2753-7048/2026.ZJU31772

carriers and can directly obtain evidence and lock down the responsible party. If the core behavior location is difficult to determine due to technical concealment (such as using floating IP or overseas servers), or the key data is scattered and stored in multiple countries, the "victim country" (including the location of the victim, the main location of the harm occurrence) can be used as a supplementary jurisdiction basis to solve the overlapping problem of simultaneous jurisdiction claims by multiple countries in the "WannaCry" case [6]. For cross-border network crimes in key infrastructure fields like the "Apple attack on China's national time center case", the victim country should have absolute jurisdiction priority. The key infrastructure location and the location of the core attack instruction issuance should be the first priority jurisdiction basis. At the same time, the jurisdiction over crimes related to key data leakage should be exclusively granted to the victim country, as such crimes directly threaten national security and public interests, and the jurisdictional needs of the victim country have priority. People can set two types of exceptions: the first is the "prior handling exception", if among multiple countries with jurisdiction, a certain country has taken the lead in filing a case and has substantially advanced evidence fixation, suspect control, etc., and does not affect the fair trial of the case, following the principle of "prior handling being superior", the country should continue to exercise jurisdiction, avoiding waste of judicial resources and procedural conflicts; the second is the "major interest exemption exception", if the country where the suspect belongs claims jurisdiction based on personal jurisdiction, and the case involves the country's major national security interests, and at the same time promises to guarantee the core demands of the victim country (such as sharing evidence, extraditing the suspect), after consultation and agreement among relevant countries, the case can be transferred to jurisdiction, but it must be on the premise of not harming the major interests of the victim country. In addition, for crimes such as cyber terrorism that harm the common interests of humanity, or cross-border large-scale data theft, the universal jurisdiction principle can be limitedly applied as a supplement, and international organizations can coordinate capable countries to exercise jurisdiction, but it must comply with the relevant provisions of the "Rome Statute" to avoid the abuse of universal jurisdiction. This hierarchical and exception-based jurisdiction rule can not only solve the jurisdiction conflicts of ordinary cross-border network crimes but also respond to the special needs of key infrastructure protection, while balancing judicial efficiency and national sovereignty, providing clear basis for cross-border law enforcement cooperation.

To optimize the connection of evidence rules, it is essential to unify the admissibility standards. Drawing on the standards for the preservation, storage and transmission of electronic evidence in network information law, a unified international admissibility rule for cross-border electronic evidence should be constructed. It is necessary to clarify that electronic evidence must meet three requirements: originality verification, whole-process traceability and subject authentication. Address the GDPR to accomplish and safeguard data transportation, prospect and control, and rights of subjects, a standard format and authorization system of cross-border transmission of electronic evidence is recommended to enhance the evidence acceptance rate [7]. This rule will be helpful in addressing the issue of the acceptance of evidence in the case of Apple Hacking, which is the variation in the standards of electronic evidence across different states, and make sure that the validity of the evidence, including attack logs and vulnerability exploitation tools that are cross-borders retrieved, meets the standard.

To increase the similarity of liability regulations, it is crucial to delineate the responsibility boundaries, define the exemptions of compliance of enterprises and situations of determining the liability and harmonizing rights and obligations. The security and data protection liability of network service providers as per the cyber information law must be added to the international criminal

DOI: 10.54254/2753-7048/2026.ZJU31772

liability model and a logical series of obligation-responsibility-exemption logically constructed. Particularly, platforms that do not meet its legal obligations (i.e. data tracking and warning against risks) and allow criminal attacks or worsen damages should be jointly liable. Technical providers who either knowingly assist in cross-border cybercrimes through program creation, or leasing of servers shall be classified as accomplices addressing the blurry division of liability between platforms and technical actors in the case of the Facebook Data Scandal. In multinational data controllers involved in such dilemmas as Google U. S. -Russia Data Compliance Conflict Case, specific limits of compliance exemptions and liability should be established. The exemptions are available when the enterprises have installed proper cross-border data compliance review systems, have completed reasonable verification obligations on outbound requests of data and cannot objectively give data because of sovereign conflicts (e.g. Country A requires data to be localized, whereas Country B requires disclosure to be made across borders) without resulting in loss of evidence or delay of investigations. On the other hand, those who decide to defraud laws by modifying data storage sites, erasing records, or avoiding inspections and thus causing loss of evidence, warrants, or participating in other harmful acts, will be held responsible in corresponding criminal liability. This will provide multinationals with a distinct direction on compliance and eliminate the tendency of them to avoid liability by taking advantage of conflicts in regulations, thereby making the liability rule alignment functional and equitable.

4.2. Connection at the mechanism level

In order to revise the convention system, it is required to encourage the rewriting of the Budapest Convention on Cybercrime and including such provisions as coordination of data sovereignty, as well as defining the principle of balancing the data localization and cross-border evidence collection. It is also recommended that special convention on transnational cybercrime governance be developed where the connection content should be included at the level rule in the convention to establish common international norms. Critical infrastructure case and multinational enterprise data compliance Special conventions must provide clear legal footing on the issues such as cross-border cybercrimes, and specific rules to resolve cases such as the cases proposed by the article on the Apple Hacking Case as well as the Google Data Compliance Dispute Case.

A rapid-track mechanism of gathering evidence must be put up to determine standardization in the process of evidence collection on the basis of cross-border data flow regulation of the network information law where emergency cases should have a response of collection of evidence within a 48 hours. This needs to establish a platform of international criminal intelligence sharing, which is integrated via the data sharing format and achieves real-time intelligence sharing, based on the experience of the EC3 platform. The nature of attacks and details of hacker groups in international cybercrime can be rapidly shared through this platform and thus will increase efficiency in collaboration.

A professional platform would be created by deploying a body named the Committee of resolution of disputes around data sovereignty as well as transnational cybercrimes under the United Nations with the leadership of legal experts and technical experts to facilitate the conflicts of jurisdiction and legal application of the law. It should have a system of precedent guidance in which the results of the handling of the common cases of disputes should be published as a guideline to be followed in future cases.

DOI: 10.54254/2753-7048/2026.ZJU31772

4.3. Connection at the implementation level

There is the need to encourage creation of routine communication system between law enforcement agencies in China and the United States on cybersecurity, including Cybersecurity Bureau of the Ministry of Public Security of China and Cyber Division of the FBI of United States and conduct transnational law enforcement collaboration conferences yearly. The system of joint investigation of law enforcement agencies of several countries should be provided in the key transnational cases of cybercrime. Where the case is crucial, like the one involving the breach of the national time-keeping center of China by Apple, a joint task force system can be implemented to bring together the police forces of different nations to carry out the investigations collaboratively. In this platform, the nature of the attacks and the details warning of hacker groups in cross border cyber crimes can be shared fast, hence increasing effectiveness of cooperation.

The use of blockchain technology must form an electronic evidence depository platform across the border to achieve the decentralized storing of and traceability of the entire evidence process electronically. Apply the benefits of automation of the artificial intelligence technology in a rational way to develop a risk early warning model of cross-border cybercrimes and incorporate data monitoring indicators in network information legislation to initiate early warning of the risk of crimes and enrich the effort of governance [8]. Observable digital evidence protection platform can protect the security and integrity challenge of the cross-border transmission of electronic evidence in transnational crimes whereas the early warning system can help multinational corporations and law enforcement agencies mitigate the chances of safeguarding similar vulnerability attacks preemptively.

Develop recidivism standards of the cross-border online platforms, whereby the enterprises need to conform with the regulations of international criminal law, as well as the implementation of data under cyber information law, and introduce a two-facet systemization of data security auditing and crime risks tracking. In the case of audits, it is required that full-process checks on cross-border data storage, transmission, and processing are done on a regular basis, they keep audit logs, and they demand that third-party compliance with audits be checked yearly with verifiable statements. To be monitored, construct an AI-drived early warning real-time platform to monitor the abnormal data streams, establish a graded warning mechanism to automatically prevent high-risk behaviors and save evidence, and clearly define monitoring limits and response time conditions to detect criminal indications in time [9]. The rules must specify courses of compliance in cases of disagreement in data sovereignty (e.g., two-way systems of local data warehousing and international statement) to eliminate paradoxes such as those which Google is experiencing. Incentivize compliance via streamlined outbound security assessments and whitelist inclusion, while imposing joint penalties (market access restrictions, heavy fines) on non-compliant enterprises to drive active governance and fulfillment of main responsibilities [10].Enterprises must also fulfill strict data monitoring obligations and report cybercrime clues promptly, forming a closed-loop system that balances data sovereignty protection and transnational cybercrime governance.

5. Conclusion

Adopting a combination of normative analysis, case analysis and comparative research methods, this paper systematically expounds the connection logic and specific paths between international criminal law and network information law, focusing on the governance of transnational cybercrimes under data sovereignty conflicts. The study finds that data sovereignty conflicts trigger governance dilemmas in three dimensions: jurisdiction, rule application and law enforcement cooperation.

DOI: 10.54254/2753-7048/2026.ZJU31772

International criminal law and network information law have synergistic and relevant foundations in terms of objectives, functions and rules, while international conventions, domestic legislation and the practices of international organizations constitute the practical support for their connection. On this basis, a complete connection system can be formed by clarifying the connection standards for jurisdiction, evidence and liability at the rule level, constructing legislative coordination, law enforcement cooperation and dispute resolution mechanisms at the mechanism level, and strengthening institutional cooperation, technical connection and enterprise compliance at the implementation level.

The theoretical contribution of this study lies in constructing a systematic framework for the connection between the two legal fields, addressing the deficiencies in existing research. The practical value lies in providing an operational solution to the governance challenges of typical cases such as "Google's US-Russia data compliance conflict case", "Apple's attack on China's national time-keeping center case", "WannaCry case", and "Facebook data scandal". Future research can further focus on regional legal connection issues under the background of the "Digital Silk Road" and refine the connection paths in combination with specific regional practices. Meanwhile, with the application of artificial intelligence technology in cybercrimes, attention should be paid to the new challenges and opportunities brought by technological development to legal connection, and it is necessary to ensure the transparency and standardized supervision of the application of artificial intelligence technology, so as to continuously improve the governance system.

References

[1] Ambrose, B.K. (2025) The inadequacy of international humanitarian law in regulating cyber warfare: A critical analysis of the Geneva Conventions and additional protocols. East African Journal of Law and Ethics, 8(1), 418-433.
[2] Li, W. and Chen, J. (2024) From brussels effect to gravity assists: Understanding the evolution of the GDPR-inspired personal information protection law in China. Computer Law & Security Review, 54, 105994.
[3] Kipande, C. (2025) Cross-Border data flow restrictions: a threat to digital evidence integrity in cybercrime investigations in Tanzania. East African Journal of Law and Ethics, 8(1), 460-474.
[4] Zuo, Z. (2024) Cross-Border Data Forensics: Challenges and strategies in the Belt and Road Initiative Digital Era. Asian Social Science, 20(2), 49.
[5] Shyshenko, A.A. (2025) Digital evidences in criminal proceedings: problems of authenticity and admissibility. Analytical and Comparative Jurisprudence, 3(5), 315-321.
[6] Dash, S. and Tiwari, I. (2025) Safeguarding digital Trust: Corporate negligence and White-Collar accountability in India’s data protection framework. International Journal for Multidisciplinary Research, 7(6).
[7] Moreira, H.F.M.A. (2023) Governing knowledge and technology: European approach to artificial intelligence.
[8] Piddubna, A.V. and Bozhuk, K.O. (2025) Artificial intelligence in criminal proceedings: modern challenges and legal perspectives. Analytical and Comparative Jurisprudence, 3(5), 234-238.
[9] Yao, H. (2025) Research on the Construction of a Financial and Accounting Supervision System in Universities from a Governance Perspective. International Business & Economics Studies, 7(6), 1.
[10] Abbasi, Z. (2025) Legal education in the age of generative artificial intelligence. Law Technology and Humans, 7(3), 1-4.