International Journal of Arts Humanities and Social Sciences Studies
Volume 11 Issue 8 ǁ August 2026
ISSN: 2582-1601
www.ijahss.com

EU Reforms to Jurisdiction over the Cross-Border Acquisition of Electronic Evidence in Criminal Matters and Their Implications for China

Yibo Ma
（Law School, Beijing Normal University, Beijing 100875, China）

ABSTRACT: *The cross-border acquisition of electronic evidence is essential to combating transnational cybercrime. Within the European Union, the jurisdictional basis for obtaining electronic evidence across borders has shifted from a data-location model to a data-controller model, a transition formally embodied in the regime of European Production and Preservation Orders. Although this reform has progressively improved the efficiency of evidence gathering in the EU, it also poses challenges to China's data sovereignty. China currently applies a data-location model: Chinese authorities exercise direct jurisdiction over electronic evidence stored within China, while evidence stored abroad must generally be obtained through international mutual legal assistance in criminal matters. This model is inefficient in bilateral cooperation and is increasingly ill-suited to the mobility of data and the complexity of cybercrime locations. China should therefore respond to both the efficiency gains and the sovereign challenges produced by the EU model and reconstruct its rules on jurisdiction over cross-border evidence gathering with the protection of national sovereignty as the primary objective. Specifically, China should retain the data-location model as the foundation, cautiously incorporate a data-controller connecting factor, classify data according to type and sensitivity, and establish a system under which overseas data controllers may directly participate in and cooperate with Chinese criminal proceedings. These measures would help balance the protection of China's data sovereignty with the lawful and orderly flow of data.*

Keywords: cross-border acquisition of electronic evidence; data location; data controller; data sovereignty.

I. Introduction

The rapid development of the Internet has created fertile ground for information-network crime, which is increasingly transnational and complex. In cross-border cybercrime cases, evidence is often distributed in data form across multiple sovereign States. States must therefore overcome territorial barriers and obtain such evidence through international mutual legal assistance in criminal matters.

Bilateral mutual legal assistance safeguards procedural legality, but it's complicated procedures and the involvement of numerous authorities often make evidence gathering inefficient. Cooperation may also be unavailable because no bilateral framework exists or because the requested State is unwilling to assist. How China should reform its current mutual-assistance mechanism for obtaining data has consequently become a pressing issue.

Legal protection for data varies among States, and the international community still lacks a unified and comprehensive jurisdictional mechanism for cross-border cybercrime investigations. Conflicts of judicial sovereignty may therefore arise in practice. Reducing jurisdictional conflict when obtaining electronic evidence abroad is crucial to China's efforts to combat transnational cybercrime and establish an efficient system for acquiring electronic evidence in criminal matters. China currently determines jurisdiction in mutual-assistance evidence gathering primarily by reference to the location of the data. Under the "data-location" model, once Chinese judicial authorities have jurisdiction to investigate a cybercrime, they may directly obtain data stored within China. If electronic evidence is stored abroad but controlled by a network service provider that offers goods or services in China and holds evidence essential to the case, Chinese authorities must ordinarily obtain it through international mutual legal assistance and may not directly compel the service provider to cooperate. By contrast, EU Member States have promoted a "data-controller" model. Under this model, a State may exercise direct evidence-gathering jurisdiction over electronic evidence held by a data controller that provides substantial services within the forum, even when the data are physically stored abroad. The extraterritorial shift from territorial jurisdiction to personality-based jurisdiction challenges China's jurisdiction over criminal data. A Chinese network service provider that offers services in the EU may fall within EU jurisdiction under the data-controller model. China's current rules, however, remain incomplete. They continue to rely on territoriality, do not yet provide a mature system for classifying data by type and sensitivity, and generally require all foreign-

stored data to be obtained through traditional mutual legal assistance. Nor has China established a legal mechanism authorizing judicial authorities to require overseas data controllers to cooperate directly. As a developing country, China differs from the EU in the degree of data openness and in restrictions on cross-border data flows. Against the background of the EU's jurisdictional transformation, China must consider how to improve its own model and overcome the institutional bottlenecks in cross-border evidence gathering.

II. Expansion and Reform of the EU Model for Cross-Border Electronic Evidence

2.1 From the European Investigation Order to European Production and Preservation Orders

The first EU-wide measure to apply the principle of mutual recognition to evidence gathering was the European Evidence Warrant. Its scope was limited, however, and after the Treaty of Lisbon entered into force, judicial cooperation in EU criminal matters was placed firmly within a framework based on the mutual recognition of judgments and judicial decisions. To implement that principle more fully, the EU adopted Directive 2014/41/EU regarding the European Investigation Order in criminal matters (the "European Investigation Order") in 2014. The Directive covers virtually all categories of evidence and investigative measures used in criminal proceedings. Whereas the European Evidence Warrant applied only to pre-existing objects, documents, and data, the European Investigation Order expanded the scope of evidence gathering to include statements by suspects and witnesses, forensic samples, and the interception of telecommunications. Some of these materials require further analysis or interpretation before they can be used. Articles 24 to 27 also extend the available investigative techniques to measures such as hearings by video-conference or telephone conference and access to bank-account and banking-transaction information. Nevertheless, although the European Investigation Order organizes judicial cooperation around the State in which data are located, it does not expressly resolve territorial jurisdiction over cross-border electronic evidence or establish a duty for network service providers to give evidence remotely.

The Belgian Yahoo! case was among the first to reveal the inadequacy of traditional territoriality in the data era. In 2007, while investigating fraud committed through the Internet and computer systems, Belgian police sought user email information from Yahoo! to identify the suspects. Yahoo! argued that it was not an electronic communications service provider established in Belgium, that Belgian prosecutors therefore lacked jurisdiction over its electronic data, and that the evidence had to be obtained through mutual legal assistance. The Belgian Court of Cassation ultimately held that Yahoo! was required to comply because it provided substantial commercial services in Belgium. The decision moved beyond strict data localization by treating the data controller's "commercial presence" in the forum—measured by the services it offered there—as a sufficient jurisdictional connection. Its importance extended beyond the individual dispute: it marked an adaptive shift from a legal order organized around physical space to one capable of governing digital space and helped create the data-controller standard as a new connecting factor for evidence-gathering jurisdiction.

With the emergence of the data economy, enhanced cooperation in criminal-data investigations is widely expected to become the dominant direction of development, and limited exceptions to ordinary data-protection rules may be justified. The mobility of electronic evidence and the rise of cloud storage have eroded traditional territorial barriers. These technological changes have reconfigured the spatial dimension of EU evidence law and made cross-border electronic evidence less dependent on the geographical boundaries of conventional jurisdictions. In the EU, a service provider's place of establishment may be separated from the territory in which its services are supplied. Microsoft Azure, for example, opened its first European data center in Ireland in 2009, marking the formal expansion of its cloud-computing services in Europe. Beginning in 2007, the United States-based Amazon Web Services established eight data centers in Europe as major hubs for cloud computing and regional operations, while its cloud-processing infrastructure came to cover availability zones in several EU Member States. The separation of the locations of storage, processing, and service establishment directly challenged rules for obtaining electronic data that were connected solely to territory. Yet the resulting jurisdictional disputes were neither addressed in the relevant EU legislation of the time nor resolved by the European Investigation Order. The traditional model was ultimately displaced by the General Data Protection Regulation (GDPR) and Regulation (EU) 2023/1543 on European Production Orders and European Preservation Orders for electronic evidence in criminal proceedings and for the execution of custodial sentences following criminal proceedings (the "European Production and Preservation Orders Regulation").

2.2 Establishment of the Data-Controller Model

The European Production and Preservation Orders Regulation departs from the traditional data-location model and uses a data-controller connecting factor to determine jurisdiction over electronic evidence. Recital 21 makes clear that application of the Regulation should not depend on the actual location of the service provider's establishment or its data-processing or storage facilities. Article 2(1) and Article 26 confine the regime to service providers offering services in the Union. A provider established in the EU but not substantively offering

services there falls outside its scope. The Regulation thus reduces the role of territoriality and relies instead on a personality-based connection. It codifies the central proposition of the Belgian Yahoo! decision: the geographical scope of services can determine the duty to assist in evidence gathering. Put differently, the location of the data is less important when European Production or Preservation Orders are issued, while the provider's offering of services in the EU becomes decisive. By enabling authorities to obtain evidence directly from service providers rather than proceeding solely through competent authorities in another State, the Regulation has become a central legal instrument for cross-border electronic evidence in the EU.

Some scholars argue that the GDPR first expanded the EU's jurisdictional reach in this field. Yet Article 2 excludes processing by competent authorities for the purposes of preventing, investigating, detecting, or prosecuting criminal offenses or executing criminal penalties. Although the GDPR did not formally establish a data-controller basis for criminal-evidence jurisdiction, it broadened the concept of the data controller and extended the EU's jurisdictional framework. Cross-border criminal evidence cannot be obtained directly by invoking the GDPR's expanded controller provisions, but multinational service providers that serve the EU market voluntarily subject themselves to EU data-privacy requirements. In such cases, the provider's place of establishment, the place of processing, and the jurisdiction in which services are supplied may diverge. Under Article 3(1) of the GDPR, processing in the context of the activities of an establishment of a controller or processor in the EU is subject to the Regulation regardless of whether the processing itself takes place in the EU. Read together, Article 3(1) and 3(2) extend the GDPR through both an establishment-based criterion and a market-targeting criterion. Processing by a controller or processor is covered when either criterion is met. The data-controller standard is therefore best understood as an extension built upon, rather than an absolute rejection of, the data-location standard.

EU legislation also increasingly requires data controllers or service providers to assist judicial authorities directly. The Belgian Code of Criminal Procedure, for example, authorizes prosecutors in criminal investigations to request identity information in writing from electronic communications providers and to use monetary penalties to secure compliance within the prescribed period. Under the European Production and Preservation Orders Regulation, a network service provider offering services in the EU must directly comply with a requesting authority's order for electronic evidence. The accompanying European Production Order Certificate (EPOC) further confirms that, when both the issuing and enforcing States are Member States, the issuing authority may require the addressee in the enforcing State to provide subscriber, access, transaction, and content data These provisions require service providers to participate directly in criminal proceedings and cooperate in evidence gathering, thereby materially increasing efficiency.

2.3 Characteristics of the Data-Controller Model

Compared with a jurisdictional rule based on data location, the data-controller standard has three principal characteristics. First, it moves beyond traditional mutual legal assistance and uses uniform regional legislation, rather than bilateral treaties, as the legal basis for direct evidence gathering by authorities within the EU. Second, it imposes a direct duty on the data controller to assist international criminal justice and affirmatively develops the power of judicial authorities to obtain data abroad. As a responsible legal actor, the controller assumes clearer obligations in cross-border cybercrime investigations and functions as a special participant in proceedings, communicating directly with the requesting authority and taking part in the acquisition of electronic evidence. This raises the question whether China might introduce a comparable mechanism under which service providers participate procedurally and assist remote evidence gathering. Third, whereas the data-location rule permits a sovereign State to localize jurisdiction over electronic evidence generated within its territory and thereby protect its data sovereignty, the data-controller standard links protection and jurisdiction to the geographical scope of services. A State no longer claims absolute control over all data within its territory solely by virtue of territorial location, and the concept of data sovereignty is correspondingly weakened. The standard may also intensify conflicts of law. A single controller's services and processing activities may span several sovereign States. If several States claim jurisdiction over the same data on that basis, or if the requesting and executing States apply different jurisdictional rules, overlapping claims and competing laws will become more pronounced. EU States applying the standard may therefore need multilateral coordination mechanisms to reconstruct the framework for cross-border electronic evidence and bridge conflicting assertions of data sovereignty.

The transformation of the EU model has progressively increased efficiency. One scholar describes the change as a shift from an "inverted-U" mutual-assistance procedure to a "straight-line" procedure of direct cooperation. Under the traditional inverted-U model, a request passes through authorities at different levels in both States and is subject to repeated transmission, review, and negotiation, producing delay and uncertainty. By contrast, Article 8 of the European Evidence Warrant provided for direct cooperation between the issuing and executing authorities, with evidence obtained in accordance with the law of the executing State. Article 7 of the

European Investigation Order restated the same basic arrangement. By reducing the number and hierarchy of participating authorities, the procedure transfers or simplifies work previously handled by central authorities in the requested State and thereby reduces procedural complexity. The European Production and Preservation Orders Regulation retains this straight-line structure and grants the issuing authority the power to obtain electronic evidence directly from the service provider.[1] In specified circumstances, the issuing State can therefore direct a data. controller under a clear legal framework without first obtaining the consent of the authorities in the provider's home State. This greatly simplifies service providers' responses to cross-border orders, lowers compliance costs, and encourages more active cooperation with law-enforcement investigations.

III. Problems with China's Current Jurisdictional Model

The Law of the People's Republic of China on International Criminal Judicial Assistance, enacted in 2018, established a basic framework under which China's cross-border acquisition of electronic evidence is grounded in the protection of national sovereignty and continues to follow the data-location model. The rise of the EU's data-controller approach, however, has exposed the limitations of China's current rules. China has not yet developed a systematic and comprehensive framework capable of responding effectively to the expansion of personality-based extraterritorial jurisdiction and the resulting challenges to Chinese judicial sovereignty.

3.1 Principal Difficulties of the Data-Location Model

3.1.1 Inefficiency of Bilateral Mutual Legal Assistance

A system based on the location of data involves complex procedures. Under the inverted-U structure described above, traditional mutual legal assistance proceeds under bilateral or multilateral treaties: the investigating authority in the requesting State first reports to its competent authority, after which the central or liaison authority transmits the request to the competent foreign authority. This multilevel process is cumbersome and requires the approval and cooperation of numerous bodies. Bilateral mutual legal assistance also takes too long. Criminal investigations often begin sometime after an offence was committed, while electronic evidence is highly mobile and susceptible to destruction or alteration. The long cycle of territoriality-based bilateral assistance makes it difficult to ensure that data remain intact. Finally, China continues to apply traditional jurisdictional principles and has not yet joined a unified international cooperation model. Differences between the requesting and executing States' rules restrict evidence gathering based on data location. A request made without sufficient understanding of the executing State's law and procedure may be refused for non-compliance with local procedural requirements, adding further complexity. Differences in investigative processes and legal interpretation may also impede timely cooperation.

3.1.2 Difficulty Accommodating the Dynamic Mobility of Data

(1) Uncertain Storage Locations in the Era of Cloud Computing

The rapid development and widespread use of cloud storage mean that data are no longer fixed on a particular physical device or server in a single geographical location. Distributed architectures and virtualization disperse them across multiple data centers, regions, and States. This flexible arrangement increases scalability and concealment, while making the actual storage location uncertain and dynamically variable. A traditional mechanism that identifies the law-enforcement authority at the company's place of establishment as the appropriate cooperation partner is therefore increasingly limited: prosecutors seeking evidence may be unable to identify where it is actually retained. Even where the data are known to be in the controller's cloud environment, synchronized backups on servers in multiple States may make it unclear which executing State and which cooperation procedure should be used. Cloud technology thus requires a departure from rigidly territorial bilateral assistance. Some service providers use technical means to conceal storage paths and reduce legal exposure, making case-related information more anonymous. Where the storage location cannot be identified and no simplified assistance mechanism exists, China should adjust the territorial principle that currently dominates its rules for cross-border electronic evidence.

(2) Separation of the Place of Storage from the Place of Access

The physical separation between the location at which data are stored and the location from which they are accessed is changing the logic of jurisdiction over electronic evidence.[2] In traditional evidence gathering, the physical location of evidence often coincided with the sphere of activity of its owner or controller. Electronic evidence is far more mobile. China may therefore encounter cases in which the target data are located in one sovereign State while the controller is incorporated in another. When storage and management are separated from actual access and use, it becomes difficult to identify the executing jurisdiction to which China

should direct a request under the data-location principle. Data controllers may also maintain branches in several States, and it is quite common for headquarters and branches transmit data via storage media overseas.The actual processing of electronic evidence may not occur where the service provider is established. Although the data-location model protects data security, it also constrains information exchange and data circulation. Subject to safeguarding data sovereignty, China should systematically improve its traditional assistance process and develop effective paths for accessing and acquiring electronic evidence.

3.2 The Impact of the EU Data-Controller Model on China's Data Sovereignty

The data-location standard is a concrete extension of national data sovereignty. Because no unified international model for data governance has emerged, institutional competition over data jurisdiction is in substance a competition to protect sovereignty, security, and developmental interests. To regulate cross-border processing and prevent risk, China requires that a sound data-security governance system should be established.[3]China also requires that certain data should be strictly assessed when network data processors provide abroad.[4] Cross-border law-enforcement access to data is an important application of data sovereignty and should likewise be guided by sovereign equality.[5] China's localization requirements for important data and its use of the data-location model to limit foreign enforcement powers are therefore expressions of respect for and protection of national data sovereignty.

Under the European Production and Preservation Orders Regulation, network service providers that offer services in the EU are subject to its rules. Neither the provider nor its branches must necessarily be incorporated in the EU; offering services there is sufficient to trigger the data-controller connecting factor. Consequently, even without an EU branch, a Chinese service provider offering services to EU users may be required under EU law to produce evidence in criminal cases, including data stored on its servers. China's unexpanded territorial model is comparatively passive. When Chinese authorities seek criminal evidence from overseas controllers, they cannot impose an equivalent direct duty on a controller that stores and processes data abroad but provides substantial services in China. This asymmetry between outward data flows and restricted inward access produces several risks. First, the EU model may adversely affect China's control over outbound data. China has established a security-assessment mechanism to promote the secure and orderly flow of data and prevent harm to national security and public interests. The EU's personality-based model allows an issuing authority to compel a Chinese data controller directly, bypassing the traditional inverted-U structure. Unless China classifies cross-border data and conducts tiered security-risk assessments, data capable of harming sovereignty or public interests may leave the country in a disorderly manner. If China does not adapt its evidence-gathering system to this non-territorial model, it may be unable to effectively protect data. Second, the departure of developed States from territorial jurisdiction reinforces their dominant position as data powers. The resulting jurisdictional imbalance increases the pressure on China to protect sovereignty and security and coordinate conflicting laws. China's rules on data circulation and legal application remain less developed than those of major data powers; failure to adjust the existing system may further weaken China's voice in the formation of cross-border data rules. Chinese service providers may also face internal compliance and risk-control pressures if they lack robust data-security awareness or standardized processing and storage practices, thereby producing additional negative effects on China's data sovereignty.

IV. China's Response: Cautious Incorporation and a Direct-Participation Mechanism

The expansion of EU evidence-gathering jurisdiction has intensified conflicts between China and other States in criminal justice. At the same time, the EU's shift toward a model centered on the data controller offers useful guidance for a safer and more efficient Chinese mechanism. To protect national data sovereignty and regulate cross-border evidence gathering, China should preserve the data-location principle as the foundation, cautiously open access to selected categories of data, and explore a duty under which overseas data controllers directly participate in and assist Chinese criminal proceedings.

4.1 Cautious Incorporation of the Data-Controller Connecting Factor

Most scholarship on China's jurisdictional model argues that the data-location approach should remain in place.[6][7] Some scholars favor a transition toward the data-controller model and a Chinese form of personality-based evidence-gathering jurisdiction.[8] Others propose a mixed model that treats localization as the primary standard and control as a supplementary standard, using limited access rights to meet the needs of cross-border investigations.[9] This Article argues that China should continue to base protection of electronic data on storage location and exercise unquestioned jurisdiction over important data stored within China, while selectively drawing on the EU approach to facilitate lawful outbound data flows.

4.1.1 Retaining the Data-Location Rule for Core Data Implicating Major Interests

First, localized storage is an expression of China's data sovereignty and the holistic approach to national security. China treats the inviolability of national sovereignty as the basic premise of cross-border electronic evidence gathering and has traditionally adopted a relatively defensive strategy.[10] In November 2024, China issued the Global Initiative on Cross-Border Data Flows Cooperation, which advocates openness and active cooperation while respecting lawful measures adopted by States to protect national security, public interests, and personal privacy.[11] The Initiative confirms that sovereignty and security remain primary concerns. Traditional mutual legal assistance is compatible with China's present conditions and should remain the principal channel for strengthening judicial cooperation with executing States. Any departure from the data-location model must therefore respect national sovereignty and should occur only where risks to national information security, trade secrets, and personal privacy are sufficiently limited and where greater data mobility is necessary to meet international criminal-justice needs.

Second, treating data location as the primary connecting factor is consistent with the cross-border evidence needs of most States. Article 22 of the 2001 Budapest Convention on Cybercrime establishes territorial jurisdiction. In August 2024, the UN Ad Hoc Committee approved the draft United Nations Convention against Cybercrime. The draft prohibited a State Party from exercising jurisdiction or performing functions in the territory of another State that are reserved exclusively to the authorities of that other State.[12] It translated cyber-sovereignty into a binding legal principle and required respect for sovereign equality, territorial integrity, and non-intervention. This demonstrates that, despite the distinctive characteristics of electronic evidence, territorial boundaries of storage and processing remain practically significant for allocating jurisdiction. The data-location rule serves the developmental interests of most States and gives cross-border data controllers a predictable legal framework. China should therefore continue to prioritize sovereignty and security and use the location of important data as the principal jurisdictional connection.

Third, the EU's economic strength has enabled it to lead in developing open access to data, but a highly liberal model of data movement does not fully correspond to China's present stage of development. As a developing country undergoing digital transformation, China faces a more complex geopolitical environment. The EU, as a mature economy, has greater influence over international rule-making and uses the data-controller model to promote cross-border openness and the digital economy. Its rules for criminal-data flows focus more on operational convenience than on resisting threats to national data sovereignty. Jurisdictional conflict over cross-border data is an inevitable feature of the digital age and reflects a deeper tension between national sovereignty and the shareable nature of data.[13] China should therefore balance security against mobility and sharing, while continuing to rely on data location for non-public evidence implicating national security or major public interests.

Finally, adopting the data-controller standard as the sole basis of jurisdiction over valuable data generated in China could, in some circumstances, enable Chinese network service providers to avoid domestic law. The standard detaches jurisdiction from territory and instead looks to the place where services are actually offered. A provider incorporated in China but serving users abroad may process the relevant data outside China. If the controller standard alone were applied, the Chinese entity might escape Chinese criminal jurisdiction even though electronic evidence generated through its operations is regulated by EU law. China would thereby lose control over criminal evidence and weaken its practical command of strategic data resources. Conversely, where a Chinese controller neither offers substantial services nor stores data in China, it may owe no duty to testify under a controller-only standard. This would create regulatory gaps and place Chinese criminal regulation at a disadvantage.

4.1.2 Moderately Opening Access to Ordinary Data Not Implicating Major Interests

The data-location model is a justified jurisdictional foundation for protecting strategic data, but it should not be treated as absolute. Subject to strict protection of national security and core interests, China may develop a more flexible cross-border mechanism for ordinary electronic evidence whose risks are controllable. Such a mechanism would supplement and flexibly apply the data-location model in response to practical needs for judicial cooperation; it would not abandon the principle itself.[14]

Procedural design should therefore classify electronic evidence by importance and confidentiality. While respecting national sovereignty, China may simplify cross-border procedures in low-risk cases and permit foreign requesting States to obtain access to ordinary data. Electronic evidence may be divided according to the interests it implicates: national interests, public interests, and individual interests. First, China should strictly control cross-border movement of data implicating core or major national interests. This requires both stringent legal restrictions on providing domestic criminal electronic evidence abroad and security assessment and legal review of foreign data entering China for use in criminal proceedings. Second, data involving public or individual interests should be managed through differentiated rules that fully protect the rights of data subjects.

One scholarly classification divides public-interest data into four categories: data protecting citizens' fundamental rights; data protecting public safety, including life, health, and the ecological environment; data protecting State-owned assets, including natural resources and biochemical energy resources; and data safeguarding the legal order.[15]Some of such data are of high importance and sensitivity, direct access could result in misinterpretation or misuse, unnecessary public panic, and threats to public order. Thus, their movement should occur through secure and controllable channels under strict legal and security assessments. Where acquisition of public-interest data creates no material risk and complies with Chinese law, procedures may instead emphasize efficient and secure two-way flows. This includes streamlined receipt of qualifying data lawfully obtained abroad and more convenient channels for lawful outbound transfers. Personal information is both a marker of individual identity and a digital link through which social relationships are formed. Obtaining sensitive or non-public personal information in criminal proceedings may threaten privacy and information security. China should therefore establish a tiered mechanism for two-way movement and, for information that is not materially private, optimize acquisition procedures while fully protecting the data subject's right to be informed.

A limited departure from the data-location principle after security assessment is a reasonable response to the mobility of data and can create a more efficient route for cross-border criminal cooperation. In a foreign investigation, the need for access may arise abroad while data generated and processed by servers remain stored in China. Subject to protection of China's data sovereignty, a controlled exception would enable foreign States to obtain ordinary electronic evidence stored in China and investigate offenses involving Chinese data more efficiently. It would also ease the bottlenecks of the traditional inverted-U process. Opening access to ordinary data may help China secure reciprocal treatment when it seeks non-core and non-sensitive electronic evidence abroad and promote more efficient bilateral rules. By eliminating unnecessary approvals, this mechanism could balance efficiency and data security, improve the quality of Chinese criminal investigations, and better accommodate rapid data movement.

In sum, China's cross-border criminal investigations cannot presently be detached from the basic framework of data localization. Rule-making must carefully balance data sovereignty against the need for cross-border movement. Core data concerning national security should remain subject to strict localization, while ordinary data presenting controllable risks may be governed by streamlined and efficient procedures.[16] China should therefore retain the data-location model as the primary rule while simplifying procedures for ordinary data, thereby modernizing its system for acquiring electronic evidence.

4.2 Establishing Direct Participation and Cooperation Duties for Overseas Data Controllers

The idea of simplifying procedures while protecting data security can be extended to cross-border criminal investigations. At the fifth meeting of the UN intergovernmental expert group on cybercrime in March 2019, experts recognized that network service providers controlling large quantities of data should play an important role in law enforcement and supported exploration of new evidence-gathering models and stronger international governance of cybercrime.[17] Professor Liu Pinxin similarly proposes treating the data controller as a special participant in proceedings whom investigators may directly require to download and submit data remotely.[18] Some data involving public interests or personal information are not highly sensitive, and their lawful movement would not materially harm national data sovereignty, public order, or individual rights. China's system may therefore be adjusted according to data type. Data implicating national sovereignty, and categories of public-interest or personal data that should not circulate, should continue to be obtained from overseas controllers through international mutual legal assistance because direct contact may challenge foreign judicial sovereignty. For public-interest or personal data that may lawfully circulate, China may draw on the EU experience while retaining the data-location foundation and permit an overseas controller, as a legally recognized participant in proceedings, to submit evidence remotely and directly to Chinese judicial authorities. This mechanism would protect overall data security while simplifying the movement of selected categories of data.

Chinese administrative law already requires domestic data controllers to cooperate directly with investigations and provide information. Article 13 of the 2013 Regulation on the Protection of the Right to Network Dissemination of Information permits copyright-administration authorities to require network service providers to disclose the name, contact details, network address, and other information of users suspected of infringement. The Regulations on Network Data Security Management, effective from January 2025, likewise require network data processors that discover clues to network-data offenses to report them to the competent authorities and cooperate with investigation, inquiry, and handling. In criminal matters, however, Chinese authorities still generally request cooperation from overseas data controllers through another State unless data are first classified and procedures simplified. Under Article 31 of the Law on International Criminal Judicial Assistance, an overseas witness or expert may participate by video or audio only after the Chinese competent

authority requests cooperation from the foreign State and receives approval. China has not yet established direct coordination with overseas data controllers in international criminal judicial assistance.

Direct cooperation by overseas data controllers would produce substantial efficiency gains. First, it would alleviate the long duration and procedural complexity of traditional bilateral assistance. Under the inverted-U structure, requiring an overseas controller to provide evidence remotely entails an application by China's central authority to the cooperating State, followed by foreign approval and coordinated execution. A system of remote submission and cooperation modeled on the EU's straight-line procedure would simplify this process and allow an overseas controller to provide evidence directly to Chinese authorities even when it has no presence in China. Second, it would reduce the high cost of obtaining electronic evidence abroad. For non-sensitive and non-harmful data that may lawfully move across borders, Chinese authorities could require the overseas controller and relevant personnel to participate remotely and submit evidence without on-site execution by the authorities of the executing State. This would enable direct acquisition at the source and materially lower costs. Third, direct remote participation as a procedural participant would improve the quality and efficiency of criminal adjudication. Evidence held by an overseas controller is often original and direct. Simplifying acquisition of low-risk data and allowing the controller to participate as a witness would enhance adversarial examination. Investigators, prosecutors, and the defense could directly question the controller about the source, integrity, and extraction method of the data. Direct participation would therefore increase the transparency and reliability of the evidentiary chain, assist accurate fact-finding, and improve case-handling efficiency.

A mechanism under which overseas data controllers communicate directly with Chinese judicial authorities, participate in proceedings, and submit evidence would also better reflect the mobility of data. In an environment of cloud storage and distributed processing, it would create a secure and targeted channel for specified categories of case-related data. When Chinese authorities request evidence and acquisition does not impair the cooperating State's data sovereignty, direct cooperation by the controller would permit precise and efficient movement of the required materials. The mechanism is, in substance, a flexible exception to the data-location model that remains grounded in the protection of data sovereignty. Moreover, the increasing dynamism and dispersal of data, the large number of remote servers, and the involvement of multiple enforcement bodies make investigations complex. Data controllers possess technical, resource, and operational advantages and are better positioned to understand network technologies, key user information, and the distribution of data processing.[19] Their direct participation can shorten investigations, accelerate case progress, and adapt evidence gathering to dynamic data flows. Cloud storage also makes preservation and backup easier and reduces the risk that data will be destroyed or altered. Even when the original data are not stored on a controller's own physical server, the controller may still be able to retrieve relevant electronic evidence. Requiring the overseas controller to cooperate and give evidence can therefore preserve the timeliness, authenticity, and integrity of the evidentiary materials.

V. Conclusion

Cross-border acquisition of electronic evidence rests on effective cooperation and mutual assistance among sovereign States in criminal justice. China should treat reform of its cross-border evidence-gathering model as a central component of combating transnational cybercrime and improving international criminal judicial assistance. In responding to the EU's shift toward the data-controller model, China should seek common ground while preserving legitimate differences and combine institutional continuity with innovation, treating the protection of data sovereignty as the foundation of rule-making. For most cross-border data, the location of storage should remain the principal jurisdictional connection because that rule corresponds to China's present conditions and developmental interests. At the same time, China should improve cooperation procedures, moderately open access to non-sensitive data that may lawfully circulate, and develop a system of direct cooperation and participation between overseas data controllers and Chinese judicial authorities. Such a system would contribute a Chinese approach to international criminal-justice cooperation and provide institutional support for improving cross-border evidence gathering while protecting national data sovereignty.

References

[1] EUROPEAN PARLIAMENT AND COUNCIL. Regulation (EU) 2023/1543, Article 5(6).

[2] Lawrence Siry, Cloudy Days Ahead: Cross-Border Evidence Collection and Its Impact on the Rights of EU Citizens, New Journal of European Criminal Law, 10, 2019, 247.

[3] NATIONAL PEOPLE'S CONGRESS OF THE PEOPLE'S REPUBLIC OF CHINA. Data Security Law of the People's Republic of China, Article 4 [Z]. 2021.

[4] STATE COUNCIL OF THE PEOPLE'S REPUBLIC OF CHINA. Regulations on Network Data Security Management, Article 37 [Z]. 2024.

[5] Sun Nanxiang, Zhang Xiaojun,On Data Security—An Examination of Game and Cooperation in Cyberspace, Pacific Journal, 23(2), 2015, 68.
[6] Liao Bin, Liu Minxian,Research on the Cross – border Electronic Evidence Collection under the Conflictof Data Sovereignty Jurisdiction, Law Science Magazine, 330(8), 2021, 157.
[7] Xie Xiaojian, Shan Senlin,The Dilemma and Solutions of Cross-border Electronic DataCollection in Criminal Cases, Inner Mongolia Social Sciences, 45(6), 2024, 83.
[8] Chen Li,China's Response to Cross-border Electronic Evidence Collection, Journal of National Prosecutors College, 30(5), 2022, 35.
[9] Chen Aifei,The "Data Controller Standard" Forensics Model and Its Response in China, Studies in Law and Business, 3, 2024, 49.
[10] Hong Yanqing,Cross-Border Access to Data for Law Enforcement Purpose in the Context of Conflict of Laws: Case Studies on the U.S., EU and China. Global Law Review, 43(1), 2021, 49.
[11] Yang Jie, Global Initiative on Cross-Border Data Flows Cooperation Released, China Securities Journal, 21 November 2024.
[12] Article 5 of United Nations Convention against Cybercrime.
[13] Wang Gang, Ren Simin, Zhang Aiyun, Legal Difficulties in the Contest over Data Sovereignty and Conflicts of Cross-Border Jurisdiction, People's Court Daily.
[14] Liang Kun, Data Sovereignty-based Mode of National Jurisdiction over the Collection of Criminal Evidence, Chinese Journal of Law, 41(2), 2019, 206.
[15] Zhao Wanyi,On Application Methods of the Social Public Interest in Private Law, Social Sciences in China, 9, 2024, 60.
[16] Wu Xuan,Cross-border Enforcement of Data under Cloud Computing: U.S. CLOUDAct and China's Proposal, Local Legislation Journal, 3, 2022, 109.
[17] Huang Daoli, Research on the Rule of Law in Cybersecurity 2020,(Huazhong University of Science and Technology Press, 2020).
[18] Liu Pinxin, EU's Approach to Cross-border Electronic Evidence Collection and Its Enlightenment to China, Journal of National Prosecutors College, 30, 2022, 22.
[19] Pei Wei,Access to Data from Internet Service Providers: The Origins, Obstacles and Construction of the NewModel of Cross-Border Digital Investigation, Hebei Law Science Journal, 4, 2021, 62.