Review Article
DOI: https://doi.org/10.22598/iele.2026.13.1.10

CROSS-BORDER DATA COLLECTION IN TRANSNATIONAL CRIME CONTROL: WHAT ASEAN CAN LEARN FROM THE US-EU EXPERIENCE

Thu Huong Vu [*]
Thi Thu Hien Tran [**]

ABSTRACT

Electronic data has become an essential source of evidence in the investigation and prosecution of transnational crime. Yet access to such data is often complicated by its cross-border nature, as information may be stored, processed, or controlled outside the territory of the investigating state. Traditional mechanisms of international cooperation, particularly mutual legal assistance, were not designed for the scale and speed of electronic evidence and have proven increasingly inadequate. In response, states have adopted different approaches, including unilateral assertions of extraterritorial jurisdiction, regional cooperation frameworks, and data localisation measures. This article analyses how cross-border data collection is regulated in the United States and the European Union and considers the implications of these approaches for ASEAN. It suggests that neither model offers a complete answer and that, in the short term, ASEAN should concentrate on improving existing cooperation mechanisms and strengthening regional coordination in a way that remains consistent with its institutional setting and respect for state sovereignty.

Key words*: cross border data, transnational crime, electronic data, ASEAN, mutual legal assistance, data sovereignty.*

[*] Hanoi Law University, Faculty of Criminal Law, Hanoi, Vietnam, huongvt@hlu.edu.vn

[**] Hanoi Law University, Faculty of Criminal Law, Hanoi, Vietnam, thuhientran.hlu@gmail.com

1. INTRODUCTION

The development of digital technologies has made electronic evidence a central element of criminal investigations. An estimate indicates that digital materials are present in around 90% of cases investigated in the United Kingdom[1], while an impact assessment by the European Commission has found that electronic evidence in some form is relevant in approximately 85% of total criminal investigations[2]. Evidence collection in criminal proceedings refers to the application of measures provided for under criminal procedural law to identify, secure, document, and preserve evidence for the purpose of establishing the facts of a criminal case. In the case of electronic evidence, collection takes place through electronic data as the relevant source of evidence. Measures used to obtain electronic evidence must, as a starting point, comply with the general requirements on legal basis, authority, and procedure governing evidence collection under each state's domestic law.

However, unlike the evidence in traditional crime, electronic evidence in transnational crime is often cross-border in nature, raising challenges relating to geography and territorial sovereignty. When an individual sends a message, an email, or conducts an online transaction, the data may be routed through multiple servers located in different jurisdictions before reaching its final storage location[3]. In many cases, investigating authorities cannot determine with certainty where the data is stored at a given moment. This uncertainty makes it difficult to identify which state has jurisdiction and which foreign authority should receive a request for assistance.

At the same time, service providers such as social media platforms, cloud computing services, and online marketplaces commonly operate on a transnational scale, with headquarters in one state, data centres in another, and users distributed across the globe[4]. Transnational crime often extends across several jurisdictions and is not limited to a single type of crime[5]. A human trafficking operation may be organised from one country, target victims in several oth-

[1] National Police Chiefs Council (NPCC): Digital Forensic Science Strategy, London, 2020.

[2] European Commisssion: *Commission Staff Working Document: Impact Assessment Accompanying the Proposal for a Regulation on European Production and Preservation Orders for Electronic Evidence in Criminal Matters*, SWD/2018, 118 final, 2018.

[3] Millard, C., Millard, C.: *Cloud Computing Law*, Oxford: Oxford University Press, 2021.

[4] Abraha, H. H.: Law enforcement access to electronic evidence across borders: mapping policy approaches and emerging reform initiatives. *International Journal of Law and Information Technology*, 29(2) 2021, pp. 118-153.

[5] Reichel, P. L., Albanese, J. S.: *Handbook of Transnational Crime and Justice*, Thousand Oaks: SAGE Publications, Incorporated, 2013.

ers, and even exploit trafficked persons to participate in so-called "romance baiting" fraud schemes[6]. Digital technologies are commonly used to enable communication among offenders through social media, dating applications, blogs, advertising platforms, and online sales sites[7]. The tools and methods used in such offences are also cross-border in nature, including foreign-based services, overseas servers, virtual private networks, anonymisation software, and cryptocurrencies.

As electronic data moves freely across borders and is subject to the authority of different states, domestic investigative powers, traditionally limited to national territory, are often insufficient. Accessing electronic evidence stored abroad generally requires the consent or cooperation of the state where the data is located. Delays or refusals may occur because of differences in criminalisation, procedural law, data protection rules, or privacy standards. In fast-moving digital environments, such delays may result in data being altered or deleted before it can be preserved. As a result, cross-border access to electronic evidence becomes unavoidable in efforts to prevent and combat transnational crime[8]. A 2018 study by the European Commission found that more than half of criminal investigations in the European Union relating to electronic evidence require cross-border access[9].

In response to these challenges, governments have established a range of formal and informal arrangements to exchange evidence across borders, while maintaining respect for territorial sovereignty[10]. Under international law, electronic evidence located abroad is traditionally obtained through five main methods: (i) international conventions that contain provisions on mutual legal assistance; (ii) bilateral or multilateral mutual legal assistance treaties and agreements; (iii) ad hoc mutual legal assistance based on the principle of reciprocity; (iv) letters rogatory issued by the courts of one state to the courts of another; and (v) bilateral and multilateral cooperation between national police

[6] Cross, C.: Romance baiting, cryptorom and 'pig butchering': an evolutionary step in romance fraud. *Current Issues in Criminal Justice*, 36(3) 2024, pp. 334-346.

[7] Slimi, H., Chichti, J.: The Nexus Between Cybercrime and Irregular Migration in the Age of Cyberspace: Implications for Geographic Flexibility and Mobility Management. *Global Journal of Flexible Systems Management*, 2026, pp. 1-38.

[8] Daskal, J.: Law Enforcement Access to Data Across Borders. *Journal of National Security Law & Policy*, 8(3) 2016, pp. 473-501.

[9] Commission Staff Working Document: Impact Assessment Accompanying the Proposal for a Regulation on European Production and Preservation Orders for Electronic Evidence in Criminal Matters, (SWD/2018/118, 2018).

[10] Abraha, H. H.: Law enforcement access to electronic evidence across borders: mapping policy approaches and emerging reform initiatives. *International Journal of Law and Information Technology*, 29(2) 2021, pp. 118-153.

authorities[11]. Each of these methods is grounded in respect for the sovereignty of the requested state. International conventions and mutual legal assistance agreements require negotiation, signature, and ratification, while individual requests for assistance or cooperation must be channelled through competent authorities or law enforcement agencies. In practice, however, conduct may not be criminalised in all jurisdictions, and the requested state retains discretion to grant or refuse assistance under its domestic law[12].

In addition, the mutual legal assistance framework was developed before the emergence of the Internet and is not well suited to the current digital and global environment[13]. Requests often take a long time to process and the growing volume of applications from multiple jurisdictions places significant pressure on competent authorities, particularly in states that host data centres of multinational corporations. In the United States, the Department of Justice reported in 2017 that "since 2000, the number of foreign requests for assistance to OIA has increased nearly 85% and the number of requests for computer records has increased over 1000%", while noting that staffing and resources at the Department of Justice's Office of International Affairs, which reviews MLAT procedures, "had not kept pace with the growth in its work"[14]. As a result, traditional mutual legal assistance procedures are commonly criticised as slow, cumbersome, and inefficient, with bilateral requests often taking between ten months and two years to complete[15]. Moreover, electronic evidence is primarily controlled by private service providers. In some situations, these providers are unable or unwilling to respond to data requests from foreign law enforcement authorities[16].

---

[11] Funk, T. M.: *Mutual Legal Assistance Treaties and Letters Rogatory: A Guide for Judges*, Washington: Federal Judicial Center, 2014; Yanqing, H.: "Game of Laws": Cross-Border Data Access for Law Enforcement Purposes-Models in the United States, Europe, and China. *Global Law Review*, 43(1) 2021, pp. 38-51.

[12] Swire, P., Hemmings, J. D.: Mutual Legal Assistance in an Era of Globalized Communications: The Analogy to the Visa Waiver Program. *NYU Annual Survey of American Law*, 71(4) 2017, pp. 687-800.

[13] Hill, J. F., Noyes, M.: Rethinking Data, Geography, and Jurisdiction, in: Ellis, R., Mohan, V. (eds.): *Rewired: Cybersecurity Governance* (pp. 195-212), Hoboken: John Wiley & Sons, 2019.

[14] United States Department of Justice, Criminal Division: *Performance Budget: FY 2017 President's Budget*, Washington: United States Department of Justice, Criminal Division, 2016.

[15] Swire, P., Hemmings, J. D.: Mutual Legal Assistance in an Era of Globalized Communications: The Analogy to the Visa Waiver Program. *NYU Annual Survey of American Law*, 71(4) 2017, pp. 687-800; Cybercrime Convention Committee: *Assessment report on Mutual Legal Assistance: Follow up given by Parties and Observers*, France: Council of Europe, 2017.

[16] Woods, A. K., 'Mutual Legal Assistance in the Digital Age', in: Gray, D.; Henderson, S. (eds.): *The Cambridge Handbook of Surveillance Law*, Cambridge: Cambridge University Press, 2017.

This situation has led to questions, both legal and practical, about whether mutual legal assistance treaties should continue to serve as the main channel for cross-border access to digital evidence. In response, states have sought other legal grounds and methods to obtain electronic evidence beyond the MLAT system. Some arrangements permit direct requests to service providers for data they hold or control, based on treaties or other cooperative instruments. Other measures operate on a unilateral basis. These measures rely on the exercise of extraterritorial investigative jurisdiction, access to data through network connections (government hacking), or domestic requirements that data, or copies of data, relating to citizens or persons within the state be stored on servers located within national territory (data localisation)[17]. Each offers a partial response but introduces its own conflicts between sovereignty, data protection standards, and investigative necessity.

Against this background, the experiences of the United States and the European Union provide useful points of comparison. The United States has adopted a control-based model that extends jurisdiction over data held by service providers subject to U.S. law, while the European Union has pursued regionally coordinated solutions grounded in judicial cooperation, mutual recognition, and data protection. Although shaped by different legal and institutional arrangements, both systems seek to address the same underlying problem of accessing electronic evidence across borders. ASEAN faces similar challenges, particularly given the prevalence of transnational crime in Southeast Asia and the diversity of legal systems within the region. This article examines how cross-border data collection is addressed in U.S. and EU law and considers what ASEAN can learn from these experiences. Rather than advocating a single model, the article focuses on identifying practical lessons and short-term options that are compatible with ASEAN's institutional framework and respect for state sovereignty.

[17] Shurson, J.: Investigative Jurisdiction: The Evolving Limits of Extraterritoriality in Transnational Digital Investigations. *International & Comparative Law Quarterly*, 74(3) 2025, pp. 675-705; Mayer, J.: Government Hacking, *Yale Law Journal*, 127(3) 2018, pp. 570-662; Svantesson, D.: Data localisation trends and challenges: Considerations for the review of the Privacy Guidelines, *OECD Digital Economy Papers*, Paris: OECD Publishing, 2020; Wang, A.: Cyber Sovereignty at its Boldest: A Chinese Perspective. *The Ohio State Technology Law Journal*, 16(2) 2020, pp. 395-466; Savelyev, A.: Russia's new personal data localization regulations: A step forward or a self-imposed sanction?. *Computer Law & Security Review*, 32(1) 2016, pp. 128-145.

2. METHODOLOGY

This article adopts descriptive and comparative legal methods to examine the legal framework governing cross-border data collection in transnational crime control. The descriptive method is used to analyse existing legal frameworks, international agreements, regional instruments, and institutional mechanisms related to law enforcement access to electronic data in the United States, the European Union, and ASEAN. Primary sources include domestic statutes, in particular the Stored Communications Act and the Clarifying Lawful Overseas Use of Data Act in the United States, Regulation (EU) 2023/1543 and Directive (EU) 2023/1544 in the European Union, and the relevant provisions of the criminal procedure law of ASEAN member states. The analysis also draws on multilateral instruments, including the Budapest Convention on Cybercrime and its Second Additional Protocol, the United Nations Convention against Cybercrime, and the 2004 ASEAN Treaty on Mutual Legal Assistance in Criminal Matters, together with judicial decisions and secondary academic literature.

The comparative method is employed to compare the legal approaches developed by the United States and the European Union in response to the growing problem of cross-border access to electronic data for criminal investigations. The two jurisdictions are selected because they have produced the most detailed legal frameworks on this subject and because they represent two different institutional models: a control-based model in the United States, under which jurisdiction follows the data controller, and a mutual-recognition model in the European Union, based on judicial cooperation among Member States. The comparison addresses three elements: the legal basis for investigative jurisdiction, the procedural conditions for access, and the rules limiting access by foreign authorities to data held within the jurisdiction.

3. RESULTS AND DISCUSSION

3.1. CROSS-BORDER DATA COLLECTION IN THE UNITED STATES AND THE EUROPEAN UNION

States address cross-border data access in two situations: where domestic authorities seek to obtain electronic data stored abroad, and where foreign authorities seek access to electronic data stored within the state.

3.1.1. THE UNITED STATES

The collection of electronic evidence under U.S. federal law is mainly regulated by the Electronic Communications Privacy Act (ECPA), which comprises three statutes: the Stored Communications Act (SCA), the Wiretap Act, and the Pen Register Act. These statutes limit the types of data that U.S.-based service providers may voluntarily disclose to domestic and foreign authorities and set out the substantive and procedural conditions under which U.S. law enforcement agencies may compel disclosure[18]. The Communications Assistance for Law Enforcement Act (CALEA) separately governs the obligation of telecommunications companies to assist in the execution of wiretap orders. Together, these laws apply to both federal and state law enforcement access to data. State law may provide stronger protections, but it cannot diminish the safeguards required under federal law.

a) Access to data stored outside U.S. territory

For many years, the SCA[19] served as the main legal basis for obtaining electronic data relating to individuals and businesses. Its application, however, was largely limited to data stored within the United States and offered little guidance on data held abroad. This limitation came to the fore in the 2016 Microsoft Ireland litigation[20], which asked whether a warrant issued under the SCA could require a U.S.-based company, Microsoft, to disclose the content of emails and related communications stored on servers located outside the United States, in Ireland[21].

The issue was addressed by the Clarifying Lawful Overseas Use of Data Act (CLOUD Act)[22], enacted in 2018. The CLOUD Act requires service providers to preserve and disclose communications, records, and other information within their possession, custody, or control, regardless of where the data is

[18] Corhay, M., Franssen, V.: Digital Evidence Gathering by US Authorities and Cross-Border Cooperation with US-Based Service Providers, in: Tosza, S.; Franssen, V. (eds.): *The Cambridge Handbook of Digital Evidence in Criminal Investigations*, Cambridge: Cambridge University Press, 2025.

[19] The Stored Communications Act, 18 U.S.C. §§ 2701-2713, 1986.

[20] United States v. Microsoft Corp., 2018.

[21] Corhay, M., Franssen, V.: Digital Evidence Gathering by US Authorities and Cross-Border Cooperation with US-Based Service Providers, in: Tosza, S.; Franssen, V. (eds.): *The Cambridge Handbook of Digital Evidence in Criminal Investigations*, Cambridge: Cambridge University Press, 2025.

[22] Clarifying Lawful Overseas Use of Data Act (CLOUD Act), 2018.

stored[23]. It applies to providers of electronic communication services and remote computing services subject to U.S. jurisdiction. This category covers not only companies incorporated or headquartered in the United States, but also foreign companies that provide services in the United States and maintain a substantial connection to the country[24].

To mitigate conflicts of law and respect the data sovereignty of other states, the CLOUD Act allows service providers to seek to quash or modify a disclosure order where the request concerns data relating to a non-U.S. person who does not reside in the United States and where compliance would conflict with the law of a "qualifying foreign government".

b) Foreign access to data stored within U.S. territory

The SCA does not directly regulate the collection of electronic data outside the United States. It does, however, set out detailed rules that limit access by foreign authorities to data stored within U.S. territory. Section 2702 SCA prohibits providers of electronic communication services and remote computing services from knowingly disclosing subscriber records or other customer information[25]. The Act permits U.S. authorities, as defined in Section 2711(4), to compel disclosure of electronic data from data controllers through a search warrant[26]. At the same time, the SCA bars U.S.-based service providers from disclosing electronic data directly to foreign government authorities. Foreign prosecuting authorities must therefore seek access through mutual legal assistance procedures under bilateral agreements.

The CLOUD Act introduced a limited exception to this framework. It allows "qualifying foreign governments" to submit direct requests for electronic data to U.S.-based service providers without using traditional mutual legal assistance channels. This option is available only to governments that meet specific statutory conditions. A qualifying state must conclude an executive agreement under 18 U.S.C. § 2523, be a party to the Budapest Convention on Cybercrime, and ensure that its domestic law complies with the requirements set out in

[23] Clarifying Lawful Overseas Use of Data Act (CLOUD Act), 2018, § 2713.

[24] U United States Department of Justice: *Promoting Public Safety, Privacy, and the Rule of Law Around the World: The Purpose and Impact of the CLOUD Act*, Washington, 2019; Hemmings, J., Srinivasan, S., Swire, P.: Defining the Scope of 'Possession, Custody, or Control' for Privacy Issues and the Cloud Act. *Journal of National Security Law & Policy*, 10 2020, pp. 631-675.

[25] The Stored Communications Act, 18 U.S.C. §§ 2701-2713, 1986, § 2702.

[26] The Stored Communications Act, 18 U.S.C. §§ 2701-2713, 1986, § 2703.

Chapters I and II of the CLOUD Act[27]. Direct requests are further limited to data relating to serious crimes[28] involving non-U.S. persons[29] and must not affect U.S. free speech protections or involve large-scale data collection. In practice, "qualifying foreign governments" are typically close U.S. allies[30]. To date, the United Kingdom and Australia are recognised as qualifying governments[31], while Canada and the European Union remain in negotiations.

Overall, the U.S. approach to data collection follows a control-based model, under which jurisdiction is linked to the location of the data controller. Given the concentration of major service providers in the United States and the scope of the CLOUD Act, U.S. authorities retain broad capacity to obtain electronic evidence across borders. At the same time, U.S. law tightly restricts foreign access to data stored within its territory. Even qualifying foreign governments must comply with U.S. standards on human rights, privacy protection, and reciprocity.

3.1.2. THE EUROPEAN UNION

a) Cross-border data collection within the European Union

For many years, the collection of electronic evidence outside the European Union relied mainly on traditional bilateral mutual legal assistance treaties. Within the EU, cross-border access to electronic evidence has instead been governed by regional instruments, in particular the Budapest Convention on

[27] Clarifying Lawful Overseas Use of Data Act, Pub. L. No. 115-141, Division V, 132 Stat. 1213, 2018, § 2713(h).

[28] Access to the data is also limited to specific individuals, accounts, addresses, or personal devices and is subject to review by a court or other independent authority in accordance with Clarifying Lawful Overseas Use of Data Act, (18 U.S.C., 2018) § 2523(b)(4)(D)(ii)–(v).

[29] In other words, the provision applies only to persons who are neither U.S. citizens nor lawful permanent residents, and who are not located in the United States, as specified in Clarifying Lawful Overseas Use of Data Act, Pub. L. No. 115-141, Division V, 132 Stat. 1213, 2018, § 2523.

[30] Shurson, J.: Investigative Jurisdiction: The Evolving Limits of Extraterritoriality in Transnational Digital Investigations. *International & Comparative Law Quarterly*, 74(3) 2025, pp. 675-705.

[31] Agreement between the Government of the United States of America and the Government of Australia on Access to Electronic Data for the Purpose of Countering Serious Crime, no. 24-130.1, 2021; Agreement between the Government of the United Kingdom of Great Britain and Northern Ireland and the Government of the United States of America on Access to Electronic Data for the Purpose of Countering Serious Crime, TS no 33/2024, 2024.

Cybercrime[32], the EU Convention on Mutual Assistance in Criminal Matters[33], and, since 2017, the European Investigation Order Directive (EIO Directive)[34]. The Budapest Convention on Cybercrime has been ratified by 81 states, including all EU Member States and a number of non-EU countries[35]. Article 18(1)(b) of the Convention authorises law enforcement authorities of a Party to require service providers within its territory to disclose non-content data in their possession or control. Accordingly, cross-border access under the Convention is limited to non-content data, such as subscriber information. In May 2022, the Second Additional Protocol to the Convention was adopted[36]. It introduces provisions on direct cooperation with service providers, but limits such cooperation to the disclosure of domain name registration data and subscriber information[37].

The European Investigation Order Directive is based on mutual recognition of judicial decisions among EU Member States[38]. When the judicial authority of one Member State issues a European Investigation Order (EIO) requesting a specific investigative measure, the authority of the executing Member State must carry out that measure within the prescribed time limits, unless the measure is unavailable under its domestic law or there are lawful grounds for refusal[39]. At the time the Directive was negotiated in the early 2010s, however, cross-border access to electronic evidence had not yet become a central concern. As a result, the Directive does not contain specific provisions on electronic evidence, and its execution deadlines are often incompatible[40] with the

[32] Convention on Cybercrime, ETS No. 185, Council of Europe, Budapest, 23.11.2001.

[33] European Convention on Mutual Assistance in Criminal Matters, ETS no. 030, Strasbourg: Council of Europe, 20.04.1959.

[34] Directive 2014/41/EU of the European Parliament and of the Council of 3 April 2014 regarding the European Investigation Order in criminal matters, *Official Journal of the European Union*, L 130, 1.05.2014, pp. 1-36.

[35] Council of Europe Treaty Office: *Chart of Signatures and Ratifications of Treaty No. 185*, 2026.

[36] Second Additional Protocol to the Convention on Cybercrime on Enhanced Co-operation and Disclosure of Electronic Evidence, CETS no. 224, Council of Europe, 2022.

[37] Second Additional Protocol to the Convention on Cybercrime on Enhanced Co-operation and Disclosure of Electronic Evidence, CETS no. 224, Council of Europe, 2022, art. 6-7.

[38] Mitsilegas, V.: *EU Criminal Law*, Oxford: Hart Publishing, 2020.

[39] Directive 2014/41/EU of the European Parliament and of the Council of 3 April 2014 regarding the European Investigation Order in criminal matters, *Official Journal of the European Union*, L 130, 01.05.2014, Art. 10, 11 & 13.

[40] From 30 to 90 days according to Art. 12 Directive 2014/41/EU of the European Parliament and of the Council of 3 April 2014 regarding the European Investigation Order in criminal matters, *Official Journal of the European Union*, L 130, 01.05.2014,

volatility of digital data and existing data retention rules. The Directive also does not apply in Denmark or Ireland, despite the fact that Ireland hosts the European headquarters of several major global service providers, including Apple, Amazon, Microsoft, and Meta.

After the adoption of the U.S. CLOUD Act in 2018, the United States asserted jurisdiction over data controlled by U.S. companies regardless of where the data is stored. This development raised concerns within the EU about conflicts with data sovereignty[41]. In response, the European Commission proposed an e-evidence package on 17 April 2018, consisting of a Regulation and a Directive, with the aim of enabling judicial authorities to obtain electronic evidence across the EU in a timely and lawful manner for criminal investigations and prosecutions[42]. Following several years of negotiations among the European Parliament, the Council, and fundamental rights organisations, the EU adopted the e-evidence package on 28 July 2023. It consists of Regulation (EU) 2023/1543 on European Production Orders and European Preservation Orders Electronic Evidence in Criminal Proceedings and for the Execution of Custodial Sentences Following Criminal Proceedings[43], together with Directive (EU) 2023/1544 of the European Parliament and of the Council of 12 July 2023 laying down harmonised rules on the designation of designated establishments and the appointment of legal representatives for the purpose of gathering electronic evidence in criminal proceedings[44]. Both instruments will apply from 18 August 2026, once Member States have completed the necessary legal and technical arrangements.

The e-evidence Regulation introduces two cross-border instruments: the European Preservation Order (EPrO) and the European Production Order (EPO). An EPrO requires a service provider[45] to preserve specified categories of data to prevent alteration or deletion. An EPO allows a competent judicial authority

[41] Juszczak, A., Sason, E.: The Use of Electronic Evidence in the European Area of Freedom, Security, and Justice. *eucrim*, (2) 2023, pp. 182-200.

[42] Juszczak, A., Sason, E.: The Use of Electronic Evidence in the European Area of Freedom, Security, and Justice. *eucrim*, (2) 2023, pp. 182-200.

[43] 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 and for the execution of custodial sentences following criminal proceedings, *Official Journal of the European Union*, L 191, 28.07.2023.

[44] Directive (EU) 2023/1544 of the European Parliament and of the Council of 12 July 2023 laying down harmonised rules on the designation of designated establishments and the appointment of legal representatives for the purpose of gathering electronic evidence in criminal proceedings, *Official Journal of the European Union*, L 191, 28.07.2023.

[45] 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

of one Member State to require a service provider established or represented in another Member State to produce electronic data directly.

A judge, investigating judge, court, public prosecutor, or other competent authority[46] may issue an EPrO for any criminal offence[47] and for all categories of data listed in Article 3(9)–(12) of the Regulation. These categories include: (i) subscriber data, such as name, address, and payment information; (ii) data requested for the sole purpose of identifying the user, such as IP addresses and timestamps; (iii) traffic data, including login records, IP addresses, and other metadata; and (iv) content data, such as text, emails, videos, images, and audio files[48].

Similarly, a judge, investigating judge, court, public prosecutor, or other competent authority may issue an EPO to obtain subscriber data and data used solely to identify the user for any criminal offence[49]. By contrast, an EPO for content data or traffic data—other than data used solely for user identification—may be issued only in relation to serious offences punishable by a custodial sentence of a maximum of at least three years, as well as certain offences listed in Article 5(4) of the Regulation, including offences relating to fraud and counterfeiting of non-cash means of payment, targeted cybercrime, child sexual abuse, and terrorism. In these cases, only a judge, an investigating judge, a court and another competent authority designated by the issuing State may issue an EPO; prosecutors do not have authority to request these categories of data[50].

Service providers must preserve data under an EPrO for 60 days, with a possible extension of 30 days where necessary[51]. Data requested under an EPO must be produced within 10 days of receipt. In emergency situations involving an imminent threat to life or physical safety, the time limit is reduced to eight hours[52]. Failure to comply with an EPO or EPrO without valid justification may give rise to penalties or enforcement measures under national law.

criminal proceedings and for the execution of custodial sentences following criminal proceedings, *Official Journal of the European Union*, L 191, 28.07.2023, Art. 3(3).

46 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 and for the execution of custodial sentences following criminal proceedings, *Official Journal of the European Union*, L 191, 28.07.2023, Art. 4(3).

47 Ibid., Art. 6(3).

48 Ibid., Art. 3(9)-(12).

49 Ibid., Art. 4(1).

50 Ibid., Art. 4(2).

51 Ibid., Art. 11(1).

52 Ibid., Art. 10(4).

Directive (EU) 2023/1544 addresses the absence of a legal presence of certain service providers in the EU. It requires service providers offering services in the EU to designate a legal representative in a Member State. The legal representative is responsible for receiving and responding to such orders. This obligation applies only to providers with a substantial connection to the EU, reflected in turnover, user numbers exceeding specified thresholds, or the targeting of services at citizens of one or more Member States[53].

In contrast to the U.S. CLOUD Act, the EU e-evidence Regulation applies only within the Union. Judicial authorities of a Member State may issue orders only to service providers that have an establishment or a designated legal representative in another Member State. Where data is held or controlled by service providers established outside the EU, Member States must continue to rely on traditional mutual legal assistance mechanisms. Whereas the CLOUD Act extends extraterritorial jurisdiction based on data control, the EU e-evidence framework rests on enhanced judicial cooperation within the EU, with an emphasis on respect for state sovereignty and the protection of fundamental rights[54].

b) Access by non-EU states to data stored within the EU

The European Union applies a strict data protection framework under the General Data Protection Regulation (GDPR), in force since 2018. The GDPR governs not only the processing of personal data for commercial purposes, but also access to personal data in the context of cross-border evidence collection. Article 48 GDPR provides that a judgment or decision of a court or administrative authority of a third country requiring the transfer or disclosure of personal data may be recognised or enforced only where it is based on an international agreement between that third country and the EU or a Member State[55]. Consequently, companies established in the EU, or processing the personal data of EU residents, may not disclose such data directly to foreign authorities in the absence of an appropriate legal basis.

---

53 Ibid., Art. 5(6).

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

55 Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), *Official Journal of the European Union*, L 119, 4.05.2016, pp. 1-88.

This provision prevents third countries, including the United States, from obtaining personal data through unilateral requests. In Schrems II (2020)[56], the Court of Justice of the European Union invalidated the EU–U.S. Privacy Shield on the basis that U.S. surveillance law did not ensure a level of data protection equivalent to that required under EU law.

Unlike the U.S. CLOUD Act, which permits direct requests by "qualifying foreign governments" to service providers, the EU retains a government-to-government approach to cross-border data access. At the same time, the EU has engaged in negotiations with the United States on a possible agreement based on the CLOUD Act framework. In 2019, the European Commission received authorisation from the Council to negotiate an international agreement that would allow EU judicial authorities to send direct requests to U.S.-based service providers, and vice versa[57]. These negotiations are ongoing, largely due to differences concerning fundamental rights safeguards and the scope of any such arrangement.

3.3. WHAT ASEAN CAN LEARN FROM THE U.S. AND EU EXPERIENCE

3.3.1. EXISTING ASEAN MECHANISMS FOR CROSS-BORDER DATA COOPERATION

Cooperation on criminal matters within ASEAN rests on a layered set of instruments rather than a single framework. These instruments can be grouped into four categories: the intra-ASEAN regional framework, multilateral instruments to which Member States are or may become parties, bilateral mutual legal assistance treaties concluded by Member States, and operational or police-to-police cooperation.

(i) The intra-ASEAN regional framework: The principal regional instrument is the 2004 ASEAN Treaty on Mutual Legal Assistance in Criminal Matters (the AMLAT 2004)[58]. It establishes a Central Authority system, a list of forms of assistance (Article 1), and a set of grounds on which assistance may be refused (Article 3), including the absence of dual criminality, the political nature of the offence, and concerns relating to sovereignty or public order. However, the

[56] Case C-311/18, *Data Protection Commissioner v Facebook Ireland Ltd and Maximillian Schrems*, ECLI:EU:C:2020:559, 16.07.2020.

[57] European Commission: *Joint Statement on the Launch of EU-U.S. Negotiations to Facilitate Access to Electronic Evidence*, Brussels: European Commission, 2019.

[58] Treaty on Mutual Legal Assistance in Criminal Matters among Like-Minded ASEAN Member Countries, Kuala Lumpur, 29.11.2004.

AMLAT 2004 was designed as a general mutual legal assistance instrument. It does not address electronic evidence specifically and contains no provisions on expedited preservation of data, on direct cooperation with service providers, or on the electronic transmission of requests.

Two thematic conventions further complement the AMLAT 2004. The 2007 ASEAN Convention on Counter-Terrorism requires States Parties, under Article 6, to exchange intelligence and information related to terrorist acts[59]. Similarly, the 2015 ASEAN Convention Against Trafficking in Persons, Especially Women and Children provides for mutual legal assistance and law-enforcement cooperation in Articles 16 to 18[60]. However, both conventions are limited to their specific subject areas and continue to rely on the broader procedural framework established by the AMLAT 2004. Beyond these binding instruments, ASEAN has adopted several non-binding texts of relevance, among them the 2017 ASEAN Declaration to Prevent and Combat Cybercrime[61], the ASEAN Cybersecurity Cooperation Strategy for 2021 to 2025[62], and the ASEAN Data Management Framework[63] together with the ASEAN Model Contractual Clauses for Cross-Border Data Flows[64]. Although the latter two instruments primarily address commercial data transfers, they contribute to the gradual development of common regional standards and principles on data protection.

(ii) Multilateral instruments relevant to digital evidence: The Budapest Convention on Cybercrime has so far been ratified by only one[65] ASEAN Member State, the Philippines, which acceded to the Convention in 2018[66]. The Second Additional Protocol to the Budapest Convention[67], which addresses direct cooperation with service providers, has limited regional take-up. By contrast,

[59] ASEAN Convention on Counter-Terrorism, 13.01.2007.

[60] ASEAN Convention Against Trafficking in Persons, Especially Women and Children, 21.11.2015.

[61] ASEAN Declaration to Prevent and Combat Cybercrime, 19.09.2017.

[62] Association of Southeast Asian Nations (ASEAN): *ASEAN Cybersecurity Cooperation Strategy 2021-2025*, Jakarta: ASEAN Secretariat, 2022.

[63] Association of Southeast Asian Nations (ASEAN): *ASEAN Data Management Framework*, Jakarta: ASEAN Secretariat, 2021.

[64] Association of Southeast Asian Nations (ASEAN): *ASEAN Model Contractual Clauses for Cross-Border Data Flows*, Jakarta: ASEAN Secretariat, 2020.

[65] Timor-Leste was invited to accede on 6 October 2022 but it has not ratified or acceded.

[66] Convention on Cybercrime, ETS No. 185, Council of Europe, Budapest, 23.11.2001.

[67] Second Additional Protocol to the Convention on Cybercrime on Enhanced Co-operation and Disclosure of Electronic Evidence, CETS no. 224, Council of Europe, 2022.

the 2024 United Nations Convention against Cybercrime[68] is more likely to gain broad support within ASEAN. Chapter V of the Convention on international cooperation contains several provisions relevant to electronic evidence, including obligations relating to the expedited preservation of stored computer data under Article 41 and limited forms of cooperation with service providers. If ratified across the region, the Convention may become the first multilateral instrument on cybercrime to bind all ASEAN Member States.

(iii) Bilateral treaties: A number of intra-ASEAN bilateral mutual legal assistance and extradition treaties predate the AMLAT 2004 and continue to operate in parallel with it, for example agreements between Vietnam and Laos[69] and Vietnam and Indonesia[70]. More important for present purposes are bilateral treaties between ASEAN Member States and key data-host states outside the region. Thailand concluded a mutual legal assistance treaty with the United States in 1986 (in force from 1993)[71], the Philippines in 1994 (in force from 1996)[72], and Malaysia in 2006 (in force from 2009)[73]. Meanwhile, Vietnam, Indonesia, Myanmar, Laos, Cambodia, and Brunei have no such treaty with the United States. Singapore instead operates on the basis of the Mutual Assistance in Criminal Matters Act 2000[74], which permits assistance on a reciprocity basis. As a result, most ASEAN Member States lack a formal treaty mechanism through which domestic authorities can directly seek electronic evidence from U.S.-based service providers. The executive-agreement mechanism created under the CLOUD Act is also not realistically available to most Member States: to date only the United Kingdom[75] and Australia[76] have been

[68] United Nations Convention against Cybercrime, no. A/RES/79/243, 2024.

[69] Hiệp định tương trợ tư pháp về dân sự và hình sự giữa nước Cộng hòa xã hội chủ nghĩa Việt Nam và nước Cộng hòa dân chủ nhân dân Lào, 1999.

[70] Hiệp định tương trợ tư pháp về hình sự giữa Cộng hòa xã hội chủ nghĩa Việt Nam và Cộng hòa In-đô-nê-xi-a, 2013.

[71] Treaty Between the Government of the United States of America and the Government of the Kingdom of Thailand on Mutual Assistance in Criminal Matters, 1986.

[72] Treaty Between the Government of the United States of America and the Government of the Republic of the Philippines on Mutual Legal Assistance in Criminal Matters, 1994.

[73] Treaty Between the Government of the United States of America and the Government of Malaysia on Mutual Legal Assistance in Criminal Matters, 2006.

[74] Mutual Assistance in Criminal Matters Act 2000 (Malaysia), Act 621, 2000.

[75] Agreement between the Government of the United Kingdom of Great Britain and Northern Ireland and the Government of the United States of America on Access to Electronic Data for the Purpose of Countering Serious Crime, TS no 33/2024, 2024.

[76] Agreement between the Government of the United States of America and the Government of Australia on Access to Electronic Data for the Purpose of Countering Serious Crime, no. 24-130.1, 2021.

designated as qualifying foreign governments, and the conditions set out in 18 U.S.C. § 2523 on rule of law, privacy protection, and procedural safeguards[77] make qualification difficult to achieve for many states in the region.

(iv) Operational networks and inter-agency cooperation: ASEANAPOL, established in 1981, facilitates regional police cooperation through annual chiefs-of-police conferences and the ASEANAPOL Database System, which is integrated with INTERPOL's I-24/7 network[78]. The system supports the exchange of operational information, case-related data, and official documents; however, information shared through ASEANAPOL channels is generally treated as police intelligence rather than evidence admissible before courts. Political coordination on transnational crime takes place through the ASEAN Ministerial Meeting on Transnational Crime[79] and the ASEAN Senior Officials Meeting on Transnational Crime[80], while cooperation on mutual legal assistance is addressed through the Senior Officials' Meeting of the Central Authorities on Mutual Legal Assistance in Criminal Matters[81]. Judicial cooperation is also gradually being developed through the Southeast Asia Justice Network, launched under the auspices of UNODC[82]. On the financial side, all ASEAN Member States belong to the Asia/Pacific Group on Money Laundering[83], while all except Vietnam, Laos and Myanmar are members of the Egmont Group of Financial Intelligence Units[84]. These networks operate alongside, rather than within, the formal mutual legal assistance framework.

[77] Clarifying Lawful Overseas Use of Data Act, Pub. L. No. 115-141, Division V, 132 Stat. 1213, 2018.

[78] ASEANAPOL Secretariat: About ASEANAPOL: Chronology, <https://www.aseanapol.org/en>, last accessed on 06/3/2026.

[79] ASEAN Secretariat: *ASEAN Ministerial Meeting on Transnational Crime (AMMTC)*, 19.09.2023.

[80] ASEAN Secretariat: *ASEAN Senior Officials Meeting on Transnational Crime (SOMTC)*, 16.08.2023.

[81] ASEAN Secretariat: Major Committees and Sectoral Bodies, <https://asean.org/our-communities/economic-community/trade-and-market-integration/sectoral-bodies/?utm>, last accessed on 14/3/2026.

[82] United Nations Office on Drugs and Crime (UNODC), *South East Asia Justice Network (SEAJust)*.

[83] Asia/Pacific Group on Money Laundering, *Members: Asia/Pacific Group on Money Laundering*.

[84] Egmont Group: Members by Region, <https://egmontgroup.org/>, last accessed on 22/2/2026.

3.3.2. INSTITUTIONAL AND STRUCTURAL OBSTACLES WITHIN ASEAN

The general critique of mutual legal assistance in cross-border digital investigations applies to ASEAN with particular force. The reasons can be divided into two groups: operational shortcomings in the way the AMLAT 2004 and bilateral treaties function in practice, and structural barriers rooted in ASEAN's institutional identity.

a) Operational shortcomings of the AMLAT 2004 and bilateral treaties

The timeliness of procedures for mutual legal assistance is the first operational issue. The volatile nature of electronic evidence makes timely processing essential, but processing times in the region are measured in months rather than days. Data published in recent mutual evaluation reports by the Asia/Pacific Group on Money Laundering and the Financial Action Task Force provide a partial but useful picture. In Indonesia, the average time for completing an incoming mutual legal assistance request between 2017 and 2022 was approximately fourteen months[85]. In the Philippines, the average completion time has been reported at around one year[86]. From 2019 to February 2025, Malaysia received 621 mutual legal assistance requests. Around 65% were considered viable, while 24% were closed due to insufficient information and 11% were withdrawn. About 53% of completed requests were resolved within twelve months, but many experienced delays, with 46 requests taking over two years and 56 still pending after two years[87]. These figures are consistent with the international literature, which records bilateral request times of between ten months and two years. They also suggest that delays are not caused solely by foreign authorities, as many requests are closed due to incomplete information.

The second operational problem concerns the procedural design of the AMLAT 2004 itself. The Treaty contains no provisions on the expedited preservation of stored computer data, no standardised forms or procedures for requests directed at service providers, no rules on the electronic transmission of requests between Central Authorities, and no specific timeframes calibrated to the volatility of digital evidence. By comparison, the European Investigation Order Directive provides for execution within thirty days as a general rule and

[85] Financial Action Task Force: *Anti-money laundering and counter-terrorist financing measures – Indonesia*, Paris: Financial Action Task Force, 2023, p. 174.

[86] APG: *Anti-money laundering and counter-terrorist financing measures - Philippines*, Sydney: APG, 2019, p. 146.

[87] Financial Action Task Force: *Mutual Evaluation Report of Malaysia*, Paris: Financial Action Task Force, 2025.

ninety days at most[88], while the e-Evidence Regulation reduces production deadlines to ten days, or eight hours in cases involving imminent threat to life or physical safety[89]. The Budapest Convention requires States Parties under Article 29 to be able to order expedited preservation of stored data[90].

The third operational problem is the service-provider gap. The AMLAT 2004 regulates cooperation between states. It cannot be used to compel disclosure by Meta, Google, Microsoft, or Apple, none of which has its global headquarters within an ASEAN Member State. To reach such providers through formal channels, an ASEAN state must either rely on a bilateral mutual legal assistance treaty with the state in which the provider is based or on direct cooperation arrangements offered by the providers themselves. The user data of Meta, Google, Microsoft, and Apple users in Southeast Asia is, in the great majority of cases, controlled by the U.S. parent (or, for some products, by Meta Platforms Ireland Ltd or Google Ireland Ltd for non-U.S. users). As noted above, only Thailand, the Philippines, and Malaysia have such a treaty with the United States. The remaining Member States must use diplomatic channels or rely on the voluntary cooperation of providers, neither of which is suited to the scale of the problem.

b) Structural barriers within ASEAN's institutional framework

The first is the principle of non-interference and the practice of consensus-based decision-making, sometimes referred to as the "ASEAN Way"[91]. The principle of non-interference is set out in the 1976 Treaty of Amity and Cooperation[92] and restated in Article 2(2)(e) and (f) of the ASEAN Charter[93], while consensus remains the standard decision-making procedure under the Charter. Against this background, mechanisms based on mutual recognition,

[88] Directive 2014/41/EU of the European Parliament and of the Council of 3 April 2014 regarding the European Investigation Order in criminal matters, *Official Journal of the European Union*, L 130, 01.05.2014, art. 12.

[89] Directive (EU) 2023/1544 of the European Parliament and of the Council of 12 July 2023 laying down harmonised rules on the designation of designated establishments and the appointment of legal representatives for the purpose of gathering electronic evidence in criminal proceedings, *Official Journal of the European Union*, L 191, 28.07.2023, art. 10.

[90] Convention on Cybercrime, ETS No. 185, Council of Europe, Budapest, 23.11.2001, Art. 29.

[91] Caballero-Anthony, M.: The ASEAN way and the changing security environment: navigating challenges to informality and centrality. *International Politics (Hague, Netherlands)*, 2022; Capie, D., Evans, P. (eds.): 'The ASEAN Way', in: *The Asia-Pacific Security Lexicon* (updated 2nd edition) (pp. 9-20), Singapore: ISEAS Publishing, 2007.

[92] Treaty of Amity and Cooperation in Southeast Asia, Bali, 24.02.1976.

[93] Charter of the Association of Southeast Asian Nations, 20.11.2007.

under which a judicial order issued in one Member State automatically produces legal effects in another without substantive re-examination, are difficult to reconcile with ASEAN's institutional structure. Cross-border information sharing and forms of cooperation that operate beyond direct state control may also be viewed as inconsistent with the principle of non-interference and are therefore unlikely to be fully embraced within ASEAN legal instruments[94].

The second barrier is the diversity of legal systems and procedural traditions across ASEAN. Owing to the region's different historical, political, and legal developments, ASEAN Member States maintain legal systems that differ significantly from one another. The region comprises common law jurisdictions (Brunei Darussalam, Malaysia, Myanmar and Singapore), civil law jurisdictions (Indonesia, Lao PDR, Thailand, Timor-Leste, and Vietnam), and hybrid jurisdictions combining civil and common law features (Cambodia and the Philippines)[95]. Elements of Islamic law also apply in certain subject areas in Brunei, Malaysia, and Indonesia, while Vietnam and Laos retain post-socialist legal features. As a result, rules on the admissibility of evidence, the role of the investigating judge, the independence of prosecutors, and the scope of judicial review of investigative measures vary accordingly. A regional production order would have to operate across ten different criminal procedure codes, each with its own safeguards and its own conception of the proper boundary between investigation and adjudication.

The third barrier is the absence of a uniform regional framework on data protection. Seven Member States have enacted general data protection legislation: the Personal Data Protection Act 2012 (as revised in 2020)[96] in Singapore, the Data Privacy Act 2012 in the Philippines[97], the Personal Data Protection Act 2010 (as amended in 2024) in Malaysia[98], the Personal Data Protection Act 2019 in Thailand[99], the Personal Data Protection Law 2022 in Indonesia[100], the Personal Data Protection Order 2025 in Brunei[101] (which applies to private-sector organisations only), and the Personal Data Protection Law 2025

[94] Sundram, P.: ASEAN cooperation to combat transnational crime: progress, perils, and prospects. *Frontiers in Political Science*, 6 2024.

[95] Smith, R. B.: Complexity of Legal Harmonisation in Southeast Asia: A Diversity of Legal Systems & Languages. *Athens Journal of Law*, 10(2) 2024, pp. 233-254.

[96] Personal Data Protection Act 2012, Republic Act No. 10173, 2012.

[97] Data Privacy Act of 2012, Republic Act No. 10173, 2012.

[98] Personal Data Protection Act 2010, Act 709, 2010.

[99] Personal Data Protection Act (Thailand), B.E. 2562, 2019.

[100] Law No. 27 of 2022 on Personal Data Protection (Indonesia), 2022.

[101] Personal Data Protection Order 2025 (Brunei Darussalam), 2025.

in Vietnam[102]. Cambodia finalised a draft Personal Data Protection Law in 2025[103] but has not yet enacted it, Laos, Myanmar, and Timor-Leste have only partial or sectoral rules. The substantive standards, the scope of lawful processing by public authorities, and the rules on cross-border transfer differ from one statute to another. Without a regional adequacy mechanism, cross-border production orders risk conflicting with the data protection law of the executing state.

3.2. SHORT-TERM LESSONS AND OPTIONS FOR ASEAN

The United States has significant legal and economic power over the leading service providers, which partly explains the effectiveness of the CLOUD Act framework. Although Singapore functions as a regional hub for the operations of major service providers, no ASEAN Member State has comparable leverage. The EU e-Evidence Regulation, by contrast, operates within a regional system founded on mutual trust, common standards of fundamental-rights protection, and supranational judicial oversight. ASEAN has, by design, not developed these features. What the two models offer instead is a set of techniques that may be adapted to the ASEAN context, in particular expedited timeframes, calibrated authority levels for different categories of data, designated legal representatives, and quashing or non-compliance procedures. On this basis, four short-term options may be considered for ASEAN.

The first option is to modernise the AMLAT 2004 and the day-to-day practice of mutual legal assistance within the region. Despite the limitations identified above, mutual legal assistance remains the foundational legal channel for cross-border criminal cooperation, and improving its operation can provide practical benefits while more advanced mechanisms are developed. At the international level, the United Nations Office on Drugs and Crime has issued a Practical Guide for Requesting Electronic Evidence Across Borders for investigators and prosecutors[104]. INTERPOL's e-MLA initiative likewise seeks to establish a technical platform for voluntary use by member countries in conducting mutual legal assistance exchanges[105]. Although neither alters the underlying legal framework, both show how clearer procedures and technical coordination can support practice. At the regional level, the AMLAT

[102] Law on Personal Data Protection (Cambodia), 2025.

[103] Draft Law on Personal Data Protection, Kingdom of Cambodia, final draft version, 2025.

[104] United Nations Office on Drugs and Crime (UNODC): *Practical Guide for Requesting Electronic Evidence Across Borders*, Vienna, 2019.

[105] INTERPOL: Electronic Mutual Legal Assistance: INTERPOL's e-MLA Initiative, 2021.

2004 should be supplemented by an instrument addressing electronic evidence specifically. Such an instrument should permit the electronic transmission of requests between Central Authorities, set indicative timeframes for different categories of data (with shorter periods for subscriber information and for emergency situations), provide for expedited preservation pending the execution of a formal request, and standardise the form in which electronic evidence is transmitted. At the national level, Member States should invest in the operational capacity of their Central Authorities. Malaysia has reported that a significant proportion of incoming mutual legal assistance requests are closed because of incomplete information[106]. This suggests that training investigators and prosecutors, introducing standardised request templates, and establishing dedicated digital-evidence units within Central Authorities are likely to support practical improvements over time.

The second line of action is to develop, on a phased and opt-in basis, a regional pilot for the mutual recognition of production and preservation orders, drawing on the EU experience but calibrated to ASEAN's constraints. Four design features would be appropriate. First, participation should be opt-in among willing Member States rather than mandatory across the region. Second, the scope of the pilot should be limited to defined offence categories in which ASEAN already has thematic conventions or established cooperation, in particular terrorism, child sexual exploitation and abuse, large-scale or transnational fraud, and human trafficking[107]. Third, the categories of data covered should initially be limited to subscriber data and traffic data, in line with the approach taken in the Second Additional Protocol to the Budapest Convention, with content data reserved for ordinary mutual legal assistance until greater institutional trust and procedural consistency are established. Fourth, participation should be conditional on bilateral or plurilateral assessments providing for mutual recognition of data protection standards among participating states. In addition, the authority competent to issue orders should vary according to the sensitivity of the data requested. Grounds for refusal should be limited but clearly defined violations of fundamental rights, threats to national security, and disproportionality.

The third line of action is to develop multi-track, multi-agency operational cooperation in parallel with the formal mutual legal assistance framework. There is scope for ASEANAPOL to develop beyond information exchange to include dedicated cybercrime units with the capacity to support and facilitate

[106] Financial Action Task Force: *Mutual Evaluation Report of Malaysia*, Paris: Financial Action Task Force, 2025, p. 52.

[107] ASEAN: ASEAN Legal Instruments, <https://agreement.asean.org/?utm>, last accessed on 14/3/2026.

cross-border investigations, pilot joint investigation arrangements for complex transnational cases, and secure channels for real-time information exchange. A regional prosecutors' coordination network could facilitate the coordination of charging decisions, evidence sharing, and parallel prosecutions. Cooperation should also extend to customs authorities, tax authorities, and Financial Intelligence Units, given the frequency with which transnational crime involves money laundering and tax evasion. Existing channels through the Egmont Group and the Asia/Pacific Group on Money Laundering can be used more systematically for this purpose. Member States would benefit from continued engagement with the implementing arrangements for the 2024 United Nations Convention against Cybercrime, in particular its provisions on expedited preservation. Seven of the eleven Member States — Brunei Darussalam, Cambodia, Lao PDR, Malaysia, the Philippines, Thailand, and Vietnam — signed the Convention at the Hanoi ceremony in October 2025, with Indonesia, Myanmar, Singapore, and Timor-Leste yet to sign[108]. Vietnam became the first ASEAN State to ratify, depositing its instrument on 17 April 2026. If a substantial number of Member States proceed to ratification, the Convention could over time produce a degree of regional harmonisation on points where the AMLAT 2004 currently contains no specific rules.

The fourth line of action is to strengthen national legal frameworks and the interface with service providers. Member States should consider aligning domestic legislation with the international instruments to which the state is a party, in particular the 2024 United Nations Convention against Cybercrime once it enters into force and the relevant offence-specific conventions on terrorism, trafficking, and corruption. National criminal procedure law should provide a clear basis for the collection, preservation, and admissibility of electronic evidence, and for the use of expedited preservation orders. Member States should also consider, individually or in coordination, the adoption of legislation requiring major service providers offering services in their territory to designate a legal representative for the purpose of receiving and responding to lawful orders concerning electronic evidence. The legislative form chosen for ASEAN need not be a binding regional instrument, which would be difficult to negotiate; similar practical effects may be achieved through a coordinated set of national measures, with thresholds adapted to the size of each market, supported by a soft-law ASEAN framework.

[108] United Nations Treaty Collection: *Status of Treaties: United Nations Convention against Cybercrime*, 2026.

4. CONCLUSION

Cross-border data access for transnational crime control represents one of the most pressing challenges facing ASEAN in an increasingly digital world. The experience of the United States and the European Union shows that no single model provides a comprehensive solution. Mutual legal assistance, unilateral access, and data localisation each address certain concerns while creating others.

For ASEAN, the path forward does not require choosing a single model but rather developing a pragmatic, multi-layered system. This system should modernise traditional mutual assistance, gradually build toward mutual recognition, employ multiple cooperation channels, and engage the private sector as a partner. While achieving the full vision may require a decade or more, beginning this process now is essential to protect ASEAN's security, prosperity, and digital future.

LITERATURE

1. Abraha, H. H.: Law enforcement access to electronic evidence across borders: mapping policy approaches and emerging reform initiatives. *International Journal of Law and Information Technology*, 29(2) 2021, pp. 118-153.
   - DOI: https://doi.org/10.1093/ijlit/eaab001
2. Agreement between the Government of the United Kingdom of Great Britain and Northern Ireland and the Government of the United States of America on Access to Electronic Data for the Purpose of Countering Serious Crime, TS no 33/2024, 2024.
3. Agreement between the Government of the United States of America and the Government of Australia on Access to Electronic Data for the Purpose of Countering Serious Crime, no. 24-130.1, 2021.
4. APG: *Anti-money laundering and counter-terrorist financing measures - Philippines*, Sydney: APG, 2019.
5. ASEAN Convention Against Trafficking in Persons, Especially Women and Children, 21.11.2015.
6. ASEAN Convention on Counter-Terrorism, 13.01.2007.
7. ASEAN Declaration to Prevent and Combat Cybercrime, 19.09.2017.
8. ASEAN Secretariat: *ASEAN Ministerial Meeting on Transnational Crime (AMMTC)*, 19.09.2023.
9. ASEAN Secretariat: *ASEAN Senior Officials Meeting on Transnational Crime (SOMTC)*, 16.08.2023.

10. ASEAN Secretariat: Major Committees and Sectoral Bodies, <https://asean.org/our-communities/economic-community/trade-and-market-integration/sectoral-bodies/?utm>, last accessed on 14/3/2026.

11. ASEAN: ASEAN Legal Instruments, <https://agreement.asean.org/?utm>, last accessed on 14/3/2026.

12. ASEANAPOL Secretariat: About ASEANAPOL: Chronology, <https://www.aseanapol.org/en>, last accessed on 06/3/2026.

13. Asia/Pacific Group on Money Laundering, *Members: Asia/Pacific Group on Money Laundering*.

14. Association of Southeast Asian Nations (ASEAN): *ASEAN Cybersecurity Cooperation Strategy 2021-2025*, Jakarta: ASEAN Secretariat, 2022.

15. Association of Southeast Asian Nations (ASEAN): *ASEAN Data Management Framework*, Jakarta: ASEAN Secretariat, 2021.

16. Association of Southeast Asian Nations (ASEAN): *ASEAN Model Contractual Clauses for Cross-Border Data Flows*, Jakarta: ASEAN Secretariat, 2020.

17. Caballero-Anthony, M.: The ASEAN way and the changing security environment: navigating challenges to informality and centrality. *International Politics (Hague, Netherlands)*, 2022.
    - DOI: https://doi.org/10.1057/s41311-022-00400-0

18. Capie, D., Evans, P. (eds.): 'The ASEAN Way', in: *The Asia-Pacific Security Lexicon* (updated 2nd edition) (pp. 9-20), Singapore: ISEAS Publishing, 2007.

19. Case C-311/18, *Data Protection Commissioner v Facebook Ireland Ltd and Maximillian Schrems*, ECLI:EU:C:2020:559, 16.07.2020.

20. Charter of the Association of Southeast Asian Nations, 20.11.2007.

21. Clarifying Lawful Overseas Use of Data Act, Pub. L. No. 115-141, Division V, 132 Stat. 1213, 2018.

22. Convention on Cybercrime, ETS No. 185, Council of Europe, Budapest, 23.11.2001.

23. Corhay, M., Franssen, V.: Digital Evidence Gathering by US Authorities and Cross-Border Cooperation with US-Based Service Providers, in: Tosza, S.; Franssen, V. (eds.): *The Cambridge Handbook of Digital Evidence in Criminal Investigations*, Cambridge: Cambridge University Press, 2025.
    - DOI: https://doi.org/10.1017/9781009049771.023

24. Council of Europe Treaty Office: *Chart of Signatures and Ratifications of Treaty No. 185*, 2026.

25. Cross, C.: Romance baiting, cryptorom and 'pig butchering': an evolutionary step in romance fraud. *Current Issues in Criminal Justice*, 36(3) 2024, pp. 334-346.
    - DOI: https://doi.org/10.1080/10345329.2023.2248670

26. Cybercrime Convention Committee: *Assessment report on Mutual Legal Assistance: Follow up given by Parties and Observers*, Strasbourg: Council of Europe, 2017.

27. Daskal, J.: Law Enforcement Access to Data Across Borders. *Journal of National Security Law & Policy*, 8(3) 2016, pp. 473-501.

28. Data Privacy Act of 2012, Republic Act No. 10173, 2012.

29. Directive (EU) 2023/1544 of the European Parliament and of the Council of 12 July 2023 laying down harmonised rules on the designation of designated establishments and the appointment of legal representatives for the purpose of gathering electronic evidence in criminal proceedings, *Official Journal of the European Union*, L 191, 28.07.2023.

30. Directive 2014/41/EU of the European Parliament and of the Council of 3 April 2014 regarding the European Investigation Order in criminal matters, *Official Journal of the European Union*, L 130, 01.05.2014, pp. 1-36.

31. Draft Law on Personal Data Protection, Kingdom of Cambodia, final draft version, 2025.

32. Egmont Group: Members by Region, <https://egmontgroup.org/>, last accessed on 22/2/2026.

33. European Commission: *Joint Statement on the Launch of EU-U.S. Negotiations to Facilitate Access to Electronic Evidence*, Brussels: European Commission, 2019.

34. European Commisssion: *Commission Staff Working Document: Impact Assessment Accompanying the Proposal for a Regulation on European Production and Preservation Orders for Electronic Evidence in Criminal Matters*, SWD/2018, 118 final, 2018.

35. European Convention on Mutual Assistance in Criminal Matters, ETS no. 030, Strasbourg: Council of Europe, 20.04.1959.

36. Financial Action Task Force: *Anti-money laundering and counter-terrorist financing measures – Indonesia*, Paris: Financial Action Task Force, 2023.

37. Financial Action Task Force: *Mutual Evaluation Report of Malaysia*, Paris: Financial Action Task Force, 2025.

38. Funk, T. M.: *Mutual Legal Assistance Treaties and Letters Rogatory: A Guide for Judges*, Washington: Federal Judicial Center, 2014.

39. Hemmings, J., Srinivasan, S., Swire, P.: Defining the Scope of 'Possession, Custody, or Control' for Privacy Issues and the Cloud Act. *Journal of National Security Law & Policy*, 10 2020, pp. 631-675.

40. Hiệp định tương trợ tư pháp về dân sự và hình sự giữa nước Cộng hòa xã hội chủ nghĩa Việt Nam và nước Cộng hòa dân chủ nhân dân Lào, 1999.

41. Hiệp định tương trợ tư pháp về hình sự giữa Cộng hòa xã hội chủ nghĩa Việt Nam và Cộng hòa In-đô-nê-xi-a, 2013.

42. Hill, J. F., Noyes, M.: Rethinking Data, Geography, and Jurisdiction, in: Ellis, R., Mohan, V. (eds.): *Rewired: Cybersecurity Governance* (pp. 195-212), Hoboken: John Wiley & Sons, 2019.

43. INTERPOL: Electronic Mutual Legal Assistance: INTERPOL's e-MLA Initiative, 2021.

44. Juszczak, A., Sason, E.: The Use of Electronic Evidence in the European Area of Freedom, Security, and Justice. eucrim, (2) 2023, pp. 182-200.

45. Law No. 27 of 2022 on Personal Data Protection (Indonesia), 2022.

46. Law on Personal Data Protection (Cambodia), 2025.

47. Mayer, J.: Government Hacking, *Yale Law Journal*, 127(3) 2018, pp. 570-662.

48. Millard, C., Millard, C.: *Cloud Computing Law*, Oxford: Oxford University Press, 2021.
    - DOI: https://doi.org/10.1093/oso/9780198716662.001.0001

49. Mitsilegas, V.: *EU Criminal Law*, Oxford: Hart Publishing, 2020.

50. Mutual Assistance in Criminal Matters Act 2000 (Malaysia), Act 621, 2000.

51. National Police Chiefs Council (NPCC): *Digital Forensic Science Strategy*, London, 2020.

52. Personal Data Protection Act (Thailand), B.E. 2562, 2019.

53. Personal Data Protection Act 2010, Act 709, 2010.

54. Personal Data Protection Act 2012, Republic Act No. 10173, 2012.

55. Personal Data Protection Order 2025 (Brunei Darussalam), 2025.

56. Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), *Official Journal of the European Union*, L 119, 4.05.2016, pp. 1-88.

57. 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 and for the execution of custodial sentences following criminal proceedings, *Official Journal of the European Union*, L 191, 28.07.2023.

58. Reichel, P. L., Albanese, J.S.: *Handbook of Transnational Crime and Justice*, Thousand Oaks: SAGE Publications, Incorporated, 2013.
    - DOI: https://doi.org/10.4135/9781452281995

59. Sachoulidou, A.: Cross-border access to electronic evidence in criminal matters: The new EU legislation and the consolidation of a paradigm shift in the area of 'judicial' cooperation. *New Journal of European Criminal Law*, 15(3) 2024, pp. 256-274.
- DOI: https://doi.org/10.1177/20322844241258649

60. Savelyev, A.: Russia's new personal data localization regulations: A step forward or a self-imposed sanction?, *Computer Law & Security Review*, 32(1) 2016, pp. 128-145.
- DOI: https://doi.org/10.1016/j.clsr.2015.12.003

61. Second Additional Protocol to the Convention on Cybercrime on Enhanced Co-operation and Disclosure of Electronic Evidence, CETS no. 224, Council of Europe, 2022.

62. Shurson, J.: Investigative Jurisdiction: The Evolving Limits of Extraterritoriality in Transnational Digital Investigations. *International & Comparative Law Quarterly*, 74(3) 2025, pp. 675-705.
- DOI: https://doi.org/10.1017/S0020589325100985

63. Slimi, H., Chichti, J.: The Nexus Between Cybercrime and Irregular Migration in the Age of Cyberspace: Implications for Geographic Flexibility and Mobility Management. *Global Journal of Flexible Systems Management*, 2026, pp. 1-38.
- DOI: https://doi.org/10.1007/s40171-025-00474-8

64. Smith, R. B.: Complexity of Legal Harmonisation in Southeast Asia: A Diversity of Legal Systems & Languages. *Athens Journal of Law*, 10(2) 2024, pp. 233-254.
- DOI: https://doi.org/10.30958/ajl.10-2-4

65. Sundram, P.: ASEAN cooperation to combat transnational crime: progress, perils, and prospects. *Frontiers in Political Science*, 6 2024.
- DOI: https://doi.org/10.3389/fpos.2024.1304828

66. Svantesson, D.: Data localisation trends and challenges: Considerations for the review of the Privacy Guidelines, *OECD Digital Economy Papers*, Paris: OECD Publishing, 2020.

67. Swire, P., Hemmings, J. D.: Mutual Legal Assistance in an Era of Globalized Communications: The Analogy to the Visa Waiver Program. *NYU Annual Survey of American Law*, 71(4) 2017, pp. 687-800.
- DOI: https://doi.org/10.2139/ssrn.2728478

68. The Stored Communications Act, 18 U.S.C. §§ 2701-2713, 1986.

69. Treaty Between the Government of the United States of America and the Government of the Kingdom of Thailand on Mutual Assistance in Criminal Matters, 1986.

70. Treaty Between the Government of the United States of America and the Government of the Republic of the Philippines on Mutual Legal Assistance in Criminal Matters, 1994.

71. Treaty Between the Government of the United States of America and the Government of Malaysia on Mutual Legal Assistance in Criminal Matters, 2006.

72. Treaty of Amity and Cooperation in Southeast Asia, Bali, 24.02.1976.

73. Treaty on Mutual Legal Assistance in Criminal Matters among Like-Minded ASEAN Member Countries, Kuala Lumpur, 29.11.2004.

74. United Nations Convention against Cybercrime, no. A/RES/79/243, 2024.

75. United Nations Office on Drugs and Crime (UNODC), *South East Asia Justice Network (SEAJust).*

76. United Nations Office on Drugs and Crime (UNODC): *Practical Guide for Requesting Electronic Evidence Across Borders*, Vienna, 2019.

77. United Nations Treaty Collection: *Status of Treaties: United Nations Convention against Cybercrime*, 2026.

78. United States Department of Justice, Criminal Division: *Performance Budget: FY 2017 President's Budget*, Washington: United States Department of Justice, Criminal Division, 2016.

79. United States Department of Justice: *Promoting Public Safety, Privacy, and the Rule of Law Around the World: The Purpose and Impact of the CLOUD Act*, Washington, 2019.

80. United States v. Microsoft Corp., 2018.

81. Wang, A.: Cyber Sovereignty at its Boldest: A Chinese Perspective. *The Ohio State Technology Law Journal*, 16(2) 2020, pp. 395-466.

82. Woods, A. K., 'Mutual Legal Assistance in the Digital Age', in: Gray, D.; Henderson, S. (eds.): *The Cambridge Handbook of Surveillance Law*, Cambridge: Cambridge University Press, 2017.

83. Yanqing, H.: "Game of Laws": Cross-Border Data Access for Law Enforcement Purposes-Models in the United States, Europe, and China. *Global Law Review*, 43(1) 2021, pp. 38-51.