Vol.6 Iss.4 2025
Modern Law Research
https://doi.org/10.37420/j.mlr.2025.027

Cross-Border Cybercrime Digital Evidence: Current Research and Fundamental Categories

Chang Guan*
School of Foreign Languages, Beijing Institute of Technology, Beijing, China
***Corresponding author E-mail:13939020675@163.com**

Abstract

Cross-border cybercrime has intensified the challenges surrounding the acquisition, preservation, and admissibility of digital evidence. Characterized by deterritorialization, volatility, and technological dependence, digital evidence underpins the investigation and adjudication of cyber offenses but is constrained by obstructed access, fragmented standards, and sovereignty conflicts. This article reviews the current state of research and practice, analyzing international and domestic legal frameworks, as well as academic debates on legality, relevance, and scientific reliability. It further outlines a structured typology of nine categories of digital evidence, ranging from communication records and financial transactions to malware, metadata, and deepfake content. By mapping these categories and their evidentiary implications, the study provides a conceptual foundation for comparative legal inquiry and highlights the need for interdisciplinary research and cross-border cooperation to address the evolving complexities of digital evidence.

Keywords

admissibility, cross-border cybercrime, digital evidence, international cooperation

1 Introduction

Cross-border cybercrime is characterized by virtuality, deterritorialization, and high accessibility, which significantly lower the cost of commission and foster the expansion of illicit digital economies across jurisdictions. Its evidentiary dimension is centered on electronic data, which underpins the processes of collection, preservation, and adjudication. Yet, in cross-border contexts, digital evidence is confronted with systemic challenges, including obstructed access, disrupted chains of custody, and divergent standards for admissibility. At the international level, cybercrime is alternately defined as a category of offenses enabled by information and communication technologies or as a digital extension of traditional crimes. Both perspectives highlight the tension between the deterritorialized nature of cyberspace and the territorial principles of jurisdiction under international law.

The rapid iteration of emerging technologies further complicates the evidentiary landscape. Artificial intelligence has enabled increasingly personalized phishing and social engineering attacks. Deepfake-generated audio and video content undermines the assessment of authenticity. The proliferation of insecure Internet of Things (IoT) devices expands the attack surface. “Cybercrime-as-a-Service” lowers entry barriers while amplifying the frequency and complexity of incidents. Ransomware has evolved into “double extortion” models that

threaten critical infrastructure. Immersive environments such as the metaverse generate new forms of crime with unique evidentiary challenges, while the dark web facilitates anonymous transactions and the circulation of criminal tools, increasing the costs of tracing and attribution.

Against this backdrop, traditional approaches that rely on the state of data storage and on conceptions of evidence modeled on physical objects have proven inadequate for addressing what may be termed a "highly dynamic, adversarial, and multi-node evidence ecology." The pressing challenge, therefore, is to reconcile sovereignty concerns and rights protection with the effective acquisition, scientific preservation, and reliable adjudication of cross-border electronic data. This article takes the notion of "full-process applicability" as its organizing framework: on the one hand, it identifies structural obstacles across the three stages of acquisition, preservation, and evaluation; on the other, it employs comparative legal analysis and a review of the literature to map the current state and basic categories of digital evidence, thereby providing a theoretical foundation for further transnational institutional and academic inquiry.

2 Literature Review

The literature on cross-border digital evidence has expanded considerably in recent years, reflecting both regulatory developments and scholarly debate. Existing contributions can broadly be divided into two strands. The first examines institutional and legal frameworks at the international, regional, and domestic levels, highlighting diverse regulatory models and their implications for sovereignty, efficiency, and rights protection. The second explores academic perspectives that analyze digital evidence through the lenses of legality, relevance, and scientific reliability, underscoring the conceptual and procedural challenges that shape its evidentiary value. Together, these strands provide a comprehensive view of the current state of research and practice, offering a foundation for further theoretical and comparative inquiry.

2.1 Global Legal Frameworks

The regulation of digital evidence in cross-border cybercrime has developed along diverse trajectories worldwide. At the international level, negotiations on the Second Additional Protocol to the Budapest Convention highlight tensions between enabling direct cross-border access to data and safeguarding state sovereignty. Within the European Union, the framework has evolved around the European Investigation Order, supplemented by preservation and production orders, which allow law enforcement to request data directly from service providers. While these instruments improve efficiency, they have also raised concerns regarding privacy and sovereignty. In the United States, the CLOUD Act establishes a "data controller" standard, requiring service providers under U.S. jurisdiction to disclose data regardless of its storage location, and is supported by bilateral agreements. Although effective in expanding access, this approach has been criticized for its unilateral tendencies. In comparison, China recognizes electronic data as an independent category of evidence under its Criminal Procedure Law and emphasizes the use of mutual legal assistance as the exclusive channel for cross-border evidence gathering, further detailed through judicial interpretations. Taken together, global regulatory models demonstrate a trend toward coexistence of territorial and personal jurisdiction, and a balance between unilateral mechanisms and multilateral cooperation, with each jurisdiction

adopting distinct approaches to reconcile efficiency with legality.

2.2 Scholarly Literature Review

From the current state of research, scholarly attention on cross-border digital evidence has gradually shifted from substantive criminal regulation to issues of criminal procedure, with particular focus on its applicability in the stages of collection, preservation, and adjudication. Around this core concern, existing scholarship has concentrated on three dimensions: legality, relevance, and scientific reliability. These dimensions reflect not only the tension between cross-border cybercrime and state sovereignty or normative frameworks, but also the practical conflicts between evidentiary efficiency, probative value, and procedural safeguards in judicial practice.

2.2.1 Legality Perspective

Legality remains the central concern in discussions of cross-border electronic evidence, with scholarly debates primarily focusing on three dimensions: state sovereignty, procedural safeguards, and the exclusion of unlawfully obtained evidence. The inherent tension lies in the cross-border flow of electronic data, which challenges the territorial limits of sovereignty. For example, the Microsoft Ireland case demonstrated how attempts by one jurisdiction to compel disclosure of data stored abroad raise questions about the extraterritorial application of domestic law. Divergent approaches to jurisdiction—some prioritizing the "location of storage" principle and others emphasizing "location of control"—have made consensus on cross-border evidence gathering particularly difficult.

From a procedural standpoint, the traditional Mutual Legal Assistance Treaty (MLAT) system has been criticized for inefficiency, often resulting in delays that render data unusable; empirical studies suggest that requests from European Union member states to the United States may take up to ten months, by which time the requested data may no longer be available. In response, scholars have proposed mechanisms such as expedited procedures for urgent cases, streamlined "fast-track" channels, and the negotiation of bilateral or multilateral instruments to balance sovereignty with efficiency.

The key challenge lies in reconciling sovereignty concerns with the need for timely access to evidence. Literature warns that neglecting principles of sovereignty and proportionality in institutional design could not only trigger diplomatic disputes but also exacerbate conflicts among competing jurisdictional models, thereby undermining the foundations of international cooperation. Achieving rapid evidence access while respecting sovereignty remains a central unresolved issue in the governance of cross-border digital evidence.

2.2.2 Relevance Perspective

Relevance is a fundamental requirement for the probative value of electronic evidence and a critical condition for the acceptance of cross-border evidence in international proceedings. Scholarly debates have largely concentrated on three issues. First is the correspondence between evidentiary content and the facts of the case. Given the complexity of digital data sources, insufficient scrutiny of relevance risks "over-col-

lection," which not only increases judicial burdens but also undermines evidentiary reliability. Second is the alignment of cross-border data with domestic judicial needs. The frequent separation of data storage locations from the locus delicti makes it difficult to narrowly tailor evidence requests. Overly broad demands, sometimes extending beyond what is necessary for adjudication, risk eroding trust between cooperating jurisdictions. Third is the scope of applicability for different methods of evidence gathering. New techniques such as remote forensics and online data extraction may improve efficiency, but they also risk bypassing established procedural safeguards, raising disputes over whether the evidence meaningfully connects to the alleged facts.

The key challenge lies in the absence of harmonized standards for assessing relevance across jurisdictions. Without clear criteria or tiered mechanisms for evidence requests, cross-border cooperation remains vulnerable to inefficiencies and conflicts. Scholars have argued that proportionality should serve as a guiding principle to limit the scope of data requests, ensuring that only information with substantial connection to the case is collected. Further, evidentiary rules should define the standard of relevance more precisely, specifying conditions for different categories of electronic data, and adopting stratified approaches to enhance operational clarity. Only under such conditions can cross-border electronic evidence attain real probative value while reducing friction in international cooperation.

2.2.3 Scientific Reliability Perspective

Scientific reliability constitutes the foundation for determining whether cross-border electronic data can serve as admissible and probative evidence. At its core lies the requirement that data must remain consistent and authentic throughout the processes of collection, preservation, and examination, so as to prevent distortion or exclusion caused by technical flaws or inadequate legal safeguards. Scholarly debate has focused on three principal aspects. First, the technical rigor of collection methods. While emerging techniques such as remote forensics and real-time transmission have enhanced efficiency, their lack of clear statutory authorization raises concerns about procedural legitimacy. Second, the integrity of data preservation. Because electronic data are inherently malleable and easily replicable, their credibility is vulnerable if not promptly secured. Measures such as hash verification, audit logs, and the use of write-once media are widely recommended to ensure continuity of the evidentiary chain. Third, the objectivity of forensic examination and verification. Current practices often emphasize "integrity" at the expense of authenticity and legality, creating an overreliance on formalistic checks and undermining substantive reliability.

The prevailing challenge lies in bridging the gap between evolving technical safeguards and the legal frameworks that regulate them. A disproportionate focus on integrity—without corresponding attention to authenticity and legality—risks reducing evidentiary review to a formal exercise, thereby weakening the substantive probative value of digital evidence. Future institutional design must therefore integrate advanced technical protocols with balanced rules that jointly secure authenticity, integrity, and legality. Only through such a framework can cross-border electronic evidence achieve both scientific robustness and procedural legitimacy.

3 Ontological Structure of Digital Evidence in Cross-Border Cybercrime

As the key medium for uncovering facts in cross-border cybercrime, the ontological structure of digital evidence can be defined at both the conceptual and typological levels. Conceptually, digital evidence refers to data in electronic form that can demonstrate the commission of cybercrime and related facts. Unlike traditional physical or documentary evidence, it is shaped by information technologies and thus exhibits distinctive attributes of virtuality, volatility, and transnationality. Typologically, digital evidence requires systematic classification to provide a foundation for subsequent evaluation and institutional design. Scholarly literature generally identifies nine categories: (1) communication evidence, (2) network evidence, (3) transactional evidence, (4) digital media evidence, (5) malicious software and tool evidence, (6) user activity evidence, (7) metadata and digital traces, (8) volatile and persistent evidence, and (9) emerging deepfake evidence.

A structured taxonomy of these categories not only facilitates understanding of the behavioral patterns and technical features of cross-border cybercrime but also provides theoretical support for the development of standards of judicial review and mechanisms of international cooperation. Accordingly, any further examination of evidentiary issues in cross-border cybercrime must begin with a clear conceptualization and classification of digital evidence, so as to delineate its essential structure and characteristics and to lay the groundwork for deeper analytical inquiry.

3.1 The Basic Concept of Digital Evidence

Digital evidence arises from different manifestations of cybercrime. Cybercrime is commonly divided into two broad categories: crimes that are dependent on digital networks and crimes facilitated by them. The first category refers to offenses that can only be committed through the use of computers, networks, or other information and communication technologies (ICTs). Such crimes directly target ICT systems, such as hacking, deploying malicious software, and ransomware attacks. By contrast, network-facilitated crimes involve the use of digital technologies to expand or intensify traditional criminal activities, such as phishing-based fraud, online grooming, or the distribution of child sexual abuse material. This distinction is essential for understanding the diverse nature of cyber threats and for developing targeted enforcement strategies.

When combined with cross-border elements, cybercrime generates a wide range of specific offenses, including financial fraud (such as phishing schemes, online investment scams, business email compromise, credit card fraud, and cryptocurrency-related fraud), ransomware attacks (often employing “double extortion” strategies by encrypting data and threatening disclosure), data breaches, online child sexual exploitation and abuse (OCSEA), cyber espionage, distributed denial-of-service (DDoS) attacks, the creation and dissemination of malicious software, intellectual property violations, cyber terrorism, human trafficking, and online gambling.

Digital evidence has become indispensable for revealing the facts underlying such cross-border cybercrimes. Conceptually, digital evidence refers to data that exists in electronic form and is capable of demon-

strating the occurrence of cybercrime and related facts. Unlike physical or documentary evidence, digital evidence is technologically mediated, represented in binary form, and characterized by its virtual, volatile, and cross-border attributes (Zheng, 2024). It encompasses information stored or transmitted through computer systems and network devices, as well as data recovered, extracted, or reconstructed using forensic technologies. In essence, digital evidence represents the informational trace of how cybercrime occurs, evolves, and produces consequences.

From an external perspective, digital evidence in cross-border cybercrime can be broadly classified into three functional categories:

Behavioral evidence, such as intrusion logs, malicious code, communication records, and user login trails, which establish the existence of specific attacks or fraudulent activities;

Financial evidence, such as online payment records, cryptocurrency transaction logs, and cross-border transfer vouchers, which reveal the flow of illicit funds and potential money-laundering pathways;

Supporting evidence, such as domain registration data, server logs, database files, and email archives, which demonstrate organizational structures and operational mechanisms.

Beyond these categories, scholarship has proposed more systematic taxonomies from the perspective of information ecosystems. Digital evidence is no longer confined to traditional electronic records, but now includes new forms generated by emerging technologies, such as blockchain-based evidence, algorithmic evidence, and simulation-based evidence.With continuous technological innovation, digital evidence has evolved into diverse forms, encompassing electronic, blockchain-based, big data, AI-driven, and virtual simulation evidence.

A clear conceptualization of digital evidence—both in terms of its intrinsic definition and its external typologies—not only sharpens scholarly understanding of its scope and attributes but also provides a theoretical foundation for establishing standards of judicial review and developing mechanisms of cross-border cooperation.

3.2 Classification and Forms of Digital Evidence

As the central medium for uncovering criminal facts, digital evidence requires systematic classification to ensure admissibility and facilitate cross-border judicial cooperation. In the context of cybercrime—where transnationality, virtuality, and technological dependence make governance especially challenging—a clear typology of digital evidence is critical. Common examples include emails, text messages, social media activity logs; computer files, images, and videos; internet search histories and browsing data; IP addresses and network logs; metadata; malicious software samples; financial transaction records and cryptocurrency data; communication and call logs; geolocation information; cloud storage and IoT device data; encrypted or deleted files; network traffic captures, system images, and memory dumps; as well as digital signatures, authentication records, and deepfake-generated audio or video.

Scholarly literature generally identifies nine categories that capture the multi-layered nature of digital evi-

dence:

(1)Communication and network evidence: including instant messaging, emails, and call records, which reflect interactions among actors; and IP addresses, routing logs, and traffic monitoring, which reveal data transmission pathways and the technological environment.

(2)Transactional and digital media evidence: transactional evidence covers electronic payments, cryptocurrency transfers, and online purchase records, reflecting financial flows; digital media evidence encompasses images, audio, video, and documents, offering direct factual representation.

(3)Malware and tool evidence, user activity evidence, and metadata or digital traces: malware samples reveal the technical tools employed; user activity data, such as browsing histories and login trails, reconstruct behavioral patterns; metadata and traces embedded in files or systems substantiate authenticity and link activities to actors.

(4)Volatile and persistent evidence, as well as deepfake evidence: volatile data, such as cache or memory, is short-lived and easily lost; persistent data, such as hard drive or cloud-stored information, is more durable; deepfake evidence, generated through artificial intelligence, presents an emerging risk that directly challenges authenticity and necessitates cross-disciplinary forensic techniques.

Taken together, this taxonomy organizes digital evidence along several dimensions: mode of interaction, medium of storage, behavioral trace, temporal durability, and technological innovation. Such a framework captures both the spatial and temporal features of digital evidence and highlights how technological iteration continuously reshapes evidentiary standards within judicial systems.

3.3 Categories of Digital Evidence

Before turning to the specific categories, it is important to note that digital evidence is not monolithic but manifests across multiple dimensions of online activity and technological infrastructure. Its forms vary according to the type of interaction, the medium of storage, the trace left by user behavior, and the durability of data over time. To capture this diversity in a structured way, the following sections outline nine representative categories of digital evidence, each with distinct characteristics, probative value, and challenges for collection, preservation, and cross-border admissibility.

(1) Communication Evidence

This category includes emails, text messages, instant messaging records, social media interactions, and metadata such as transmission routes and timestamps. Communication evidence is frequently used to identify suspects, reconstruct relationship networks, and reveal contact patterns. It plays a central role in cases of fraud, online recruitment, cyberbullying, and child sexual exploitation. Its strength lies in its immediacy and ability to form core evidentiary chains. However, cross-border storage complicates access: service providers often impose short retention periods, and international retrieval depends heavily on mutual legal assistance, which increases the risk of broken chains of custody.

(2)Network Evidence

Network-based materials comprise IP addresses, server logs, and traffic capture data. These are essential for tracing hacking incidents, identifying distributed denial-of-service (DDoS) attacks, and pinpointing abnormal access activities. Network evidence provides valuable technical insights into the pathways of intrusion. At the same time, its reliability is undermined by anonymization tools such as proxies, VPNs, or Tor, which obscure attribution and weaken traceability.

(3)Transactional Evidence

This category covers bank records, electronic payment data, cryptocurrency transactions, and cross-border remittance documentation. Transactional evidence is crucial in reconstructing financial flows in cases of fraud, ransomware, and money laundering. Its advantage lies in the quantitative nature of financial trails. Yet cryptocurrency anonymization practices—such as mixing services and off-chain transactions—significantly reduce traceability, underscoring the need for advanced forensic tools and international regulatory cooperation.

(4)Digital Media Evidence

Digital media encompasses images, videos, audio files, documents, and CCTV recordings. It is highly intuitive and therefore persuasive in judicial contexts, particularly in intellectual property violations, cyberbullying, and terrorist propaganda cases. However, the ease of manipulation, including risks associated with deepfakes, challenges its authenticity. Verification through metadata analysis and expert examination is often necessary to establish reliability.

(5)Malware and Tool Evidence

This includes viruses, worms, trojans, ransomware, phishing kits, and command-and-control (C&C) server data. Such evidence directly reveals the tools and methods employed in attacks, particularly in ransomware cases. Its value lies in its ability to demonstrate modus operandi, but reverse engineering requires significant technical expertise. Moreover, once malicious infrastructure is dismantled or relocated across borders, evidence may be lost, creating preservation difficulties.

(6)User Activity Evidence

User-related data includes browsing histories, search records, GPS logs, call histories, and contact lists. These materials are frequently used to corroborate alibis, reconstruct movement patterns, and reveal networks of accomplices. While highly probative, user activity evidence implicates sensitive personal information and therefore raises concerns regarding proportionality and authorization in the process of acquisition.

(7)Metadata and Digital Traces

This evidence type comprises timestamps, authorship information, system logs, and other automatically generated data. Metadata is often hidden from users but provides crucial proof of data origin, authenticity, and behavioral reconstruction. It is relatively resistant to tampering, but inconsistencies in extraction methods across jurisdictions may lead to incomplete records and disputes over reliability.

(8)Volatile and Persistent Evidence

Volatile evidence includes cache and random-access memory (RAM), which can quickly disappear, while persistent evidence refers to data stored on hard drives or cloud servers, which remains available over time. The forensic principle of "collect volatile data before persistent data" reflects their evidentiary hierarchy. In cross-border cases, however, procedural delays often result in the loss of volatile information, leaving crucial system states unrecoverable.

(9)Deepfake Evidence

As a newly emerging category, deepfake evidence involves artificially generated audio-visual materials created through advanced machine learning techniques. Such content is increasingly used for impersonation, fraud, and disinformation campaigns. Its sophistication presents serious challenges to authenticity assessments, necessitating cross-disciplinary verification methods such as algorithmic provenance analysis and forensic imaging.

Overall, digital evidence in cross-border cybercrime is highly diverse, encompassing communication, network, transactional, media, malware, user activity, and metadata-related forms, among others. Common features across these categories include technological dependence, volatility, transnational circulation, and chain-like interconnectivity. A systematic classification of digital evidence not only contributes to greater consistency in judicial practice but also provides a conceptual foundation for cross-border cooperation and mutual recognition of evidentiary standards.

4 Conclusion

The rise of cross-border cybercrime has positioned digital evidence as one of the most complex and contested issues in contemporary legal practice. With the growing deterritorialization and accessibility of cybercrime, traditional evidentiary approaches—anchored in the physical location of data and offline investigative models—have become increasingly inadequate for managing today's fluid and multifaceted evidence ecology. Emerging technologies such as artificial intelligence, blockchain, the Internet of Things, and deepfake applications further expand both the scope and risks of digital evidence, complicating the assessment of authenticity, integrity, and admissibility.

Existing institutional and academic efforts have produced valuable insights, yet two limitations remain salient. First, legal regimes diverge considerably: the United States has emphasized extraterritorial access through service-provider obligations, while the European Union has prioritized regionalized cooperation frameworks. These divergent approaches inevitably generate tensions surrounding sovereignty and rights protection. Second, while technical discussions of forensic methods are relatively advanced, scholarship has been less systematic in addressing issues of legality, procedural safeguards, and judicial applicability. As a result, governance of cross-border digital evidence remains exploratory, lacking a universally applicable framework.

This article contributes to the field by mapping the current state of digital evidence from a full-process

perspective and by clarifying its basic categories through a structured typology. The classification—from communication records and financial transactions to user activity data and deepfake evidence—illuminates the multidimensional architecture of cross-border evidence and establishes a basis for comparative legal inquiry and future institutional design. Looking ahead, the increasing complexity of digital evidence will demand interdisciplinary perspectives and transnational cooperation. Advancing standards for the collection, preservation, and adjudication of such evidence is not merely a technical concern of criminal procedure but a critical test of whether a stable and coherent legal order can be maintained in global cyberspace.

Reference

[1]European Parliament. (2024). Cybercrime: A Multidimensional National Security Threat. Retrieved from https://www.europarl.europa.eu/RegData/etudes/BRIE/2024/760356/EPRS_BRI(2024)760356_EN.pdf

[2]FAWCO. (2025). Top Eight Cyber Crime Trends You Should Prepare for in 2025. Retrieved from https://www.fawco.org/global-issues/human-rights/cyber-crime

[3]INTERPOL. (2022, March 25). Financial and Cybercrimes Top Global Police Concerns, Says New INTERPOL Report. Retrieved from https://www.interpol.int/News-and-Events/News/2022/Financial-and-cybercrimes-top-global-police-concerns-says-new-INTERPOL-report

[4]Ng, J. (2016). International cybercrime, transnational evidence gathering and the challenges in Australia: Finding the delicate balance. International Journal of Information and Communication Technology, 9(2), 177–190.

[5]Díaz-Pérez, L. C., et al. (2022). A review of cross-border cooperation regulation for digital media. Aslib Journal of Information Management, 74(3), 367–383. https://doi.org/10.1108/ACI-01-2022-0010

[6]Sachoulidou, A. (2024). Cross-border access to electronic evidence in criminal investigations: An analysis of EU regulation. New Journal of European Criminal Law, 15(1), 25–46. https://doi.org/10.1177/20322844241258649

[7]Stoykova, R. A. (2024). A new right to procedural accuracy: A governance model for digital evidence processing. Computer Law & Security Review, 52, 105775. https://doi.org/10.1016/j.clsr.2024.105775

[8]United Nations Office on Drugs and Crime (UNODC). (n.d.). United Nations Convention against Cybercrime; Strengthening International Cooperation for Combating Certain Crimes Committed by Means of ICT Systems and for the Sharing of Evidence in Electronic Form of Serious Crimes. Retrieved from https://www.unodc.org/unodc/en/cybercrime/convention/text/convention-full-text.html

[9]Feng, J. W. (2019). The development and reflection on the cross-border electronic evidence collection system. Law Journal, 40(06), 25–26. (in Chinese)

[10]European Protection Order Regulation (EPOR). Art. 2(2).

[11]Liu, P. X. (2022). The EU's scheme on cross-border electronic evidence collection and its implications. Journal of National Prosecutors College, 30(05), 15–17. (in Chinese)

[12]United States Congress. (2017). S.2383 – CLOUD Act (115th Congress). Retrieved from https://www.congress.gov/bill/115th-congress/senate-bill/2383/text

[13]Renmin University of China Press. (2020). On Data Governance. Beijing, p. 117. (in Chinese)

[14]Chen, L. (2022). China's response to cross-border electronic evidence collection. Journal of National Prosecutors College, 30(05), 26–29. (in Chinese)

[15]Hu, M. (2025). On the ternary structure of criminal evidence in the digital age. Peking University Law Journal, 37(01), 45–64. (in Chinese)
[16]Wu, H. Q. (2024). The legal positioning and theoretical reflection on the integrity of electronic data. Journal of National Prosecutors College, 32(01), 146–160. (in Chinese)
[17]Maier, B. (2010). How has the law attempted to tackle the borderless nature of the internet? International Journal of Law and Information Technology, 18(2), 142–143.
[18]Guo, S. (2022). Data sovereignty protection in cloud storage: An analysis of blocking statutes against "long-arm jurisdiction." China Law Review, (06), 72–85. (in Chinese)
[19]Liang, K. (2019). Development trends and implications of the EU's cross-border expedited e-evidence mechanism. Journal of People's Public Security University of China (Social Sciences Edition), 35(1), 33–36. (in Chinese)
[20]Zhang, B. S. (2024). Improvement of the evidence system in the revised Criminal Procedure Law. Chinese Journal of Law, (04), 6–15. (in Chinese)
[21]Liu, P. X. (2016). Relevance of electronic evidence. Chinese Journal of Law Studies, 38(06), 178–182. (in Chinese)
[22]Xie, D. K. (2020). Rethinking and reconstructing rules on online collection of electronic data. Dongfang Law, (03), 89–100. (in Chinese)
[23]Pei, W. (2022). On remote on-site examination: An analysis based on the systematic review of investigative measures. Tribune of Political Science and Law, 40(04), 156–166. (in Chinese)
[24]Ye, Y. B. (2020). Constructing a diversified cross-border electronic evidence collection system. Journal of People's Public Security University of China (Social Sciences Edition), 36(04), 48–58. (in Chinese)
[25]Zheng, F. (2024). Digital evidence and its hierarchical review mechanism. Chinese Journal of Law Studies, 46(05), 170–173. (in Chinese)
[26]Law Enforcement Cyber Center. (n.d.). Digital Evidence. Retrieved from https://www.iacpcybercenter.org/officers/cyber-crime-investigations/digital-evidence/
[27]Chu, F. M. (2018). Three levels of authenticity of electronic evidence: An analysis based on criminal procedure. Chinese Journal of Law Studies, 40(04), 121–138. (in Chinese)
[28]Zhang, J. W. (2024). Judicial application of digital technology: Breakthrough of spatio-temporal limitations and its regulation. Rule of Law Studies, (05), 28–40. (in Chinese)
[29]Mullen, M. (2022). A new reality: Deepfake technology and the world around us. Mitchell Hamline Law Review, 48, 210–230.