Proceedings of ICGPSH 2024 Workshop: Industry 5 and Society 5 – A Study from The Global Politics and Socio-Humanity Perspective
DOI: 10.54254/2753-7048/2025.LC19166

Challenges and Countermeasures in Cross-Border Data Collection

Jia Wang[1,a,*]

[1]School of Economic Law, East China University of Political Science and Law, Guangfulin Street, Shanghai, China
a. 23020101139@ecupl.edu.cn
**corresponding author*

Abstract: In the context of globalization, cross-border data collection has become a crucial tool for countries combating transnational crime. China primarily employs international criminal judicial assistance to conduct cross-border data collection. While this approach respects national sovereignty, it faces practical challenges such as low efficiency and limited authority. In contrast, the United States and the European Union adopt a more flexible data controller model, achieving robust cross-border data collection capabilities. However, conflicts in data sovereignty and differences in legal systems hinder the direct application of these models in China. This paper employs a comparative research methodology to analyze the legislative frameworks and backgrounds of the U.S. and EU cross-border data collection approaches, identifying reasons these models are unsuitable for direct implementation in China. Building on insights from these legislative models, the paper proposes recommendations such as increasing the number of bilateral judicial assistance agreements and establishing a categorized data management system, aiming to provide a reference for China's future development in this field.

Keywords: Cross-Border Data, Evidence Collection Models, Comparative Analysis.

1. Introduction

In the context of globalization and digitalization, cross-border data collection has become an essential tool in combating cybercrime, transnational crime, and other activities that threaten national security. In cases of transnational crime, data is often stored on servers located in different countries. Consequently, obtaining such data effectively has become a critical issue within global criminal justice cooperation. However, cross-border data collection not only involves disparities in legal systems but also touches on sensitive issues of national and data sovereignty.

Taking the "Zhang Kaimin and 52 others' telecommunications fraud case" as an example, Chinese investigative authorities collaborated with judicial bodies in Kenya and Indonesia through international criminal judicial assistance to obtain data on the suspects' cross-border fraud activities. Although both countries cooperated actively, it took an additional 11 hours after apprehending the suspects to acquire the relevant electronic devices, raising concerns about data authenticity due to the delay [1]. As the number of involved countries increases, the efficiency of evidence collection could decrease further, especially if the countries involved are not covered under existing international judicial assistance treaties. These issues make cross-border data collection a complex and challenging topic.

Existing research predominantly focuses on responses to conflicts over data sovereignty. Regarding China’s challenges in cross-border data collection, scholars generally agree that the current legal framework results in low efficiency, and there are concerns that the United States and the European Union might bypass judicial assistance procedures to collect data within China, posing a potential threat to China’s data security [2,3]. A small number of scholars have compared the legislative models of cross-border data collection in the United States, the EU, and China. Scholars widely recognize that the United States adopts a data controller model, whereas China adheres to a data localization standard. As for the EU, some scholars examine the internal evidence collection rules among EU member states, which follow a regionally open model, while others focus on its external jurisdiction rules, suggesting that the EU leverages the Digital Single Market to expand its judicial reach [4,5].

However, current research lacks a cohesive and comprehensive theoretical framework that addresses the political and institutional contexts of these three models, identifies specific legal conflicts with China, and offers solutions for effectively addressing these issues. In light of this, this paper seeks to examine the practical challenges China faces by reviewing the general framework of international criminal judicial assistance. It systematically analyzes and summarizes the legislative models of cross-border data collection in the United States, the EU, and China, explores the institutional backgrounds behind the development of U.S. and EU models, and assesses their relevance for China. The goal is to propose constructive recommendations for improving China’s cross-border data collection legislation, thereby advancing the effective implementation of judicial practices and providing constructive guidance for China's future legislative efforts in this area.

2. Challenges in Cross-Border Data Collection: Overview of International Criminal Judicial Assistance Regulations

2.1. Current Provisions and Challenges in China’s International Criminal Judicial Assistance for Evidence Collection

China’s cross-border data collection currently relies heavily on the model of international criminal judicial assistance. According to the Law of the People's Republic of China on International Criminal Judicial Assistance, the process of judicial assistance involves multiple stages. The investigative agency must prepare a request for judicial assistance, accompanied by relevant materials. Upon approval by the competent authority, the request is submitted to foreign authorities through designated liaison channels. Once the foreign authority consents, it issues an evidence collection order to its subordinate investigative agencies, which collect the evidence and return it through established channels. This lengthy process, involving multiple agencies and approvals from domestic to foreign entities, often extends case timelines, with typical waits exceeding ten months [4]. Additionally, the need for cooperation from foreign judicial authorities introduces further uncertainty regarding the timeline.

Furthermore, China imposes strict limitations on cross-border data collection conducted by foreign entities within its jurisdiction. Based on the principle of data localization, the Law of the People's Republic of China on International Criminal Judicial Assistance stipulates that no organization or individual may provide evidence to foreign parties without prior approval from Chinese competent authorities. In line with principles of national sovereignty, international courtesy, and security protection, cross-border data transfers are subject to a stringent approval process [3].

2.2. Extraterritorial Regulations on Cross-Border Data Collection

The limitations on cross-border data collection stem primarily from conflicts over data sovereignty. Data sovereignty refers to the principle that data is subject to the laws and privacy regulations of the specific geographic location where it is stored [6].

The United States, through CLOUD Act imposed in 2018, explicitly adopted a "data controller" model. Under this framework, U.S. law enforcement agencies can request data controllers to provide data stored abroad, provided the data controller has sufficient ties to the United States. This reflects the U.S. dominance in the data domain and its strategy of extraterritorial jurisdiction [5].

The European Union introduced the General Data Protection Regulation (GDPR), establishing a "data processor" model. Article 3(2) of the GDPR explicitly states that data controllers or processors not established in the EU but processing personal data of individuals within the EU--or offering goods, services, or monitoring behavior within the EU--are subject to GDPR jurisdiction, as long as the activities occur within the EU.

In summary, China’s approach to cross-border data collection is defensive, whereas the United States and the EU have adopted offensive strategies. Differences in standards for cross-border data collection among countries lead to data sovereignty conflicts. China, prioritizing national sovereignty, has taken a relatively conservative approach. However, this stance places China in a passive position in cross-border data collection when foreign entities do not cooperate, creating limitations for evidence collection.

3. Analysis of Cross-Border Data Collections Models Abroad

3.1. Interpretation of the Legislative Background of the U.S. Cross-Border Data Collection Model

The United States currently employs a data controller model for cross-border data collection, which is detailed in the CLOUD Act. Prior to the CLOUD Act, the U.S. relied on the Stored Communications Act (SCA), enacted in 1986, as the legal basis for cross-border data requests. Due to its outdated provisions, the U.S. proposed amendments through the Law Enforcement Access to Data Stored Abroad Act (LEADS Act) in 2015 and the International Communications Privacy Act (ICPA) in 2017, yet neither was passed [7,8].

The catalyst for the CLOUD Act’s enactment in 2018 was a legal dispute between the FBI and Microsoft over cross-border data access. A court order demanded that Microsoft provide email account records and other information related to a U.S. citizen’s account. Microsoft challenged the order, arguing that the data was stored in Dublin, Ireland, and that the order lacked extraterritorial authority [9]. While the SCA allows the government to compel internet service providers to disclose customer information under certain conditions, it does not explicitly authorize access to data stored abroad. Although the FBI could request assistance through Ireland’s Mutual Legal Assistance Treaty (MLAT), the process is time-consuming and hinders enforcement efficiency.

Additionally, U.S. and foreign law enforcement agencies increasingly need access to electronic communications stored on foreign servers. This need arises because tech companies can store data in locations far from users, leading to criminal investigation data often residing in countries other than where the crime occurred [10]. In response, Congress enacted and the President signed the CLOUD Act, which added a provision: "A provider of electronic communication service or remote computing service shall comply with the obligations of this chapter to preserve, backup, or disclose the contents of a wire or electronic communication and any record or other information pertaining to a customer or subscriber within such provider’s possession, custody, or control, regardless of whether such communication, record, or other information is located within or outside of the United States."

(CLOUD Act §103(a)(1)) [11]. This means that although the data was stored in Ireland, Microsoft, as the data controller located within the U.S., is obliged to provide user data to the U.S. government.

The U.S. data controller model was established to meet domestic judicial needs. On one hand, the U.S. can bypass the MLAT process and directly obtain data stored abroad, circumventing traditional data localization standards. On the other hand, as a global internet leader with companies like Amazon, Facebook, Google, and Twitter, the U.S. has access to substantial user information, enhancing its data resources for governmental use.

3.2. Interpretation of the Legislative Background of the EU Cross-Border Data Collection Model

The GDPR extends and refines the existing requirements of the 1995 Data Protection Directive. In the EU, privacy is considered a human right, which is the foundation of the EU's strong approach to personal data protection [12]. The Data Protection Directive represented the EU's earliest unified framework for personal data protection. However, over time, it proved insufficient in addressing the needs posed by modern information technologies and the evolving internet ecosystem. When the 1995 law was enacted, the internet was still in its early stages, unable to foresee the technological advancements and complex data ecosystems that would follow, necessitating updated legislation.

First, the enforcement of the Data Protection Directive lacked sufficient deterrence against illegal conduct. For example, in 2017, France's data protection authority fined Facebook €150,000 after discovering it had collected large amounts of user information for targeted advertising. Compared to Facebook's quarterly revenues in the billions, this fine was relatively insignificant.

Second, although the Directive had legal force across all EU member states and required them to incorporate its provisions into national law, it was not directly applicable and left room for flexibility in implementation. As a result, member states could create national laws that suited their circumstances, leading to variations in data protection laws across the EU. This lack of uniformity created fragmented regulations, which increased compliance costs and complexity for multinational companies operating in different countries. Prior to the GDPR, each EU member state had its data protection laws, which meant that companies faced diverse legal requirements when operating across borders. The fragmented legal landscape increased compliance costs and complexity.

Third, the EU aimed to boost public trust in the digital economy by encouraging individuals to share data online, while ensuring companies were transparent and responsible in their data usage. By protecting privacy and strengthening oversight, the GDPR sought to foster a more trustworthy digital market environment.

Currently, data protection in the EU is primarily regulated by the GDPR, which took effect in 2018. The GDPR applies directly to all EU member states, providing a unified legal framework for data protection and ensuring coordination across the EU. This eliminates the need for individual member states to create foundational data protection laws parallel to the GDPR, as they now follow its unified rules and standards. Although the GDPR establishes a consistent legal framework, it allows member states to make supplementary adjustments in specific areas to align with their cultural and legal contexts.

4. Relevance of U.S. and EU Cross-Border Data Collection Models for China

4.1. Reasons U.S. and EU Models Cannot Be Directly Implemented in China

First, there is a fundamental conflict in concepts of data sovereignty and differences in institutional backgrounds. CLOUD Act allows its law enforcement agencies to access data stored overseas without always requiring foreign permission. This approach, based on personal jurisdiction, conflicts with China's data sovereignty principles, which mandate that cross-border data transfers must be approved to ensure national security and data sovereignty. Consequently, China is unlikely to accept foreign countries directly accessing data stored within its borders without prior consent. The GDPR, meanwhile, was developed in response to the specific needs of EU member states, a context that does not exist within China.

Second, there are fundamental differences in legal foundations. The legal systems of China, the U.S., and the EU are inherently distinct. The U.S. follows a common law system with flexible interpretations, enabling it to adapt quickly to emerging cross-border data collection issues. The EU benefits from a supranational legal framework that facilitates judicial cooperation among member states. In contrast, China's legal system is based on statutory law, meaning that cross-border data collection issues must be addressed through a strict legislative process, as case law cannot directly expand enforcement powers. This creates legislative challenges for China in adopting models from other jurisdictions.

Third, international cooperation mechanisms are not fully developed. The U.S. and the EU have relatively well-established bilateral and multilateral judicial assistance frameworks, such as the European Investigation Order within the EU. In contrast, China's mechanisms for cross-border data collection are still developing and rely primarily on international criminal judicial cooperation. Due to the lack of a unified international agreement, China cannot, like the EU, rely on a pre-existing judicial cooperation framework to obtain data.

4.2. Drawing Lessons from U.S. and EU Models to Optimize China's Cross-Border Data Collection Strategies

To address challenges in cross-border data collection, China can draw on the experiences of the U.S. and EU, adapting their approaches within the framework of Chinese law and sovereignty requirements to gradually build a more efficient and sovereignty-respecting cross-border data collection mechanism.

First, expanding the international judicial cooperation network can improve evidence collection efficiency [13]. Currently, China's cross-border data collection relies on international criminal judicial assistance, which tends to be inefficient. To enhance efficiency, China could take inspiration from the EU's regional cooperation model by establishing "data-sharing agreements" or "cross-border investigation cooperation agreements" with willing partners. For instance, China could strengthen bilateral and multilateral cooperation with key economic partners and countries along the Belt and Road Initiative, reducing the number of judicial assistance layers to expedite response times. Moreover, similar to the EU's European Investigation Order, China could establish a simplified cross-border data collection process with signatory countries, reducing unnecessary bureaucratic steps to enable rapid data sharing and support in urgent situations.

Second, implementing a data classification management system can allow for more flexible control [14,15]. China could introduce a classification mechanism for cross-border data based on the sensitivity level and actual cross-border data transfer needs, balancing national data security with cross-border cooperation requirements. Data could be classified into three levels: "highly sensitive", "sensitive," and "general." Different data categories would have different transfer and sharing requirements. For instance, highly sensitive data related to national security could be prohibited from being transferred abroad; sensitive data affecting national interests or public security could be allowed to flow abroad only after stringent approval, with explicit standards for storage and transmission; general data (such as non-sensitive data not impacting public interests) could move freely as long as basic legal requirements are met. Additionally, China could establish an outbound security assessment mechanism for sensitive data and, drawing on GDPR's "data transfer safeguard clauses", set essential security and privacy protection standards for cross-border data transfers. This approach would protect national sovereignty while enabling more effective international integration within a compliance framework.

Finally, China could introduce extraterritorial applicability clauses to extend the reach of domestic laws. In cross-border data collection, China could follow the U.S. CLOUD Act's example by imposing legal obligations on data controllers. Regardless of where the data is stored, data controllers with substantial ties to China should be required to comply with Chinese data collection laws. This would help ensure the legality and efficiency of evidence collection and enhance China's control in cross-border data collection. Specifically, clear legal obligations for data controllers could be established, requiring foreign and multinational companies operating in China to cooperate with cross-border data collection efforts per Chinese legal requirements. For non-compliant entities, administrative penalties, restricted market access, or other measures could be applied to improve legal enforcement. Additionally, by specifying clauses for extraterritorial enforcement cooperation, China could mandate that multinational companies comply with Chinese law enforcement requests in specific criminal investigations, facilitating compliant data sharing and reducing obstacles due to jurisdictional conflicts.

By adapting U.S. and EU models to suit its own conditions, China could gradually establish a cross-border data collection mechanism that balances national security and cross-border cooperation, providing comprehensive support for the legality and efficiency of China's cross-border data collection efforts.

5. Conclusions

China currently employs an international criminal judicial assistance model for cross-border data collection. Due to the need for cooperation across different countries and a layered application process requiring formal submissions, this model faces significant challenges in terms of efficiency and authority. China's approach to cross-border data collection, whether for requesting data from other countries or for foreign entities accessing data within China, is centered on respect for national sovereignty and adopts a relatively conservative stance. Although this model maintains national sovereignty to some extent, it falls short as a sustainable solution for resolving conflicts over cross-border data flow.

Drawing on the U.S. and EU models of cross-border data collection, these jurisdictions have expanded the interpretation of their jurisdiction to enable more flexible and assertive cross-border data collection capabilities when accessing data from other countries. However, due to differences in data sovereignty principles, legal systems, and incomplete international cooperation mechanisms, these models cannot be directly applied in China.

Based on this analysis, this paper proposes three recommendations. First, China should expand the number of countries with which it has international criminal judicial assistance agreements. Second, China should establish a data classification management system, setting differentiated access permissions according to the nature of the data and the interests involved, to improve flexibility and adaptability in cross-border evidence collection. Third, China could introduce extraterritorial applicability clauses to enhance the reach of domestic laws abroad. By combining international best practices with China's unique context, this paper aims to provide constructive guidance for improving China's legal framework and operational models in cross-border data collection, offering recommendations for future legislation and practice in this field.

References

[1] Supreme People's Procuratorate of the People's Republic of China. (2020) Gazette of the Supreme People's Procuratorate of the People's Republic of China, 176(3), 19-23.

[2] *Liang Kun. (2019) The Development Trends of the EU's Fast-Track Cross-Border Electronic Evidence Collection System and Its Implications, Journal of People's Public Security University of China (Social Sciences Edition), 35(1), 33-43.*

[3] *Liao Bin, Liu Minxian. (2021) Research on the Cross-border Electronic Evidence Collection under the Conflict of Data Sovereignty Jurisdiction. Law Science Magazine, 42(8), 147-161.*

[4] *Liang Kun. (2019) A National Criminal Evidence Collection Jurisdiction Model Based on Data Sovereignty, Chinese Journal of Law, 41(2), 188-208.*

[5] *U.S. Department of Justice. (2019) Promoting Public Safety, Privacy, and the Rule of Law Around the World: The Purpose and Impact of the CLOUD Act. Retrieved from https://www.justice.gov/opa/press-release/file/1153446/dl.*

[6] *CLOUDIAN. (2024) What Is Data Sovereignty?--Challenges and Considerations. Retrieved from https://cloudian.com/guides/data-protection/data-sovereignty-in-the-cloud-key-considerations/.*

[7] *Law Enforcement Access to Data Stored Abroad (Act S.512). Retrieved from https://www.congress.gov/bill/114th-congress/senate-bill/512/text.*

[8] *International Communications Privacy Act. (S.1671) Retrieved from https://www.congress.gov/bill/115th-congress/senate-bill/1671.*

[9] *United States v. Microsoft Corp., 584 U.S. (2018).*

[10] *Stephen P. Mulligan. (2018) Cross-Border Data Sharing Under the CLOUD Act. Washington: Congressional Research Service.*

[11] *CLOUD Act (H.R.4943). Retrieved from https://www.congress.gov/bill/115th-congress/house-bill/4943.*

[12] *Hoofnagle, C. J., van der Sloot, B., Borgesius, F. Z. (2019) The European Union general data protection regulation: what it is and what it means. Information & Communications Technology Law, 28(1), 65-98.*

[13] *Yun Yi, Ji Zhaoyang. (2024) Governance Challenges and Responses to Cross-Border Electronic Evidence Collection in the Era of Big Data. Journal of CUPL, 4, 180-191.*

[14] *Tang Binbin. (2020) Research on Cross-border Data Collection in Criminal Justice. The Jurist, 4, 156-170+196.*

[15] *Zhao Haile. (2024) On the Conflict Between U.S. Cross-Border Electronic Evidence Collection and China's Data Security Legislation and Countermeasures. Journal of Anhui University (Philosophy and Social Sciences Edition), 48(01), 100-108.*