Science of Law Journal (2025)
Clausius Scientific Press, Canada

DOI: 10.23977/law.2025.040504
ISSN 2616-2296 Vol. 4 Num. 5

Challenges and Impacts of Cross-Border Electronic Data Forensics

Chutong Zhang*

School of Law, Shenyang University of Technology, Shenyang, Liaoning, China
**Corresponding author*

Keywords: Cross-Border Electronic Data, Forensics, Privacy Rights, Jurisdiction

Abstract: With the continuous advancement of digital technology and the deepening of globalization, cross-border electronic data forensics, as a crucial link in combating cross-border cybercrimes and maintaining the order of the digital space, has become increasingly important. However, cross-border electronic data forensics inherently possesses both cross-border and technical attributes, and in practice, it faces multiple obstacles. Differences in the concept of data sovereignty among countries give rise to jurisdictional conflicts, the upgrading of encryption technology and the massive volume of data create technical barriers, the lengthy international judicial assistance process leads to inefficient collaboration, and the inadaptability of traditional forensics rules to the needs of the digital age are intertwined. These problems have led cross-border electronic data forensics to fall into the practical predicament of difficulty in obtaining evidence, verifying evidence, and collaborating. Therefore, this article will take the international law dimension of cross-border electronic data forensics as the core research perspective, and analyze four aspects: an overview of cross-border electronic data forensics, the difficulties faced by cross-border electronic forensics, the situation of extraterritorial cross-border electronic data forensics, and the optimization path of cross-border electronic data forensics. The aim is to provide readers with a systematic and comprehensive understanding.

1. Overview of Cross-Border Electronic Data Forensics

1.1 The Definition of Cross-border Transactions

In the context of cross-border electronic forensics, the definition of "cross-border" should be analyzed from both the physical connection of data flow and the jurisdictional boundaries of legal authority.

From the physical perspective, "cross-border" originates from the cross-border connection at any stage of the electronic data transmission chain. Taking web data transmission as an example, when any node such as the data provider, network service provider, or remote server is located outside the country, or when the data transmission path crosses national borders, it constitutes a physical level of cross-border. This definition breaks through the limitations of traditional geographical boundaries, including both the physical cross-border of storage media such as overseas servers and cross-border hard drives, as well as the "unbounded cross-border" of data transmission in the virtual

network. This means that even if the data does not directly cross geographical space, as long as its transmission involves an overseas node, it possesses cross-border attributes.

From the legal perspective, "cross-border" is essentially the triggering of jurisdictional conflicts. Criminal jurisdiction is based on the actual geographical space, but the non-boundary nature of the cyber space blurs the boundaries with geographical space, making electronic data a hiding place in the overlapping space of the two. When key electronic data is located outside the country and the investigation authorities cannot obtain it through domestic channels, the cross-border electronic forensics procedure is initiated. At this time, "cross-border" is not only the crossing of physical space, but also the collision of jurisdictional authority in different legal domains. If cross-border forensics is not carried out through judicial assistance and is directly implemented, it may lose the legality of the evidence due to infringement of the sovereignty of other countries.

In conclusion, in cross-border electronic forensics, "cross-border" is the integration of physical space cross-border and legal jurisdiction cross-border. This means that in addition to examining the cross-border connection of the data transmission chain, it is also necessary to pay attention to the jurisdictional conflicts it triggers, and ultimately define the boundaries of the legality and legitimacy of cross-border electronic forensics through both physical and legal standards.

1.2 The Concept of Electronic Data

In the context of cross-border electronic evidence collection, electronic data refers to digital information records stored, transmitted, or generated in electronic form, directly related to cross-border criminal activities, and capable of proving the facts of the case. It is the behavioral traces left by criminals using electronic devices such as computers and mobile phones in the virtual network space, and is also the core evidence carrier for law enforcement agencies to break through national border restrictions and combat cross-border cyber crimes.

From a functional perspective, this type of electronic data shares the common characteristics of general electronic data. For example, first, it is replicable. Unlike traditional paper evidence that is difficult to restore once the original is damaged, this type of electronic data can be replicated and retained completely without loss by using professional technical tools and compliant operation procedures. This characteristic is of crucial value in cross-border circulation scenarios. Whether it is retrieving data from an overseas server or transferring evidence between different national judicial authorities, lossless replication can effectively avoid the risk of evidence loss due to physical transportation, changes in storage environment, or human operational errors, ensuring the integrity and availability of the data. Second, it is easily modifiable. Electronic data is easily deleted or tampered with in the virtual space, which poses higher requirements for the technical standardization of cross-border evidence collection. If during the cross-border retrieval of chat records from overseas servers, international common evidence collection standards are not followed or no technical measures such as full encryption and evidence fixation are taken, the data may be illegally intercepted and tampered with during transmission, or the data may be distorted due to non-standard procedures during the operation of the overseas evidence collection entity, ultimately affecting the legal effect of the evidence. Third, it is accessible. In the practice of cross-border case evidence collection, the acquisition path of this type of electronic data is relatively clear, and it can be achieved through two methods. The first is direct extraction, that is, when the suspect's mobile phone or laptop and other electronic devices are within the control of the domestic judicial authority, the cross-border-related data stored in the device can be directly read using professional data extraction equipment. The second method is to extract after seizing the electronic device. If the electronic device involves cross-border connections and requires further in-depth data exploration, it can be legally seized first, and then the hidden cross-border data in the device can be extracted

through professional technical means in a laboratory environment with security protection conditions. Fourth, it is massive. Since the electronic data is stored in cross-border servers or devices, it is necessary to identify the core information related to the case from a large amount of data. Moreover, this type of electronic data has special value due to its "cross-border" attribute. It is the key link connecting different legal domains of criminal facts. It covers cross-border chat records, cross-border emails, files stored on overseas servers, IP address trajectories involving multiple countries, etc., and plays an irreplaceable role in proving the cross-border connections of criminal activities and determining cross-border criminal facts.

1.3 The Main Technical Means of Electronic Data Forensics

The main technical means of electronic data forensics mainly include disk forensics, memory forensics, and traffic forensics. These three technical means not only provide technical support for extracting, fixing, and analyzing electronic data, but also directly relate to the legality, authenticity, and relevance of evidence.

The first technical means is disk forensics. Disk forensics, as the most basic forensic method, focuses on the fixation and analysis of static data in the storage medium. Unlike the intuitiveness of traditional physical evidence, disk forensics requires the restoration of the original state of the storage device through technical means. From a legal perspective, this technical means is directly related to the determination of the authenticity of evidence. For example, in intellectual property disputes, by restoring deleted source code files through disk forensics, the implementation path of infringement can be directly proved. In criminal cases, the technical analysis of encrypted partitions remaining in the disk can provide key clues for case investigation. It is worth noting that disk forensics must strictly follow legal procedures, such as the traceability record of the forensics process and the introduction of a third-party witnessing mechanism, to ensure that the obtained electronic evidence meets the standards of judicial review and avoid the loss of evidence due to flaws in the forensics process.

The second technical means is memory forensics. Memory data often truly reflects the running state and user behavior of a computer at a specific moment. In the field of law, memory forensics is often used in the investigation of cybercrime cases. For example, by extracting the cache information of instant messaging software, the communication content and time nodes of the suspect can be restored. Compared with the static nature of disk forensics, memory forensics emphasizes the fixation of instantaneous evidence. In addition, memory forensics also raises legal controversies regarding personal privacy protection. How to strike a balance between combating crime and protecting citizens' privacy rights has become a problem to be solved in judicial practice.

The third technical means is traffic forensics. This technology captures, records, and analyzes network communication data to prove the interaction relationship and communication content between the subjects. Its legal function is to convert the information transmission process in the virtual space into an evidence chain that can be reviewed by the court. Due to the strong real-time nature and large data volume of network data streams, this technology poses special challenges to the standardization and legality of the forensics process.For instance, during the data screening process, how do the relevant staff members balance the issue of investigation efficiency and the protection of citizens' communication privacy? The conclusion of traffic forensics is crucial for establishing the correlation between each evidence node and proving criminal agreement and collaborative behavior, and is the core technical support for handling cybercrime cases.

2. The challenges faced by cross-border electronic evidence collection

With the deep penetration of digital technology and the increasing frequency of cross-border

interactions, electronic data has become a critical link connecting criminal facts across different legal jurisdictions, making its investigation a key component in combating transnational crimes. However, cross-border electronic evidence collection is not a simple extension of domestic procedures but a complex systemic endeavor fraught with multiple challenges. In practice, significant legal disparities exist among nations regarding data sovereignty and evidentiary validity, rendering legal applicability conflicts and selection the primary hurdle during investigations. Additionally, the inherent susceptibility to tampering and vast volume of electronic data elevate technical difficulties in preservation, extraction, and verification far beyond domestic evidence collection. Meanwhile, transnational judicial cooperation involves coordination of authorities, procedural approvals, and information exchange among multiple countries, with cumbersome procedural requirements further delaying investigation efficiency. These interwoven challenges not only constrain the resolution of cross-border cases but also pose severe threats to the global digital-era judicial collaboration system. The three primary difficulties faced by cross-border electronic evidence collection are as follows.

2.1 The Legal Application of Cross-border Electronic Data Forensics is Extremely Complex

The primary characteristic of cross-border electronic data forensics is that it faces an extremely complex legal application environment. Evidence collection activities are essentially the exercise of a country's judicial sovereignty, but when data is stored overseas, it directly contacts the data sovereignty and laws and regulations of other countries. There are significant differences and even conflicts in legal concepts, data protection standards, and enforcement procedures among different jurisdictions. For example, requesting a country to retrieve data in accordance with its own laws may violate the strict data localization or privacy protection laws of the country where the data is located. At the same time, some countries advocate for jurisdiction over overseas data controlled by their own enterprises, which directly opposes the jurisdiction claims of other countries based on data storage locations, putting law enforcement agencies and multinational corporations in a dilemma of "which country's laws to comply with". The intense collision and selection of applicable legal rules constitute the fundamental obstacle to cross-border evidence collection. The typical manifestation of this issue is the Microsoft Ireland case. In this case, the US Department of Justice, in order to investigate drug trafficking cases, requested Microsoft to provide its user email data stored on servers in Ireland in accordance with domestic laws. Microsoft has raised objections to this and advocates that such cross-border transfers should be conducted through judicial assistance channels between the two countries, while the unilateral demands of the US government lack international legal basis and constitute a violation of law enforcement powers. Although the case ultimately came to an end with the passage of the Cloud Act by the US Congress, which authorized the agency to access user data controlled by network service providers both within and outside the United States. In this case, the United States claims jurisdiction over overseas data controlled by its own companies, while Ireland claims jurisdiction based on data storage. The legal concepts and jurisdictional claims of the two sides are directly opposed, putting Microsoft in a dilemma and fully reflecting the complexity of legal application in cross-border electronic data authentication.

2.2 The Technical Difficulty of Cross-border Electronic Data Forensics is High

Cross border electronic data forensics faces severe challenges at the technical level that far exceed domestic forensics. Due to the massive, volatile, and easily tampered nature of data, some criminal gangs may also set up automatic cleaning mechanisms, and data may be overwritten and deleted within 24 to 72 hours. However, geographical distance and judicial barriers may cause delays in the timing of evidence collection and increase the risk of evidence loss. Moreover, the

technical confrontation during the evidence collection process is extremely strong. Suspect generally use strong encryption technologies such as quantum key and chaotic encryption, or use anonymous network tools such as fake IP pools to hide identity and communication content. The keys are often hidden in overseas hardware devices, and the IP trajectories are scattered across dozens of nodes worldwide. This makes conventional decryption and traceability methods completely ineffective, and judicial authorities need to invest a lot of resources in developing specialized technologies, often falling into a vicious cycle of "cracking updating". This greatly increases the difficulty of data decryption and traceability. The highly complex forensic environment is also a major challenge, especially when conducting forensic work on distributed architecture cloud platforms. Data may be dynamically stored on multiple nodes worldwide, and data on distributed cloud platforms may dynamically migrate between global nodes every 6 hours. How to obtain complete and compliant evidence without violating local laws places extremely high demands on technical solutions. A slight deviation may lead to the invalidation of evidence or trigger legal disputes. These factors collectively lead to technical difficulties in data positioning, acquisition, fixation, and analysis in cross-border forensics.

2.3 The Collaboration Process is Cumbersome

The collaborative process of cross-border electronic data forensics presents significant complexity and inefficiency due to the complex linkage involving multiple parties and links. This has become a key bottleneck restricting the timeliness of cross-border crime crackdown. From the perspective of official mainstream collaboration channels, conducting evidence collection based on international judicial assistance treaties or bilateral agreements is currently the most compliant but also the most time-consuming path. This process needs to go through layers of transmission from various agencies. Firstly, the case handling authorities of the requesting country shall organize the evidence collection requirements and submit them to the central authorities of their own country for review. After approval, it needs to be transmitted to the central authorities of the requested country through diplomatic channels. Then, the central authorities of the requested country conduct a second review of the legality and completeness of the request document, confirm its accuracy, and forward it to the corresponding local law enforcement department in their country. Finally, local law enforcement departments carried out evidence collection operations and provided feedback on the results in reverse according to the original path. Throughout the process, the documents need to comply with the format standards of different countries, and some links also require multilingual translation and notarization. The preparation and review of the documents alone may take several weeks. In addition, some countries have significant differences in administrative efficiency, or communication costs are increased due to differences in diplomatic relations and legal systems, resulting in a complete process that often takes several months, and complex cases may even require waiting for one to two years, forming a sharp contradiction with the core requirement of strong timeliness of electronic evidence. The result of this issue is that by the time the evidence collection results are finally fed back, some of the data may have been destroyed, or the criminal gang may have already moved their crime scene, significantly reducing the value of evidence collection. Although some countries have begun to explore alternative ways of directly cooperating with multinational technology companies to break through efficiency bottlenecks, such as using internal compliance teams to assist in accessing overseas stored data, this model lacks unified international rules support. There are differences in the legal definition of whether enterprises have the right to provide data across borders in different countries. Some countries recognize companies providing data based on user agreements or law enforcement requests, while others require that official judicial assistance channels be used. Direct cooperation may be suspected of violating local

data sovereignty laws. At the same time, the collaboration standards of enterprises are also opaque, and some enterprises may selectively respond to evidence collection requests based on their own commercial interests or regional policies, resulting in significant differences in collaboration efficiency among different cases. The legitimacy, stability, and fairness of this "non standardized" collaboration have always been controversial and difficult to become a reliable supplementary path for cross-border evidence collection[1].

3. The Situation of Cross-border Electronic Data Forensics outside the Domain

3.1 The Rules and Practices of Data Forensics outside the European Union

In the field of cross-border data governance, the European Union has established an overseas data forensics system that combines strict data protection and regional judicial cooperation, with the General Data Protection Regulation (GDPR) as its core.

From a legislative perspective, GDPR includes data controllers or processors who have data exchange with EU citizens outside the EU through its expansive extraterritorial provisions. This means that even if the subject of evidence is located outside the EU, as long as it processes data of EU citizens, it must comply with GDPR compliance requirements regarding data retrieval, including principles such as data subject consent and purpose limitations. At the same time, the European Union has established a standardized cross-border electronic evidence collection cooperation mechanism within the region. Member states can quickly initiate overseas data retrieval procedures through this order, improving evidence collection efficiency while safeguarding the rights of data subjects.

In practical operation, the collection of data outside the EU requires a balance between data protection and judicial needs. On the one hand, we strictly adhere to the legality basis of GDPR regarding data processing, ensuring that evidence collection activities comply with principles such as "legitimate purpose, minimum necessity". On the other hand, the relevant authorities should leverage the EU's internal judicial cooperation framework to streamline processes and shorten cycle times. For example, in cases involving cross-border cybercrime, EU member states may retrieve electronic data from overseas service providers in accordance with the European Investigative Order directive, and this process must simultaneously meet the protection requirements of the data subject's rights to know and object. This model reflects the EU's delicate balance between data sovereignty, personal information protection, and judicial cooperation. It not only prevents data abuse through strict rules, but also enhances the practicality of overseas data collection through regional integration mechanisms, becoming a highly representative institutional sample in global cross-border data governance[2].

3.2 The Rules and Practices of Data Forensics outside the United States

The United States has formed a rule system in the field of overseas data forensics characterized by legislative expansion and judicial flexibility, and its operational mode reflects strong initiative. The United States has expanded the jurisdictional boundaries of data forensics through the Cloud Act, which stipulates that as long as data controlled by US service providers is related to US judicial proceedings, federal courts can require service providers to provide data disclosure in order to access foreign data. In the civil field, based on the unique system of evidence disclosure, US courts may require foreign parties to submit evidence materials stored abroad without the prerequisite of international judicial assistance procedures. This further expands the channels for obtaining overseas data. At the same time, the United States has also noted the international coordination issues involved in cross-border data forensics. By engaging in dialogue with other jurisdictions, the

aim is to provide more feasible pathways for cross-border data forensics. This approach of responding to cross-border data forensics through various means reflects the continuous adjustment of relevant legal frameworks in the context of the digital age. Overall, the United States' approach to overseas data forensics demonstrates an attempt to address cross-border data governance challenges through a combination of domestic legal procedures and international cooperation.

4. Optimization Path for Cross border Electronic Evidence Collection

With the increasingly prominent role of cross-border electronic data in global judicial practice, issues such as differences in rules, technical difficulties, and poor collaboration in its evidence collection process are gradually becoming apparent. The optimization of cross-border electronic evidence collection needs to be based on practical needs, steadily promoted around the three dimensions of "rule coordination, technological empowerment, and collaborative upgrading", gradually resolving practical difficulties on the basis of respecting the principles of data governance in various countries, and building a more suitable cross-border evidence collection work system.

4.1 At the Level of Legal Rules

At the level of legal rules, it is necessary to focus on building a compatible and adaptable regulatory framework to provide clear guidance for cross-border electronic evidence collection. From the perspective of improving domestic standards, there is still room for refinement in the current operational procedures for cross-border electronic data extraction, fixation, and verification. For example, the approval process for retrieving different types of data and the handling of defects in overseas evidence collection procedures are not fully clear, which can easily lead to inconsistent practical operations. In this regard, within the existing legal framework, judicial interpretations or guiding documents can be issued to further clarify the approval levels for overseas data retrieval.We should distinguish between the approval requirements for general data and data involving personal privacy and trade secrets. Meanwhile, we also need to refine the specific standards for determining the validity of evidence. For example, in response to situations such as translation deviations in overseas data and incomplete evidence collection records, we should clarify the reasonable methods and time limits for correction.At the same time, it is necessary to balance the efficiency of evidence collection and information protection, and integrate the principles of necessity and moderation into specific operations. For example, when retrieving cross-border data, it is clear to only extract content directly related to the case to avoid excessive collection. From the perspective of international rule coordination, there are differences in data jurisdiction and evidence collection rules among countries, which can easily lead to differences in cooperation. In bilateral judicial assistance treaty negotiations, efforts can be made to further standardize the relevant provisions on electronic data forensics, clarify the basic elements of request letters, data transmission formats, and reasonable time limits for collaborative responses[3]. We should refer to the established legal frameworks in other countries to mitigate collaboration barriers arising from ambiguous rules. Concurrently, we must actively engage in multilateral dialogues on data governance to forge broader international consensus on the core principles of cross-border evidence collection. For example, respecting the management requirements of the country to which the data belongs and ensuring the legality of the evidence collection procedures lay the foundation for mutual recognition of cross-border evidence collection rules.

4.2 At the Level of Technical Support

At the technical support level, it is necessary to enhance the practicality and reliability of cross-

border electronic forensics through technological empowerment. In response to the technical difficulties in current cross-border forensics, such as encrypted data processing and massive data filtering, efforts can be made to increase the research and application of related technologies. On the one hand, we will promote the research and development of technologies such as encrypted data parsing and remote security forensics, establish a professional technical research platform, and collaborate with research institutions and enterprises to tackle key issues. Simultaneously, we should explore the standardized application of technology, such as promoting unified technical standards in regional cooperation, ensuring the traceability and verifiability of cross-border data transmission, and reducing the risk of data tampering. On the other hand, in response to the problem of large cross-border data volume and high screening difficulty, an intelligent data processing platform is built to automatically identify core data related to cases through pre-set case feature models, reducing the workload and error rate of manual screening. At the same time, in the application of technology, attention is paid to information protection, embedding data anonymization modules to shield irrelevant personal information, and balancing forensic efficiency and privacy security[4].

4.3 At the Level of Collaboration Mechanism

At the level of collaboration mechanism, it is necessary to establish a multi-layered collaborative network to enhance the efficiency of cross-border electronic forensics collaboration. In order to optimize the cross-border judicial cooperation process and address the high timeliness requirements for evidence collection in some cases, it is possible to explore the establishment of a fast cooperation channel under bilateral or multilateral frameworks to simplify the approval process for urgent cases.For instance, we can enhance cooperation by clarifying the applicable situations and processing time limits for urgent requests, and by establishing a standard communication platform. This would enable direct communication between Chinese and foreign law enforcement agencies, reducing information transmission links and improving response efficiency.In terms of regional and international cooperation, we will rely on existing regional cooperation mechanisms to deepen the integration of technology and rules. For example, we should promote the sharing and application of cross-border electronic evidence storage platforms within the framework of regional organizations to achieve mutual recognition of technical standards. By leveraging multilateral platforms such as the International Criminal Police Organization, we aim to improve the connectivity of data collaboration and provide more collaborative support to countries. In addition, communication with cross-border network service providers can be strengthened by signing cooperation memorandums and other means to clarify their basic processes and compliance requirements for cooperating with cross-border data retrieval. We should also provide necessary legal guidance to service providers to help them coordinate compliance requirements in different regions and reduce collaboration delays caused by compliance disputes.

Overall, the optimization of cross-border electronic forensics is a gradual process. We need to aim for "clear rules, reliable technology, and smooth cooperation", and gradually improve rules, upgrade technology, and optimize cooperation on the basis of respecting the actual situation of each country, to promote more standardized and efficient cross-border electronic evidence collection work, and provide strong support for the fair handling of global cross-border cases[5].

5. Conclusion

Cross-border electronic data forensics under international law currently faces core challenges, including collaboration barriers due to regulatory ambiguity and inconsistent standards for admitting digital evidence. To address these issues, relevant institutions must clarify data approval

requirements and evidence verification procedures. They should also engage in multilateral governance dialogues to build consensus on core forensics principles, while promoting unified technical standards and direct communication channels for law enforcement. Only through the synergy of rules, consensus, and technology can a viable path be forged to resolve the cross-border data forensics dilemma, thereby contributing to the advancement of global data governance.

References

[1] Liu P X. (2022). EU's Approach to Cross-border Electronic Evidence Collection and Its Enlightenment to China[J]. Journal of National Prosecutors College,30(05):3-23.

[2] Sachoulidou A .(2024).Cross-border access to electronic evidence in criminal matters: The new EU legislation and the consolidation of a paradigm shift in the area of 'judicial' cooperation[J].New Journal of European Criminal Law, 15(3): 256-274.

[3] Zhu W. (2024). Research on the Application of Artificial Intelligence in Criminal Evidence Examination and Judgment[J]. Scientific Journal of Intelligent Systems Research,6(11):1-8.

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

[5] ZHOU X. (2025). The Application of Big Data and Artificial Intelligence in Cross-Border E-Commerce[J]. Integration of Industry and Education Journal,4(1):24-33.