Vol.6 Iss.3 2025
Modern Law Research
https://doi.org/10.37420/j.mlr.2025.020

On the Fundamental Structure and Flow Framework of Data in Cross-Border Cybercrime

Zhixi Li

School of foreign studies, University of Science and Technology Beijing, China
Corresponding author E-mail: LiZhixi357@163.com

Abstract

Data in cross-border cybercrime is primarily categorized into electronic data, traffic data, and content data. It can also be structurally divided into core versus non-core data and enterprise versus personal data, sharing essential commonalities with—yet differing from—evidence. Both domestic and international jurisdictions have established regulatory frameworks for cross-border data flows in cybercrime, which often relies on technology-driven mechanisms to facilitate data movement, exhibiting significant fluidity across diverse domains. Amid rapid digitalization, the escalating complexity and diversity of cross-border cybercrime necessitate a renewed research perspective to reexamine the role of data in criminal activities. By systematically studying data structures and flow patterns, this research aims to advance legal theory and practical guidance for combating cross-border cybercrime, contributing China's insights and solutions to global digital governance and cybersecurity.

Keywords

Cross-border cybercrime; Data structure; Data flow; National sovereignty; Technology governance

1 Introduction

On December 24, 2024, the United Nations General Assembly formally adopted the United Nations Convention against Cybercrime, the first international legal instrument addressing cybercrime and electronic evidence. Article 2 of the Convention meticulously classifies data into electronic data, traffic data, content data, and personal data, while standardizing their application in international cooperation against cross-border cybercrime. The report of the 20th National Congress of the Communist Party of China (CPC) articulated the strategic goal of "accelerating the development of a strong cyber nation and a digital China," positioning data as a foundational strategic resource in the new era. The Decision on Comprehensively Deepening Reforms and Advancing Chinese Modernization, adopted at the Third Plenary Session of the CPC Central Committee, further emphasized "building a foundational data governance system and improving mechanisms for protecting data-related rights." These top-level designs reflect data's evolution from a technical element to a core issue of national governance. Regulating cross-border data flows and combating cybercrime present dual challenges to modernizing the rule of law amid China's digital transformation.

Driven by global digitalization, the proliferation of information networks and frequent cross-border exchanges have intensified cybercrime. According to 2023 statistics from the United Nations Office on Drugs and Crime (UNODC), global cybercrime is growing at an annual rate of 15%, with cross-border offenses exceeding 60% of cases. Such crimes transcend geographical boundaries, characterized by global reach, cross-jurisdictional complexity, and covert operations, posing unprecedented challenges to national legal systems. This paper systematically examines data structures and flow paradigms to strengthen legal frameworks and offer practical strategies against cross-border cybercrime.

2 Data Structure and Interrelationships in Cross-Border Cybercrime

A thorough deconstruction of data architecture and interrelationships in cross-border cybercrime necessitates: First, clarifying the functional attributes of three core data types—electronic data, traffic data, and content data—while elucidating their pivotal role in criminal investigations and the inherent challenges in cross-border evidence collection. Second, systematizing the binary classifications distinguishing core data from non-core data and enterprise data from personal data. Finally, analyzing the intrinsic relationship and legal boundaries between data and evidence, thereby delineating statutory pathways and review standards for transforming data into judicial evidence.

2.1 Classification of Core Data Types

In judicial practice concerning cross-border cybercrime cases, diverse data types are involved. Based on their nature and legal significance, these may be categorized as follows.

2.1.1Electronic Data

As the most fundamental and widely utilized data type, electronic data is explicitly recognized as statutory evidence under China's Criminal Procedure Law and its ancillary regulations. Per the Provisions on Several Issues Concerning the Collection, Extraction, and Review of Electronic Data in Criminal Cases, electronic data refers to "information generated during the occurrence of a case, stored, processed, or transmitted in digital form, capable of proving facts pertinent to the case." This definition is highly inclusive, encompassing not only traditional electronic files (e.g., documents, images, audio/video) but also records generated through network activities, such as user registration details, electronic transaction logs, and digital certificates. Technically, electronic data relies on external storage media (e.g., hard disks, servers) and internal data carriers, with its generation, storage, and transmission necessitating computer information systems.

In criminal judicial practice, electronic data often serves as pivotal evidence for uncovering criminal facts. For instance, in cross-border telecommunication fraud cases, chat logs of criminal syndicates, transaction platform fund flows, and fraudulent website content all exist as electronic data. Such data directly demonstrates core aspects of criminal acts—including execution processes, participants, and fund trajectories—and may even prove the nature of criminal tools (e.g., program code for illegal system intrusion or virus-distributing files). However, its susceptibility to tampering poses challenges to authenticity and integrity during cross-border evidence collection and judicial review, requiring specific technical measures and legal procedures to ensure evidentiary validity.

2.1.2 Traffic Data

As a critical subset of electronic data, traffic data primarily comprises metadata recording communication processes, network activities, or user behaviors—excluding the substantive content of communications. Examples include communication records, login logs, user registration details, and IP addresses. Although devoid of specific informational content, embedded elements like timestamps, transmission paths, and device identifiers play a key role in tracing criminal trajectories, identifying perpetrators, and linking discrete criminal activities. In cross-border cybercrime investigations, the value of traffic data is particularly pronounced: Primarily, analyzing IP address geolocations or device MAC addresses can pinpoint suspect activity zones, providing geographical leads for cross-border inquiries. Secondarily, user accounts and access permissions in login logs may reveal organizational hierarchies and role distributions within criminal groups. Tertiary, traffic data such as login records from identical devices can connect distinct criminal acts (e.g., fraud and money laundering), reconstructing end-to-end crime chains.

2.1.3 Content Data

Content data focuses on the substantive content of communications or files, directly reflecting ideational exchanges and information conveyance. Under the Electronic Data Provisions, web content, instant messaging text, and electronic document specifics qualify as content data. Compared to traffic data, content data carries heightened privacy expectations, leading most jurisdictions to impose strict cross-border access constraints (e.g., heightened warrant requirements or explicit user consent). In cross-border cybercrime cases, content data constitutes core evidence for establishing criminal intent and circumstances. Examples include fraudulent scripts in chat logs, operational assignments within criminal syndicates, or attack plans in encrypted emails of terrorist organizations—all directly material to determining criminal culpability. Furthermore, analyzing content data such as incendiary forum posts by suspects can substantiate mens rea (criminal intent).

2.2 Binary Data Structures

2.2.1 Core Data vs. Non-Core Data

Within the data architecture of cross-border cybercrime, core data and non-core data are distinguished by their functional significance in proving criminal conduct. Core data directly substantiates elements of a crime and serves as a decisive factor for conviction and sentencing. Examples include criminal toolkits (e.g., malware), critical login logs, and operational planning records. Its absence may preclude the establishment of material facts. In contrast, non-core data primarily corroborates contextual details (e.g., surveillance footage from crime scenes, suspects' routine communications) but cannot independently prove guilt. It reinforces evidentiary integrity by mutually validating core data.

The interplay between these categories operates across three dimensions. The first is foundational primacy. Core data anchors the factual framework of a case, while non-core data provides contextual enrichment. For example, in cross-border money laundering, bank transaction records (core data) directly evidence illicit flows, whereas account holders' communications (non-core data) corroborate the unlawful nature of these transactions. The second is contextual fluidity. The boundary between core and non-core data is dynamic. As investigations progress, non-core data may transition to core status—such as when a suspect's social media activity reveals a criminal syndicate' s operational base. The third is synergistic reconstruction: Integrating both categories enables comprehensive crime scene reconstruction. Judicial authorities leverage this synergy to lawfully and sufficiently establish all elements of the offense.

2.2.2. Enterprise Data vs. Personal Data

The interaction between enterprise data and personal data in cross-border cybercrime underscores how criminal acts violate distinct rights. Enterprise data—encompassing trade secrets, customer information, and financial records—constitutes core competitive assets and is frequently targeted by criminal groups. Personal data (i.e., natural persons' identifiable information) serves dual roles: as a target of crime (e.g., stolen for identity fraud) or a tool facilitating offenses (e.g., synthetic identities for scams).

These categories exhibit significant entanglement. On the one hand, enterprise systems often store substantial personal data; breaches thus simultaneously compromise both (e.g., employee records exposed during corporate espionage). On the other hand, criminal acts may involve illegal processing of both types—e.g., hacking enterprise servers to steal trade secrets often accesses employees' personal data. China' s Data Security Law (DSL) and Personal Information Protection Law (PIPL) mandate balanced protection for both. Judicial authorities must ensure lawful processing while safeguarding enterprise and personal data security during investigations.

2.3 Data and Evidence: Intrinsic Commonalities and Distinctions

Evidence and data share an essential commonality as value carriers for establishing criminal facts. Data serves as the digital manifestation of evidence, while evidence represents the functional realization of data within judicial domains. In cross-border cybercrime cases, electronic data, traffic data, and content data ultimately serve as evidence submitted to judicial authorities to substantiate criminal processes and consequences. From an information theory perspective, data acquires legal significance as evidentiary information through technical extraction and analysis—both derive core value from revealing case facts. Crucially, however, data's transformation into evidence requires statutory collection procedures and judicial review to ensure lawful sourcing and factual relevance. Illegally obtained data, even if authentic, may be excluded due to procedural violations.

Notwithstanding these commonalities, data and evidence exhibit fundamental distinctions in legal attributes and functional positioning. First, data constitutes an objectively existing information carrier lacking inherent evidentiary validity per se. Evidence, conversely, denotes data judicially authenticated to prove case facts, possessing definitive legal attributes. The conversion of data into evidence necessitates compliance with statutory procedures and standards—a process reflecting law's selective evaluation of objective facts. Second, data encompasses a broader scope including irrelevant information, whereas evidence exclusively denotes case-relevant data with probative value. Investigative agencies collect substantial data, yet only a subset attains evidentiary status. For example, in cross-border online gambling investigations, user registration data from gambling platforms may be obtained, but solely gambling-related user data qualifies as evidence; unrelated personal information remains non-evidential. Third, data processing emphasizes technical operations (e.g., extraction, recovery, analysis), while evidence handling focuses on legal determinations (e.g., admissibility review, probative value assessment). In cross-border cybercrime, technical specialists process data using professional methods to support judicial authorities; judicial personnel evaluate data's compliance with legal standards to determine its evidentiary admissibility and weight.

3 Regulatory Frameworks and Fundamental Paradigms of Data Flows in Cross-Border Cybercrime

The data flow system of cross-border cybercrime will be analyzed from three dimensions. First, examining international and domestic legislative frameworks to reveal the interplay and coordination of cross-border data flow rules across different jurisdictions, alongside China' s regulatory system established under the Data Security Law and Personal Information Protection Law. Second, dissecting the covert data transmission pathways constructed by criminals using techniques such as multi-node hopping, encryption/anonymization technologies, and camouflage of legitimate traffic, as well as the challenges these pose to judicial evidence collection. Third, through analysis of typical scenarios, elaborating on the distinct flow patterns and characteristics of data in criminal activities including cross-border data theft, cyber-enabled fraud/money laundering, and terrorism dissemination.

3.1 Legislative Frameworks

Currently, no unified global convention governs cross-border data flows. Relevant rules are dispersed across regional agreements, industry standards, and bilateral judicial assistance treaties. While Article 32b of the United Nations Convention on Cybercrime (Budapest Convention) stipulates a rapid response mechanism for cross-border data access, it binds only 65 signatory jurisdictions. The "adequacy decision" mechanism established under Article 48 of the EU' s General Data Protection Regulation (GDPR) essentially constructs an EU-centric paradigm for data flows. The US CLOUD Act creates a technology-hegemony-backed data control system through its "qualifying foreign government" certification process.

China’ s core legal instruments governing cross-border data are the Data Security Law of the People’ s Republic of China (hereinafter “DSL”) and the Personal Information Protection Law of the People’ s Republic of China (hereinafter “PIPL”), which jointly constitute the top-level design for regulating outbound data transfers. The promulgation of the DSL established China’ s foundational framework for data sovereignty and security governance. Specifically, Article 36 explicitly prohibits domestic organizations and individuals from providing data stored within China to foreign judicial or law enforcement agencies without approval from competent Chinese authorities. This provision serves as a robust countermeasure against extraterritorial assertions of long-arm jurisdiction under laws such as the US CLOUD Act. In practice, this article strictly regulates foreign agencies’ access to domestic data: all requests must follow statutory channels like the International Criminal Judicial Assistance Law, and enterprises lack authority to directly provide data. For example, in a 2023 case, the Cyberspace Administration of China (CAC) instructed the Chinese branch of a major multinational consulting firm to reject its US headquarters’ internal audit request for sensitive operational data of Chinese clients, mandating resolution through Sino-US judicial assistance channels. This action demonstrated China’ s resolve to safeguard data sovereignty while providing enterprises with clear operational guidance. Article 21 establishes a national data classification and grading system. At the national level, supporting documents including the Data Security Management Certification Implementation Rules and Network Data Processing Security Specifications have been issued to guide classification efforts. Sectorally, the Industrial and Information Technology Data Security Management Measures (Trial) categorizes industrial data into R&D data, production/operation data, and management data, explicitly prohibiting the export of core industrial data and mandating stringent security assessments for important industrial data transfers. The PIPL focuses on personal information rights and scenario-based governance. Article 38 sets three primary pathways for cross-border transfers of personal information. First, security assessment organized by the national cybersecurity authority. This is the primary route for large-scale transfers (e.g., >1 million individuals) or sensitive personal information (biometrics, religious beliefs, specific identities, medical/health data, financial accounts, location tracking). In 2023, a leading short-video platform triggered this assessment when proposing to share non-sensitive browsing data of Chinese users with overseas affiliates for algorithm optimization, as the massive user base necessitated compliance despite non-sensitive content. Second, certification by specialized institutions according to CAC regulations. This applies to intra-group transfers within multinational corporations or among members of the same economic entity, with certification bodies auditing against national standards. Third, execution of standard contracts formulated by CAC with overseas recipients. This offers a streamlined path for SMEs or small-scale processing. The Measures on Standard Contracts for Outbound Transfer of Personal Information took effect on June 1, 2023, with published contract templates detailing data processing activities, security obligations, and mechanisms for data subject redress.

3.2 Technology-Driven Flow Paths

In cross-border cybercrime, criminals construct complex and covert data flow pathways using various technical means to achieve illegal objectives and evade detection. These pathways skillfully exploit characteristics of modern network technologies, making the true source and ultimate destination of data difficult to trace. Specifically, they primarily include three approaches: utilizing multi-node hopping to achieve concealed transmission, employing encryption and anonymization techniques to hide traces and content, and disguising illegal data within legitimate business traffic.

3.2.1 Concealed Transmission via Multi-Node Hopping

Criminal data is typically not sent directly from point A to point B. Instead, like a parcel being repeatedly forwarded and relabeled in an international postal system, it passes through numerous intermediate "stations"—network nodes usually located on servers across different countries or regions. This method is termed multi-node hopping. Its core principle involves routing criminal data through a series of proxy servers (e.g., VPNs), anonymizing networks (e.g., Tor' s "onion routing," which encrypts and forwards data layer by layer like peeling an onion, ensuring each node knows only the immediate previous and next hop without seeing the full path), or compromised "hop servers." Before reaching its final destination, the data circulates through global networks. Each hop may alter the data's network address information, increasing tracking difficulty. Such pathways often span multiple jurisdictions, requiring law enforcement to engage in complex international cooperation during investigations. Moreover, each node may retain only partial transmission records, making it challenging to reconstruct a complete evidentiary chain.

3.2.2 Concealment of traces and Content Through Encryption and Anonymization

Data content encryption refers to the conversion of original data (e.g., chat logs, stolen trade secrets) into meaningless ciphertext via encryption algorithms. Only those possessing a specific "key" can decrypt and view the original content. A common implementation is end-to-end encryption (E2EE), adopted by many instant messaging applications (e.g., WhatsApp, Signal), which ensures even service providers cannot access user communications. Criminals exploit this to freely discuss and transmit illegal information on such platforms. Some encrypted email services (e.g., ProtonMail) further offer "self-destruct" functionality, automatically destroying emails after reading without leaving traces.

Identity anonymization involves concealing the real identities of data senders and recipients. Beyond the inherent anonymity of Tor networks, in the financial realm, certain cryptocurrencies (e.g., Monero) are favored by criminals for money laundering due to their high anonymity, making fund flows and associated data streams untraceable to specific individuals. Cryptocurrency mixer services further obscure original fund paths by pooling and redistributing cryptocurrencies from diverse sources, severing links between data and real identities.

Strong encryption renders data unreadable to law enforcement even if intercepted, while anonymization makes identifying suspects extremely difficult. This directly challenges traditional investigation models and evidentiary rules. For instance, requirements for original evidence under China' s Criminal Procedure Law face difficulties in verifying the authenticity and integrity of electronically data subjected to complex encryption and anonymization.

3.2.3 Disguising Illegal Data as Legitimate Business Traffic

Blending illegal data flows within normal internet operations represents a more sophisticated tactic. Criminals may exploit the global infrastructure and robust storage/backup capabilities of major cloud services (e.g., AWS, Microsoft Azure, Alibaba Cloud) to disguise stolen data as routine business files backed up to overseas cloud servers, enabling covert data transfer. Criminals also abuse content delivery networks (CDNs). Designed to accelerate website access by caching content on globally distributed servers, CDNs can be exploited to distribute illegal material (e.g., pirated media, malware, gambling/pornographic content). Caching across multiple global nodes not only speeds up dissemination but also complicates tracing to source servers. Abusing legitimate application programming interfaces (APIs) is another common approach. APIs serve as bridges for data exchange between software systems. If enterprise APIs contain security vulnerabilities or are misused, criminals may secretly transmit illegal data through these seemingly legitimate channels. For example, an e-commerce platform’ s order inquiry API lacking strict access controls and content filtering could be exploited to relay gambling-related commands or micro-fund transfers, hidden within massive volumes of legitimate API calls.

The combined use of these techniques endows cross-border cybercrime data flows with high concealment, complexity, and transnationality, presenting unprecedented challenges to legal regulation and judicial enforcement worldwide.

3.3 Analysis of Flow Characteristics in Typical Scenarios

Different types of cross-border cybercrime exhibit distinct data flow patterns. Cross-border data theft, cyber-enabled fraud and money laundering, and terrorism and illegal content dissemination each demonstrate unique data flow characteristics within their operational contexts.

Cross-Border Data Theft typically refers to long-term, targeted cyber attacks by hacker groups or state-sponsored actors against specific entities (e.g., government agencies, large corporations, research institutes) to steal high-value sensitive data (state secrets, core business data, intellectual property, etc.). During initial attack phases, data flows may be minimal, primarily involving reconnaissance and vulnerability scanning. Once a foothold is established (e.g., via supply chain compromises like malware implantation), attackers maintain persistence within internal networks while gradually expanding control. During data aggregation and exfiltration, stolen data is rarely transmitted en masse to avoid triggering security alerts. Attackers typically filter, compress, and encrypt data within the target network before transmitting it overseas in small batches through covert channels. In the SolarWinds supply chain incident, for instance, infected systems established hidden connections with attacker-controlled foreign servers to exfiltrate data incrementally.

Cyber Fraud and Associated Money Laundering represent highly prevalent cross-border crimes. Fraud syndicates typically operate from overseas bases (e.g., Southeast Asia, Middle East), obtaining scam scripts, victim profiles, and counterfeit app or website templates from “upstream” sources via instant messaging tools. Internal data flows rapidly within these groups during operational planning and training. Subsequently, fraudsters broadcast scam content at scale to potential victims domestically or in target countries using phone calls, SMS blasts, social media ads, and phishing emails. Upon successful scams, illicit proceeds are rapidly transferred abroad through layered bank accounts, third-party payment platforms, and particularly cryptocurrencies. To evade detection, syndicates recruit individuals to provide accounts for fund receipt and transfer. Platforms record account information and transaction data, often stored on overseas servers. In such operations, scam content appears as standardized text, voice or images, victim data serves as the critical component, and financial flow data remains highly fragmented and anonymized.

Terrorism and Illegal Content Dissemination constitute another archetypal cross-border cybercrime. Terrorist organizations and extremist groups heavily rely on digital platforms for propaganda, recruitment, planning, and communication, exhibiting data flows characterized by rapid proliferation and persistence. Core members communicate via strongly encrypted tools for covert coordination, while public platforms (Facebook, Twitter, YouTube) and dark web forums disseminate propaganda videos, recruitment materials, and extremist ideology. These groups employ "guerrilla tactics"—swiftly creating new accounts when existing ones are suspended. Their data encompasses text, images, audio, and video formats, often featuring inflammatory content designed for visual impact. Leveraging algorithmic recommendations and user-driven sharing, they achieve viral propagation across networks.

Table 1 Flow Characteristics and Impacts in Typical Scenarios

Scenario	Flow Characteristics	Impact
Cross-Border Data Theft	• Initial Phase: Minimal data flows, primarily reconnaissance and vulnerability scanning. • Post-Breach: Data filtered, compressed, and encrypted internally; transmitted overseas in small batches via covert channels to evade detection.	Theft of high-value sensitive data (state secrets, core business data, intellectual property) causing significant security and economic losses.
Cyber Fraud & Money Laundering	• Rapid internal data exchange/updates (e.g., scam scripts/victim profiles via IM tools). • Standardized scam content (text/voice/images) broadcast at scale from overseas bases. • Highly fragmented/anonymized fund flows (layered bank accounts/cryptocurrencies).	High-prevalence crime; victim data exposure as critical risk; illicit proceeds rapidly moved offshore causing capital loss and regulatory evasion.
Terrorism & Illegal Content Dissemination	• Rapid proliferation and persistence: - Core members coordinate via encrypted channels. - Public platforms/dark web distribute propaganda. • Guerrilla tactics (rapid account regeneration post-suspension). • Viral propagation via algorithms/user sharing using multimodal content (text/images/audio/video).	Dissemination of extremist ideology and recruitment activities threatening social stability; persistent inflammatory content resistant to eradication.

4 Conclusion

In cross-border cybercrime, data plays a pivotal role and can be broadly categorized into three primary types: electronic data, traffic data, and content data. Electronic data typically refers to information stored on electronic devices such as hard drives and servers; traffic data concerns the transmission process of data across networks, including the sending and receiving of data packets; while content data focuses on the substantive information contained within the data, such as text, images, and videos. Furthermore, these data types can be structurally divided through binary classification into core versus non-core data, as well as enterprise versus personal data. Core data generally denotes critical information decisive for establishing criminal conduct, whereas non-core data holds secondary importance; enterprise data pertains to corporate or organizational information, while personal data involves individual privacy and personally identifiable information.

These data classifications share fundamental commonalities with evidence, as all may serve to substantiate criminal activities. Nevertheless, significant distinctions exist in aspects such as data provenance, reliability, and processing methodologies. Within cross-border cybercrime, data exhibits pronounced fluidity and dynamism, with perpetrators frequently leveraging advanced technical means to enable rapid data transfer and dissemination. To address data flow challenges in such crimes, legislative and regulatory authorities across jurisdictions have established corresponding normative frameworks. These frameworks aim to regulate cross-border data transfers, protect the privacy rights of individuals and enterprises, and combat criminal activities. For instance, the European Union's General Data Protection Regulation (GDPR) imposes stringent requirements for cross-border data transfers to ensure secure and lawful data flows.

This category of criminal activity predominantly relies on technology-driven mechanisms to achieve rapid data movement. Across diverse domains such as the internet and mobile communication networks, cross-border cybercrime demonstrates distinctive fluid characteristics. Criminals employ various technical measures—including encryption, anonymizing networks, and cryptocurrencies—to conceal illicit activities, thereby complicating investigative tracking and evidence collection. Consequently, enhanced cooperation among national law enforcement agencies and international organizations is imperative to collectively address this global challenge. An integrated approach combining technical countermeasures and legal instruments will prove essential for effective combat against cross-border cybercrime.

References

[1]Chen, Z., Wang, G., Hu, S., et al. (2015). Big data security and autonomous controllability. Chinese Science Bulletin, (Z1), 427-432.

[2]Fang, H. (2025). The limit of criminal law protection for corporate data rights under the background of new economic crimes. Journal of Shenzhen University (Humanities & Social Sciences Edition), (3), 98-107.

[3]Huang, B. (2024). Research on key regulatory technologies for onion service websites facing Tor network(Master's thesis, China People's Public Security University).

[4]Liu, J. (2025). Contractual protection mechanism of information subject rights in personal data transactions: Focusing on the application of the Personal Information Protection Law. Journal of Zhengzhou University (Philosophy and Social Sciences Edition), (3), 53-60.

[5]Park, T. J., & Rohatgi, A. (2024). Balancing the platform responsibility paradox: A case for amplification regulation to mitigate the spread of harmful but legal content online. Computer Law & Security Review: The International Journal of Technology Law and Practice, 52, 105960.

[6]Qu, D. (2020). On the legal guarantee of two-way compliance for enterprises under cross-border data flow regulation. Oriental Law, (2), 185-197.

[7]Xu, J. (2024). Research on international criminal judicial assistance in cross-border electronic data forensics in China(Master's thesis, Guizhou University).

[8]Zang, Z. (2022). Research on cross-border electronic evidence collection system(Master's thesis, Shanghai University of Finance and Economics).

[9]Zhang, X. (2023). Research on international regulation of personal data cross-border flow(Master's thesis, Jiangxi University of Finance and Economics).

[10]Zhang, C., Zhang, H., & Zhu, S. (2009). Research on wireless jamming and data masquerading technology based on IEEE802.11. Computer System Applications, (7), 138-140.

[11]Zang, G., Jia, Q., Chen, H., et al. (2022). Encrypted deduplication scheme without third-party server based on data popularity. Journal of Communications, (8), 17-29.

[12]V.Karamchand Gandhi.(2012).An Overview Study on Cyber crimes in Internet.Journal of Information Engineering and Applications.

[13]YuLan,CongQiyan & LiSixin.(2024).Study on International Cooperation to Address Cross-border Telecommunication Network Fraud Offence.Journal of Politics and Law,17(2),51-51.

[14]Zhang Hengyue & Gong Xiangqian.(2024).The research on an electronic evidence forensic system for cross-border cybercrime.The International Journal of Evidence & Proof,28(1),21-44.

[15]Xu Wang.(2025).Challenges and Responses to China's Participation in Cross-border Data Flows.Scientific Journal of Economics and Management Research,7(4),80-87.

[16]Gyanchandani Vandana.(2024).Cross-border flow of personal data (digital trade) ought to have data protection.Journal of Data Protection & Privacy,7(1),61-79.

[17]ZuoZhuan.(2024).Cross-Border Data Forensics: Challenges and Strategies in the Belt and Road Initiative Digital Era.Asian Social Science,20(2),49-49.