

**INTERNATIONAL JOURNAL OF LAW
MANAGEMENT & HUMANITIES**
[ISSN 2581-5369]

Volume 9 | Issue 4

2026

© 2026 *International Journal of Law Management & Humanities*

Follow this and additional works at: <https://www.ijlmh.com/>

Under the aegis of VidhiAagaz – Inking Your Brain (<https://www.vidhiaagaz.com/>)

This article is brought to you for free and open access by the International Journal of Law Management & Humanities at VidhiAagaz. It has been accepted for inclusion in the International Journal of Law Management & Humanities after due review.

In case of **any suggestions or complaints**, kindly contact support@vidhiaagaz.com.

To submit your Manuscript for Publication in the **International Journal of Law Management & Humanities**, kindly email your Manuscript to submission@ijlmh.com.

Cross-Border Access to Cloud Data in Criminal Investigations: Legal Challenges and Recommendations for Reforming Vietnamese Law

YEN TRINH THI*

ABSTRACT

The development of cloud computing has given rise to a fundamental paradox in contemporary criminal procedure: while national criminal jurisdiction remains primarily grounded in territoriality, evidentiary data increasingly exists and is controlled beyond the territorial boundaries of the prosecuting state. As transnational service providers hold and manage data essential to criminal investigations through infrastructure distributed across multiple jurisdictions, access to such data has become a critical factor determining the effectiveness of the exercise of criminal jurisdiction. From this perspective, cross-border data issues not only necessitate the development of mechanisms for obtaining electronic evidence but also reflect a broader shift in the exercise of public power from territorial space to data space. Although extensive scholarship has examined electronic evidence, the relationship between criminal jurisdiction, data sovereignty, and cloud service providers' obligations to disclose data remains insufficiently explored in the context of Vietnamese law. Drawing on doctrinal legal analysis and comparative research, this article examines the limitations of the current legal framework governing access to data stored outside the national territory. It argues that the central challenge facing criminal investigations in the digital environment lies not in the technical capacity to collect data, but in establishing a sound legal basis for lawfully accessing cross-border data sources. On this basis, the article proposes reforms to Vietnam's criminal procedural law aimed at establishing an effective framework for cross-border data access while maintaining an appropriate balance between the enforcement of criminal jurisdiction, the protection of privacy, and the preservation of national data sovereignty in the digital age.

Keywords: cloud computing, cross-border data, criminal investigations, data sovereignty, right of access to data

* Author is a Vice Dean at the Faculty of Law, Vietnam Women's Academy, Hanoi, Vietnam.

I. INTRODUCTION

The development of cloud computing is fundamentally transforming the relationship between public authority, territorial space, and data. Traditional criminal jurisdiction is primarily based on territoriality, under which states exercise investigative, prosecutorial, and adjudicative powers over offences committed within their territory and collect evidence through control over persons, property, and information located therein. However, global digital infrastructure is increasingly weakening the traditional link between territorial jurisdiction and access to information for criminal justice purposes.

In cloud computing environments, data is no longer necessarily stored at a clearly identifiable physical location. Instead, it may be distributed across data centres in multiple jurisdictions and controlled by transnational technology companies. Data generated or accessed in Vietnam may therefore be processed, stored, or managed outside Vietnamese territory. As a result, access to data is becoming increasingly detached from territorial control, creating significant challenges for the exercise of criminal jurisdiction.

This development produces a fundamental paradox in contemporary criminal procedure: a state may possess jurisdiction to investigate an offence while lacking direct legal or practical access to the data necessary for that investigation. Data controlled by cross-border service providers has consequently become an increasingly important, and sometimes decisive, source of evidence in cases involving cybercrime, online fraud, money laundering, terrorism, and other offences. The central challenge is therefore shifting from the mere collection of electronic evidence to the establishment of a lawful legal basis for accessing cross-border data.

Unlike the physical environment, where investigative authorities can rely on territorial powers to search, seize, or retain physical evidence, access to digital data may depend on the location of the data, the jurisdiction governing the service provider, personal-data and privacy regulations, and international cooperation mechanisms. Cross-border data access thus lies at the intersection of criminal procedural law, international law, data governance, and cybersecurity law.

International legal developments demonstrate a gradual shift away from exclusive reliance on traditional mutual legal assistance mechanisms toward more direct and efficient forms of access to electronic evidence. The U.S. CLOUD Act, the European Production Order and European Preservation Order mechanisms, and the Second Additional Protocol to the Budapest Convention illustrate different approaches to facilitating lawful access to data controlled by service providers across borders. These developments indicate that the central legal question is

no longer whether electronic data can constitute evidence, but how states may lawfully obtain access to data located or controlled across borders.

In Vietnam, the 2015 Criminal Procedure Code recognises electronic data as a source of evidence, while the 2018 Cybersecurity Law, the 2024 Law on Data, and related regulations have established important elements of the legal framework governing data in the digital environment. Nevertheless, the existing framework does not yet provide a comprehensive mechanism for accessing cross-border data controlled by foreign cloud service providers. This gap creates significant practical difficulties for criminal investigations as data becomes increasingly central to proving criminal offences.

Against this background, this article examines the collection of data from cross-border cloud service providers through the broader concept of cross-border access to data, rather than solely through the traditional framework of electronic evidence collection. It analyses the relationship between criminal jurisdiction, data sovereignty, and the disclosure obligations of digital service providers, evaluates the current Vietnamese legal framework in light of international developments, and proposes legal reforms aimed at establishing effective and lawful mechanisms for accessing cross-border data while maintaining an appropriate balance between criminal law enforcement, privacy protection, and national data sovereignty.

II. CROSS-BORDER DATA COLLECTION AND CHALLENGES TO CRIMINAL JURISDICTION IN THE DIGITAL ENVIRONMENT

Traditional criminal jurisdiction is primarily grounded in the principle of territoriality, under which a state has the authority to investigate, prosecute, and adjudicate criminal conduct occurring within its territory or producing effects within its territory.¹ This model developed in a context where sources of evidence, objects of investigation, and criminal conduct generally existed in tangible forms and were connected to a specific physical location. Accordingly, jurisdiction over criminal conduct and control over sources of evidence typically coincided within the same geographical space.

However, the rapid development of digital technologies, particularly cloud computing, has significantly weakened the traditional connection between data and national territory. In the digital environment, a criminal act may be committed in one country, while electronic data of evidentiary value may be stored on servers located in another country or controlled by a service provider headquartered in a third country. As a result, the authorities with jurisdiction to

¹ RESTATEMENT (FOURTH) OF THE FOREIGN RELATIONS LAW OF THE UNITED STATES § 402 (Am. L. Inst. 2018).

investigate a criminal offence do not always have the legal ability to access the data necessary to collect evidence and establish the commission of the offence.²

This reality reflects an increasingly pronounced separation between the traditional space of jurisdiction and the space in which digital data exists. For cross-border platforms such as Google, Meta, Microsoft, and Amazon Web Services, user data is often distributed or simultaneously backed up across multiple countries in order to optimise operational efficiency and ensure system security. Against this background, determining which state has the authority to require the disclosure of data and which state has the authority to control its use has become a complex legal issue in modern criminal investigations.³

This shift calls for a reconsideration of several foundational concepts in criminal justice and digital governance.

First, data sovereignty refers to the authority of a state to control, govern, and regulate activities relating to data falling within the scope of national interests in accordance with domestic law. In recent years, the concept has increasingly been associated with the broader notion of “digital sovereignty,” reflecting states’ efforts to retain control over data flows and strategically significant digital infrastructure. From this perspective, the issue concerns not only the physical location of data but also a state’s capacity to establish legal conditions governing the collection, processing, transfer, and use of data.⁴

Second, jurisdiction over data refers to a state’s ability to apply and enforce its laws in relation to data or the entities controlling such data. Unlike traditional territorial jurisdiction, which is primarily based on geographical considerations, jurisdiction over data may be established on a number of different grounds, including the location where the data is stored, the place where the service provider is headquartered, the nationality or residence of the user, or the place where consequences arise or economic benefits are derived from the use of the data. Consequently, the same dataset may simultaneously fall within the regulatory scope of multiple legal systems, increasing the potential for jurisdictional conflicts between states.⁵

Third, cross-border access to data refers to measures undertaken by the competent authorities of one state to obtain electronic data stored outside that state’s territory or controlled and

² Orin S. Kerr & Peter Swire, *Law Enforcement Access to Overseas Data Under the CLOUD Act*, CONG. RSCH. SERV. Legal Sidebar LSB10125, at 1–3 (2018).

³ COUNCIL OF EUROPE, EXPLANATORY REPORT TO THE CONVENTION ON CYBERCRIME 24–35 (2001); Jennifer Daskal, *Borders and Bits*, 71 VAND. L. REV. 179, 184–92 (2018).

⁴ Christopher Kuner, *Data Sovereignty and the Future of Data Governance*, in TRANSBORDER DATA FLOWS AND DATA PRIVACY LAW 15, 18–24 (Oxford Univ. Press 2013).

⁵ Jennifer Daskal, *Borders and Bits*, 71 VAND. L. REV. 179, 193–204 (2018).

managed by foreign entities. Such access may be achieved through traditional mutual legal assistance mechanisms in criminal matters, direct cooperation with service providers, or specialised international cooperation mechanisms concerning electronic evidence that have emerged in recent years.⁶

From a theoretical perspective, the current legal debate does not primarily concern which state “owns” the data, but rather which state has the lawful authority to access the data for law enforcement purposes. In other words, the core challenge facing criminal investigations in the era of cloud computing does not arise from technological limitations, but from the absence of a uniform international legal framework governing cross-border access to data. This issue lies at the intersection of three important sets of interests: safeguarding national sovereignty, protecting privacy and fundamental individual rights, and maintaining stability in the operations of transnational digital service providers. Balancing these interests has become one of the central challenges facing criminal procedural law and cybersecurity law at the global level.

III. THE CURRENT VIETNAMESE LEGAL FRAMEWORK FOR CROSS-BORDER ACCESS TO DATA FROM CLOUD SERVICE PROVIDERS

A. The Current Legal Framework for Access to Data for Criminal Investigation Purposes

i. The 2015 Criminal Procedure Code: Recognising Electronic Data as a Source of Evidence but Failing to Establish a Cross-Border Data Access Mechanism

The 2015 Criminal Procedure Code (CPC) marked an important step in the modernisation of Vietnamese criminal procedural law by formally recognising electronic data as an independent source of evidence for the first time. Under Article 87(1) of the 2015 CPC, evidence may be obtained from various sources, including electronic data. Article 99 further defines electronic data as symbols, writings, numbers, images, sounds, or similar forms of information created, stored, transmitted, or received by electronic means.⁷ This recognition reflects a shift in legislative thinking in response to the need to adapt criminal procedure to developments in information technology and the digital environment.

However, the scope of these provisions focuses primarily on establishing the legal status and evidentiary value of electronic data, rather than creating a legal mechanism for accessing and obtaining data in a cross-border context. In other words, the 2015 CPC addresses the question of “whether electronic data constitutes evidence,” but does not adequately address the question

⁶ U.S. DEP’T OF JUST., PROMOTING PUBLIC SAFETY, PRIVACY, AND THE RULE OF LAW AROUND THE WORLD: THE PURPOSE AND IMPACT OF THE CLOUD ACT 2–5 (2019); COUNCIL OF EUROPE, THE BUDAPEST CONVENTION AND CROSS-BORDER ACCESS TO ELECTRONIC EVIDENCE 5–8 (2024).

⁷ Criminal Procedure Code, No. 101/2015/QH13, arts. 87, 99 (Viet.).

of “how procedural authorities may lawfully access data when it is located outside the national territory.” This constitutes a particularly significant legal gap given that a substantial proportion of electronic data is now stored on cloud computing systems distributed across jurisdictions worldwide.⁸

In practice, traditional investigative measures provided for under the CPC, such as searches, temporary seizure, seizure of physical evidence, and the collection of documents, are premised on the assumption that information-bearing objects exist in tangible form and fall within the actual control of procedural authorities. This approach is relatively well suited to paper documents or physical storage devices such as computers, mobile phones, and hard drives. In a cloud computing environment, however, control over an end-user device does not necessarily confer access to data stored remotely. Investigative authorities may seize a user’s telephone or computer but do not thereby acquire automatic access to data stored on Google Drive, Microsoft OneDrive, Apple iCloud, or similar platforms without cooperation from the service provider or the competent authorities of a foreign state.⁹

This limitation reflects the widening gap between territorially based criminal jurisdiction and the realities of data governance in the digital economy. In many cases, data relevant to a criminal investigation concerning conduct occurring in Vietnam may be stored on servers located in multiple countries or controlled by an enterprise headquartered abroad. In such circumstances, obtaining the data is no longer merely an evidentiary activity; it also raises issues of competing jurisdictions, national sovereignty, and the legal obligations of cross-border digital service providers.¹⁰

Notably, the 2015 CPC does not establish several specialised procedural tools that have become widely recognised in international frameworks governing electronic evidence. For example, Vietnamese procedural law does not currently provide for a data preservation order requiring a service provider to temporarily preserve data that may otherwise be deleted; a data production order compelling an entity in possession or control of data to disclose it to a competent authority; or a mechanism for directly requiring digital service providers to produce electronic data. By contrast, these tools constitute fundamental measures under the Budapest Convention on Cybercrime and in a number of modern legal systems, where they are designed to ensure the timely and effective acquisition of electronic evidence.¹¹

⁸ Jennifer Daskal, *Borders and Bits*, 71 VAND. L. REV. 179, 184–92 (2018).

⁹ Orin S. Kerr & Peter Swire, *Law Enforcement Access to Overseas Data Under the CLOUD Act*, CONG. RSCH. SERV. Legal Sidebar LSB10125, at 1–3 (2018).

¹⁰ Jennifer Daskal, *The Un-Territoriality of Data*, 125 YALE L.J. 326, 329–40 (2015).

ii. The 2018 Cybersecurity Law: Strengthening Data Sovereignty and Corporate Cooperation Obligations

The 2018 Cybersecurity Law approaches the issue of electronic data primarily from the perspective of state governance of cyberspace and the protection of national security.

One of the most notable provisions of the 2018 Cybersecurity Law is Article 26, under which certain enterprises providing services in cyberspace and operating in Vietnam are required to store data in accordance with Vietnamese law and to cooperate with competent authorities in preventing, detecting, and handling violations of law.¹²

The requirements of Article 26 are further elaborated in Decree No. 53/2022/ND-CP. Under this framework, enterprises falling within its scope may be subject to several important obligations, including: (i) storing certain categories of data in Vietnam; (ii) establishing a branch or representative office in Vietnam in cases prescribed by law; and (iii) cooperating in providing information at the request of competent authorities for purposes of protecting national security and maintaining social order and safety.¹³

From the perspective of criminal investigations, data localisation requirements may help mitigate difficulties arising when procedural authorities need to access electronic evidence stored abroad. In theory, locating data within the national territory may reduce reliance on mutual legal assistance mechanisms in criminal matters, which are often time-consuming and procedurally complex. At the same time, requiring service providers to establish a commercial presence in Vietnam may facilitate the implementation of cooperation requests made by state authorities.

However, the 2018 Cybersecurity Law is not legislation directly governing the collection of evidence in criminal proceedings. The cooperation obligations imposed on enterprises are primarily formulated at a framework level and do not establish a comprehensive procedural mechanism through which procedural authorities may access electronic data for the investigation and adjudication of criminal cases. Several important issues therefore remain insufficiently addressed, including which authorities are competent to issue data disclosure requests, the procedures and requirements governing such requests, the scope of data that may be accessed, safeguards for users' privacy rights, and mechanisms for dealing with situations in which foreign service providers refuse to cooperate.

¹¹ Convention on Cybercrime arts. 16–18, Nov. 23, 2001, E.T.S. No. 185; COUNCIL OF EUROPE, EXPLANATORY REPORT TO THE CONVENTION ON CYBERCRIME 139–73 (2001).

¹² Cybersecurity Law, No. 24/2018/QH14, art. 26 (Viet.).

¹³ Decree No. 53/2022/ND-CP Detailing Certain Provisions of the Cybersecurity Law, arts. 26–27 (Viet.).

iii. The 2024 Law on Data and the Emergence of a National Data Governance Framework

The 2024 Law on Data establishes principles for data governance at the national level, including the development of databases, the development of data infrastructure, the promotion of data sharing among state agencies, and the enhancement of the capacity to exploit data for public administration purposes.¹⁴ Through these provisions, Vietnamese law is gradually moving from a fragmented model of data management towards a more systematic and interconnected data governance framework. This development constitutes an important foundation for building a data-driven economy and enhancing the effectiveness of public governance in the digital environment.

From a theoretical perspective, the 2024 Law on Data also reflects a shift towards an approach grounded in national data sovereignty. This approach is based on the view that data constitutes a strategic resource that should be governed and protected in a manner comparable to other critical national resources. From the perspective of criminal procedure, however, the 2024 Law on Data is not legislation that directly regulates the collection of evidence or the investigation of criminal offences. Although the Law establishes an important legal foundation for the governance, sharing, and use of data, its provisions are primarily directed towards administrative governance and the development of national data infrastructure, rather than establishing specialised procedural mechanisms for accessing data for criminal investigations. In other words, the Law addresses the question of “data governance” but does not yet fully address the question of “obtaining data as evidence” in criminal proceedings.

In particular, the Law does not establish specialised legal mechanisms for accessing electronic data controlled by foreign enterprises or data stored outside Vietnamese territory. Core issues arising in criminal investigations in the digital environment—including the authority to request cross-border data disclosure, procedures for accessing electronic evidence, mechanisms for preserving data for investigative purposes, and the enforcement obligations of transnational service providers—remain either fragmented across different areas of the existing legal framework or insufficiently regulated.

iv. International Mutual Legal Assistance Mechanisms for Cross-Border Collection of Electronic Data

For electronic data stored abroad, the most important legal mechanism currently available remains international mutual legal assistance in criminal matters (MLA). Under the 2007 Law on Mutual Legal Assistance, bilateral mutual legal assistance treaties, and the principle of

¹⁴ Law on Data, No. 60/2024/QH15 (Viet.), arts. 1, 4, 10, 20.

reciprocity in international relations, competent Vietnamese authorities may request assistance from foreign states in obtaining electronic data or other sources of evidence for the purposes of investigating, prosecuting, and adjudicating criminal cases.¹⁵

However, traditional mutual legal assistance mechanisms were designed around inter-State cooperation in a context where evidence primarily existed in physical form. In the digital environment, much of the evidentiary data is instead held by transnational technology companies such as Google, Meta, Microsoft, and Apple. Consequently, procedural authorities generally cannot access such data directly and must instead act through the competent authorities of the state in which the service provider is headquartered or the data is stored.¹⁶

In practice, mutual legal assistance procedures are often time-consuming, whereas electronic data is inherently volatile and may be altered, deleted, or lose its evidentiary value over time. The mismatch between the speed of traditional mutual legal assistance procedures and the instantaneous nature of digital data has significantly reduced the effectiveness of cross-border electronic evidence collection.¹⁷ Accordingly, although traditional mutual legal assistance remains the principal mechanism for international cooperation, it increasingly requires supplementation by faster and more effective mechanisms for accessing data in the digital age.

B. The Practical Experience of Accessing Data from Cross-Border Cloud Service Providers

In recent years, alongside the growing prevalence of high-tech crime and criminal activities committed in cyberspace, the need to access data controlled by cross-border service providers such as Google, Meta (Facebook), Microsoft, Apple, Telegram, and TikTok has become increasingly common in criminal investigations in Vietnam. The types of data typically requested by procedural authorities include account registration information, IP addresses, access logs, location data, email content, electronic communications, and data stored on cloud computing platforms. These sources of evidence play an important role in identifying offenders, tracing criminal conduct, and establishing relevant facts of a case.¹⁸

However, access to these sources of data remains relatively limited in practice due to the development of cross-border data storage models. Although the 2015 Criminal Procedure Code formally recognises electronic data as a source of evidence, the existing criminal procedural framework still lacks specialised mechanisms for obtaining, preserving, and using electronic

¹⁵ Law on Mutual Legal Assistance, No. 08/2007/QH12 (Viet.).

¹⁶ Jennifer Daskal, *Borders and Bits*, 71 VAND. L. REV. 179, 206–15 (2018).

¹⁷ Council of Eur., Convention on Cybercrime, arts. 25–35, Nov. 23, 2001, E.T.S. No. 185.

¹⁸ Criminal Procedure Code, No. 101/2015/QH13, arts. 87, 99 (Viet.).

data stored in networked environments, particularly data controlled by foreign service providers.¹⁹ The growing reliance on transnational digital platforms has created a significant gap between the investigative powers of procedural authorities and their practical ability to access electronic evidence relevant to criminal cases.²⁰

In particular, Vietnam currently lacks a legal mechanism enabling competent authorities to directly require cross-border service providers to disclose data for criminal investigation purposes. In most cases, access to such data must still be pursued through mutual legal assistance in criminal matters or other forms of international cooperation. These procedures are often time-consuming and involve multiple procedural stages, making them difficult to reconcile with the time-sensitive nature of electronic evidence collection.²¹ The appraisal report on the draft Law on Data issued by the National Assembly's Committee on National Defence and Security also recognised that data relating to Vietnamese users is currently stored across multiple countries, creating difficulties in accessing and using such data for crime prevention and control.²²

The development of cloud computing also poses challenges to traditional criteria for determining territory and jurisdiction. Data in a digital environment may be simultaneously backed up, processed, and transferred among multiple data centres located in different countries, making the legal location of data considerably more difficult to determine than in the case of traditional forms of evidence.²³ This not only affects the determination of which state has the authority to request disclosure of the data but also increases the potential for jurisdictional conflicts among different legal systems.

Another obstacle arises from the complex organisational structures of global technology companies. The same digital platform may be operated by different legal entities depending on the relevant geographical region, while the rights to manage and control the data may be vested in another legal entity located in a different country. In practice, this makes it difficult to determine which entity is legally obliged to receive and comply with a data disclosure request from Vietnamese competent authorities.²⁴

¹⁹ Nguyễn Hữu Cầu, *Collection and Use of Electronic Evidence in the Investigation of High-Tech Crimes*, 12 KIEM SAT JOURNAL 15, 18–21 (2023).

²⁰ Nguyễn Ngọc Anh, *Electronic Evidence in Vietnamese Criminal Procedure and Issues Arising Therefrom*, 6 STATE AND LAW REVIEW 34, 39–42 (2022).

²¹ Nguyễn Thái Phúc, *International Cooperation in the Collection of Electronic Evidence for the Investigation of Transnational Crimes*, 18 LEGISLATIVE STUDIES JOURNAL 23, 27–30 (2023).

²² APPRAISAL REPORT NO. 2905/BC-UBQPAN15 OF THE NATIONAL ASSEMBLY'S COMMITTEE ON NATIONAL DEFENCE AND SECURITY ON THE DRAFT LAW ON DATA (2024).

²³ Nguyễn Thị Quế Anh, *Data Sovereignty and National Jurisdiction in Cyberspace*, 4 STATE AND LAW REVIEW 12, 16–19 (2024).

²⁴ Jennifer Daskal, *Borders and Bits*, 71 VAND. L. REV. 179, 193–204 (2018).

In addition, electronic data is highly volatile and is often retained only for a limited period in accordance with a service provider's data retention policies. Numerous studies have indicated that delays in requesting and obtaining data may result in its deletion, alteration, or loss of evidentiary value, thereby significantly undermining the effectiveness of criminal investigations and prosecutions. This demonstrates that a substantial gap remains between the practical requirements of criminal investigations and the existing legal framework governing cross-border access to data, underscoring the need for legal reform and enhanced international cooperation in this area.

IV. INTERNATIONAL EXPERIENCE IN CROSS-BORDER DATA ACCESS IN CRIMINAL INVESTIGATIONS AND ITS RELEVANCE TO VIETNAM

The development of cloud computing and cross-border digital platforms has diminished the significance of territoriality as a criterion for determining authority to access electronic evidence. Data may be generated, processed, and stored across multiple jurisdictions, making it increasingly difficult to determine jurisdiction solely on the basis of the location of a server. In response to this reality, many states have shifted from an approach based on physical control over storage devices towards one based on lawful access to data. This trend has provided a foundation for mechanisms that enable law enforcement authorities to directly access data held by technology companies, rather than relying exclusively on traditional mutual legal assistance mechanisms.²⁵

The CLOUD Act of 2018 marked a significant development in U.S. law by requiring companies subject to U.S. jurisdiction to disclose data within their possession, custody, or control, regardless of where the data is stored.²⁶ This approach shifts the focus from the physical location of data to the entity exercising control over it, thereby enhancing investigative effectiveness in circumstances where a substantial proportion of global data is held by transnational technology companies. However, this model also creates potential conflicts of jurisdiction and raises concerns regarding data sovereignty. Accordingly, the United States has simultaneously promoted bilateral cooperation agreements designed to mitigate the legal conflicts that may arise.²⁷

Unlike the United States, the European Union (EU) has developed a cross-border data access framework based on balancing investigative effectiveness with the protection of human rights.

²⁵ Jennifer Daskal, *Borders and Bits*, 71 VAND. L. REV. 179, 184–204 (2018).

²⁶ Clarifying Lawful Overseas Use of Data Act (CLOUD Act), Pub. L. No. 115-141, div. V, 132 Stat. 348 (2018).

²⁷ Orin S. Kerr & Peter Swire, *Law Enforcement Access to Overseas Data Under the CLOUD Act*, CONG. RSCH. SERV. Legal Sidebar LSB10125 (2018).

Regulation (EU) 2023/1543 enables judicial authorities of Member States to directly request service providers to preserve or produce electronic data for the purposes of criminal investigations.²⁸ Such access, however, must comply with the principles of necessity and proportionality and remain subject to judicial oversight. This model demonstrates that expanding access to data must be accompanied by safeguards for privacy and the protection of personal data.²⁹

The 2001 Budapest Convention on Cybercrime is widely regarded as one of the most important international frameworks concerning electronic evidence. The Convention establishes mechanisms for the expedited preservation of electronic data and strengthens international cooperation in obtaining digital evidence.³⁰ In particular, the Second Additional Protocol of 2022 expands possibilities for cross-border access to data by permitting direct requests for certain categories of data from service providers and strengthening mechanisms for urgent cooperation.³¹ Unlike the U.S. model, which is primarily grounded in national jurisdiction, or the EU model, which operates within a regional legal framework, the Budapest Convention seeks to establish common standards capable of being broadly accepted by states with different legal systems.

International experience indicates a general trend towards reducing reliance on traditional mutual legal assistance mechanisms and strengthening mechanisms for direct access to data controlled by service providers. For Vietnam, this development suggests three important directions. First, the Criminal Procedure Code should be supplemented with specialised procedural tools, including data preservation orders, data production orders, and mechanisms for handling urgent requests. Second, a clear legal basis should be established for cooperation with cross-border digital service providers in order to enhance access to electronic evidence. Third, all mechanisms for accessing data should operate under the control of law and judicial authorities to ensure an appropriate balance between the requirements of crime prevention and control and the protection of individual privacy. At the same time, studying and gradually aligning Vietnamese law with the standards of the Budapest Convention represents an important

²⁸ Regulation (EU) 2023/1543 of the European Parliament and of the Council of 12 July 2023, 2023 O.J. (L 191) 118.

²⁹ EUROPEAN UNION AGENCY FOR FUNDAMENTAL RIGHTS, HANDBOOK ON EUROPEAN DATA PROTECTION LAW (2024).

³⁰ Council of Eur., Convention on Cybercrime, Nov. 23, 2001, E.T.S. No. 185.

³¹ Second Additional Protocol to the Convention on Cybercrime on Enhanced Co-operation and Disclosure of Electronic Evidence, May 12, 2022, C.E.T.S. No. 224.

avenue for the development of Vietnam's legal framework governing cross-border data collection.³²

V. RECOMMENDATIONS FOR REFORMING VIETNAMESE LAW ON ACCESS TO DATA FROM CROSS-BORDER CLOUD SERVICE PROVIDERS

The foregoing analysis demonstrates that the principal limitation of Vietnamese law at present lies not in its failure to recognise electronic data as a source of evidence, but in the absence of a comprehensive legal mechanism for accessing data stored outside the national territory. In an environment where data is distributed across cloud computing systems and controlled by transnational technology companies, an approach relying primarily on traditional mutual legal assistance in criminal matters is increasingly inadequate to meet the needs of criminal investigations in the digital environment. Accordingly, the reform of Vietnamese law should aim to establish a specialised legal framework governing cross-border access to data in criminal proceedings.

First, the Criminal Procedure Code should be amended to introduce specialised procedural measures concerning electronic data. At present, the 2015 Criminal Procedure Code focuses primarily on establishing the evidentiary value of electronic data but does not provide adequate legal tools for accessing and preserving data prior to its collection. This represents a significant gap when compared with the international standards reflected in the Budapest Convention. Accordingly, the law should introduce a mechanism for requesting the preservation of electronic data, enabling competent authorities to require organisations and enterprises to preserve relevant data in its original state for a specified period in order to prevent its deletion or alteration. In addition, a mechanism for requesting the production of electronic data should be established to provide a legal basis for requiring entities controlling or possessing data to disclose information for investigative purposes. The law should also clearly specify the authorities competent to issue such requests, the conditions for their issuance, the applicable time limits, and the legal consequences of non-compliance with lawful requests made by procedural authorities.³³

More importantly, amendments to the Criminal Procedure Code should not be limited to expanding investigative powers to obtain data, but should also establish procedural principles specifically applicable to electronic evidence. In the digital environment, the evidentiary value of data depends heavily on the ability to establish its authenticity and integrity. Accordingly, the

³² Nguyễn Thị Quế Anh, *Data Sovereignty and National Jurisdiction in Cyberspace*, 4 STATE AND LAW REVIEW 12, 18–20 (2024).

³³ Council of Eur., Convention on Cybercrime arts. 16–18, Nov. 23, 2001, E.T.S. No. 185.

law should recognise principles governing the preservation and authentication of electronic evidence and the maintenance of a digital chain of custody throughout the processes of collecting, copying, storing, and using data. These safeguards are essential to ensuring that electronic data can constitute reliable evidence before procedural authorities and the courts.

Second, Vietnam should gradually establish a mechanism for direct access to data from cross-border cloud service providers. One of the defining characteristics of the digital economy is that much of the evidentiary data required for criminal investigations is no longer under the direct control of users but is instead held by global technology companies such as Google, Microsoft, Apple, and Meta. Under these circumstances, complete reliance on mutual legal assistance in criminal matters may result in data collection procedures taking considerably longer than the lifespan of the electronic evidence itself. The experience of the United States, the European Union, and the Second Additional Protocol to the Budapest Convention demonstrates a broader international trend towards enabling competent authorities to establish direct legal relationships with service providers in circumstances prescribed by law.³⁴

For Vietnam, an initial step should be to establish a designated national authority responsible for cross-border access to electronic data, with functions including receiving, processing, and coordinating requests relating to electronic data. In the longer term, Vietnam should consider establishing a legal mechanism allowing requests for the preservation or production of certain categories of data to be submitted directly to cross-border service providers operating in Vietnam. At the same time, negotiating bilateral or multilateral agreements on the sharing of electronic data for criminal investigation purposes should be regarded as a strategic direction for enhancing law enforcement effectiveness in the digital environment.

Third, expanding access to data must be balanced against the protection of human rights and national data sovereignty. The experience of the European Union demonstrates that the sustainable effectiveness of criminal investigations depends on subjecting access to data to the principles of necessity, proportionality, and purpose limitation. Accordingly, Vietnamese law should distinguish among different categories of data, such as subscriber information, access data, traffic data, and content data, and establish corresponding conditions for access. For categories of data capable of significantly affecting privacy, particularly content data, collection should be subject to prior authorisation or judicial oversight by a competent judicial authority. At the same time, mechanisms protecting the rights of data subjects should be strengthened,

³⁴ Clarifying Lawful Overseas Use of Data Act, Pub. L. No. 115-141, div. V, 132 Stat. 348 (2018); Second Additional Protocol to the Convention on Cybercrime on Enhanced Co-operation and Disclosure of Electronic Evidence, May 12, 2022, C.E.T.S. No. 224.

including the right to notification in appropriate circumstances, the right to lodge complaints, and the right to seek compensation where data has been unlawfully collected or used.³⁵

VI. CONCLUSION

The rapid development of cloud computing and cross-border digital services has fundamentally challenged the territorial foundations of traditional criminal jurisdiction. As electronic data is increasingly generated, processed, stored, and controlled across multiple jurisdictions, the location of data can no longer serve as the sole or decisive basis for determining a state's lawful authority to access electronic evidence. The central challenge for contemporary criminal investigations therefore lies not merely in the technical capacity to collect electronic data, but in establishing a clear, legitimate, and effective legal basis for accessing data held by foreign or transnational service providers.

The analysis in this article demonstrates that Vietnamese law has made important progress in recognising and regulating electronic data. The 2015 Criminal Procedure Code formally recognises electronic data as a source of evidence, while the 2018 Cybersecurity Law and the 2024 Data Law have established important foundations for data governance, cybersecurity, and national data management. Nevertheless, these instruments have not yet established a comprehensive procedural framework specifically governing access to electronic data stored outside Vietnam or controlled by cross-border cloud service providers. In particular, the existing legal framework does not adequately address data preservation, production orders, direct requests to service providers, urgent access mechanisms, judicial oversight, or the allocation of responsibilities among relevant authorities and service providers.

The continued reliance on traditional mutual legal assistance mechanisms also presents significant practical limitations. Although mutual legal assistance remains an essential instrument of international cooperation, its procedures may be too slow and procedurally complex to respond effectively to the volatile nature of electronic evidence. The increasing role of global technology companies as custodians of evidentiary data further demonstrates that criminal justice systems can no longer rely exclusively on state-to-state cooperation. Effective cross-border investigations require appropriate legal mechanisms through which competent authorities can, under clearly defined conditions, obtain data directly from entities that possess or control it.

³⁵ Regulation (EU) 2023/1543 of the European Parliament and of the Council of 12 July 2023 on European Production Orders and European Preservation Orders for Electronic Evidence in Criminal Proceedings, 2023 O.J. (L 191) 118; Jennifer Daskal, *Borders and Bits*, 71 VAND. L. REV. 179, 223–31 (2018).

Comparative experience from the United States, the European Union, and the Budapest Convention demonstrates a broader international movement towards more flexible and direct mechanisms for accessing electronic evidence, while simultaneously strengthening safeguards for privacy, data protection, proportionality, and judicial oversight. These developments suggest that the future of cross-border electronic evidence should not be understood as a choice between territorial sovereignty and unrestricted access to data. Rather, the central legal task is to construct a framework capable of reconciling effective criminal jurisdiction, data sovereignty, international cooperation, and fundamental rights.

For Vietnam, the reform of the legal framework should therefore proceed in several interconnected directions. First, the Criminal Procedure Code should be supplemented with specialised procedural mechanisms for the preservation and production of electronic data, together with clear rules on authentication, integrity, and the digital chain of custody. Second, Vietnam should develop an institutional mechanism for coordinating cross-border requests for electronic evidence and gradually establish a legal basis for direct cooperation with cloud service providers operating across borders. Third, access to data should be differentiated according to the sensitivity of the information concerned, with stronger procedural safeguards for traffic and content data that may significantly interfere with privacy and other fundamental rights. Fourth, Vietnam should strengthen bilateral and multilateral cooperation and progressively align its legal framework with emerging international standards on cross-border electronic evidence, including those reflected in the Budapest Convention and its Second Additional Protocol.

Ultimately, the challenge of cross-border cloud data is not simply a question of where data is physically located. It is a question of who may lawfully access data, on what legal basis, through which procedure, and subject to what safeguards. The transformation of data from a territorially bounded resource into a globally distributed and privately controlled resource requires a corresponding transformation in the legal framework governing criminal investigations. For Vietnam, establishing such a framework is essential not only to enhance the effectiveness of criminal investigations and prosecution, but also to ensure that the exercise of criminal jurisdiction remains consistent with the rule of law, individual rights, and the principles of national sovereignty in the digital age.

VII. BIBLIOGRAPHY

Legislation

1. Clarifying Lawful Overseas Use of Data Act (CLOUD Act), Pub. L. No. 115-141, div. V, 132 Stat. 348 (2018).
2. Criminal Procedure Code, No. 101/2015/QH13 (Viet.).
3. Cybersecurity Law, No. 24/2018/QH14 (Viet.).
4. Decree No. 53/2022/ND-CP Detailing Certain Provisions of the Cybersecurity Law (Viet.).
5. Law on Data, No. 60/2024/QH15 (Viet.).
6. Law on Mutual Legal Assistance, No. 08/2007/QH12 (Viet.).
7. Regulation (EU) 2023/1543 of the European Parliament and of the Council of 12 July 2023 on European Production Orders and European Preservation Orders for Electronic Evidence in Criminal Proceedings, 2023 O.J. (L 191)

Journal Articles

8. Jennifer Daskal, *Borders and Bits*, 71 VAND. L. REV. 179 (2018).
9. Jennifer Daskal, *The Un-Territoriality of Data*, 125 YALE L.J. 326 (2015).
10. Nguyễn Hữu Cầu, *Collection and Use of Electronic Evidence in the Investigation of High-Tech Crimes*, 12 KIEM SAT JOURNAL 15, 18–21 (2023).
11. Nguyễn Ngọc Anh, *Electronic Evidence in Vietnamese Criminal Procedure and Issues Arising Therefrom*, 6 STATE AND LAW REVIEW 34, 39–42 (2022).
12. Nguyễn Thái Phúc, *International Cooperation in the Collection of Electronic Evidence for the Investigation of Transnational Crimes*, 18 LEGISLATIVE STUDIES JOURNAL 23, 27–30 (2023).
13. Nguyễn Thị Quế Anh, *Data Sovereignty and National Jurisdiction in Cyberspace*, 4 STATE AND LAW REVIEW 12, 16–19 (2024).

Books and Book Chapters

14. Christopher Kuner, *Data Sovereignty and the Future of Data Governance*, in TRANSBORDER DATA FLOWS AND DATA PRIVACY LAW (Oxford Univ. Press 2013).
15. RESTATEMENT (FOURTH) OF THE FOREIGN RELATIONS LAW OF THE UNITED STATES § 402 (Am. L. Inst. 2018).

Reports and Institutional Publications

16. APPRAISAL REPORT NO. 2905/BC-UBQPAN15 OF THE NATIONAL ASSEMBLY COMMITTEE ON NATIONAL DEFENCE AND SECURITY ON THE DRAFT LAW ON DATA (2024).
17. COUNCIL OF EUROPE, EXPLANATORY REPORT TO THE CONVENTION ON CYBERCRIME (2001).
18. COUNCIL OF EUROPE, THE BUDAPEST CONVENTION AND CROSS-BORDER ACCESS TO ELECTRONIC EVIDENCE (2024).
19. EUROPEAN UNION AGENCY FOR FUNDAMENTAL RIGHTS, HANDBOOK ON EUROPEAN DATA PROTECTION LAW (2024).
20. NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY, THE NIST DEFINITION OF CLOUD COMPUTING, SPECIAL PUBLICATION 800-145 (2011).
21. Orin S. Kerr & Peter Swire, *Law Enforcement Access to Overseas Data Under the CLOUD Act*, CONG. RSCH. SERV. Legal Sidebar LSB10125 (2018).
22. UNITED NATIONS OFFICE ON DRUGS AND CRIME, PRACTICAL GUIDE FOR REQUESTING ELECTRONIC EVIDENCE ACROSS BORDERS (2019).
23. U.S. DEPARTMENT OF JUSTICE, PROMOTING PUBLIC SAFETY, PRIVACY, AND THE RULE OF LAW AROUND THE WORLD: THE PURPOSE AND IMPACT OF THE CLOUD ACT (2019).

Treaties and International Instruments

24. Convention on Cybercrime, Nov. 23, 2001, E.T.S. No. 185.
25. Second Additional Protocol to the Convention on Cybercrime on Enhanced Co-operation and Disclosure of Electronic Evidence, May 12, 2022, C.E.T.S. No. 224.
