Siber International Journal of Advanced Law (SIJAL)
E-ISSN : 2987-5595
P-ISSN : 2987-5609
https://review.e-siber.org/SIJAL siberpublisher.info@gmail.com +62 812-1046-7572
DOI: https://doi.org/10.38035/sijal.v4i1

Received: 22-08-2026 | **Revised:** 11-09-2026 | **Accepted:** 15-09-2026

Bridging Legal Systems in The Era of Digital Commerce: A Comparative Study of Indonesia and Thailand

Budihardjo Hardisurjo[1], M. S. Tumanggor[2], and St. Laksanto Utomo[3]
[1]Universitas Bhayangkara Jakarta Raya, Jakarta, Indonesia, budiharjo@gmail.com.
[2]Universitas Bhayangkara Jakarta Raya, Jakarta, Indonesia
[3]Universitas Bhayangkara Jakarta Raya, Jakarta, Indonesia

Corresponding Author: budiharjo@gmail.com[1]

Abstract: Digital commerce has transformed cross-border economic relations in Southeast Asia while exposing the limits of territorially bounded regulation. Indonesia and Thailand, two major ASEAN digital markets, have adopted rules on electronic transactions, consumer protection, personal data, cybersecurity, and platform services, yet differences in regulatory structure and enforcement continue to generate uncertainty. This article examines how the two legal systems may be bridged without eliminating legitimate national regulatory autonomy. It employs normative legal research using statutory, conceptual, and comparative approaches. Primary materials include Indonesian and Thai legislation, UNCITRAL instruments, and ASEAN agreements; secondary materials comprise peer-reviewed scholarship and authoritative books on digital trade, data governance, platform regulation, and online dispute resolution. The analysis finds substantial normative convergence in functional equivalence, electronic authentication, privacy protection, and consumer confidence, but identifies divergence in platform supervision, institutional design, cross-border data-transfer safeguards, and remedial mechanisms. It argues for functional harmonization based on minimum interoperable standards rather than wholesale legal unification. A proposed Indonesia–Thailand legal bridge consists of mutual recognition of trustworthy electronic transactions, compatible data-governance safeguards, risk-based platform accountability, coordinated consumer redress, and interoperable online dispute resolution. Such an approach can strengthen legal certainty, preserve regulatory space, and support an inclusive ASEAN digital economy sustainably.

Keywords: ASEAN, Digital commerce, Indonesia, Legal harmonization, Online dispute resolution, Thailand.

INTRODUCTION

Digital trade in Southeast Asia has grown rapidly along with the increasing use of e-commerce, digital platforms, electronic payments, and cross-border data exchange. In the ASEAN context, the development of e-commerce is influenced not only by individual factors, but also by country characteristics, institutional readiness, national culture, and society's capacity to access digital technology (Ayob, 2021). Indonesia and Thailand have become two important countries in ASEAN's digital economy because both have large markets, a continuously growing digital consumer base, and active involvement in regional trade.

The digitalization of trade has transformed economic relations that were once primarily domestic into increasingly cross-border interactions. Digital transactions may involve consumers in one country, business actors in another, global platforms, cross-jurisdictional payment systems, and data processing distributed across various legal territories. Within the Asian framework, digital trade governance has also developed into a complex regime that is not singular and often overlaps (Gao & Chen, 2025). This complexity has generated new legal issues, particularly concerning applicable law, digital consumer protection, personal data security, platform responsibility, digital taxation, and cross-border dispute settlement. Therefore, the regulation of digital trade requires legal harmonization to prevent regulatory fragmentation that may hinder business actors and harm consumers (Deane et al., 2024). Thus, ASEAN digital trade should be directed toward legal certainty, protection of digital society, and adaptive regional legal cooperation (Burri et al., 2024).

Electronic transactions are one of the main foundations of digital trade because they enable legal relations between business actors and consumers to take place without physical presence. Through electronic contracts, electronic signatures, digital payments, and electronic documents, trade activities can be conducted more quickly, efficiently, and across national borders. However, the nature of electronic transactions, which does not always bring the parties together directly, creates the need for legal rules that guarantee the validity of transactions, the identity of the parties, payment security, and the evidentiary value of electronic documents. In this context, digital consumer protection becomes an important issue. Consumers in digital transactions are often in a weaker position because they depend on information provided by business actors or platforms. The risks that arise include inaccurate product information, delivery delays, goods that do not match the order, online fraud, and difficulties in obtaining compensation.

In addition to consumer protection, the security and protection of personal data are also inseparable from digital trade. Every digital transaction usually involves the collection, processing, storage, and transfer of personal data. If such data is misused or leaked, consumers may suffer economic loss, privacy violations, and even identity theft. Therefore, data security standards, the consent of data owners, and legal responsibility for data controllers and processors are necessary. Digital taxation is also a challenge because digital economic activities can be carried out across jurisdictions without the physical presence of business actors. The state needs to ensure that digital business actors fulfill their tax obligations fairly. On the other hand, digital platform supervision is necessary because platforms play a major role in connecting business actors and consumers. Such supervision is important to maintain fair business competition, prevent data misuse, protect consumers, and ensure that digital trade takes place safely, fairly, and responsibly.

To date, there has not been a strong model of legal harmonization between Indonesia and Thailand in the field of digital trade. In fact, legal harmonization is needed to establish common principles regarding the recognition of electronic transactions, digital consumer protection, personal data security, platform supervision, and cross-border dispute settlement. Harmonization does not have to mean unifying all national rules, but rather building minimum standards that can bridge the differences between the legal systems of the two countries. With a stronger model of harmonization, digital trade between Indonesia and Thailand can develop with greater certainty, safety, fairness, and support for ASEAN digital economic integration.

Digital trade regulation in Indonesia and Thailand still reflects a sectoral character because it does not stand within a single integrated legal regime. Issues such as electronic transactions, consumer protection, personal data, digital taxation, business competition, payment systems, and platform supervision generally develop through different legal instruments. In the Southeast Asian context, the variation in these legal frameworks reflects the fact that ASEAN countries pursue digitalization through different paths, whether in terms of policy priorities, institutional capacity, or regulatory readiness (Suranto et al., 2025).

This situation has resulted in regulatory fragmentation. Fragmentation does not merely mean that rules are scattered across different legal instruments; it also indicates the possibility of overlapping authority, differing protection standards, and unequal law enforcement mechanisms. In digital trade, a single transaction may simultaneously involve aspects of electronic contracts, data transfers, cross-border payments, taxation, platform responsibility, and consumer protection. If these aspects are not coordinated within a coherent legal framework, business actors and consumers will face uncertainty regarding their rights, obligations, dispute settlement forums, and the applicable law (Gao & Chen, 2025).

The differences between the legal systems and national policies of Indonesia and Thailand also have the potential to increase legal uncertainty. Digital trade is cross-jurisdictional in nature, whereas national laws still operate based on the territorial boundaries of the state. Therefore, transactions conducted through digital platforms may raise issues concerning the validity of electronic contracts, personal data protection, the responsibility of platform providers, and the effectiveness of consumer remedies. Recent studies on digital trade law show that, without cooperation and convergence of principles, differences in data regulations and national interests may become barriers to trade (Deane et al., 2024).

In the Indonesia–Thailand relationship, there is not yet a strong and specific model of legal harmonization for digital trade. In fact, the global development of digital economy agreements shows that countries are beginning to move toward the formation of common standards concerning data, electronic transactions, digital identity, electronic payments, and emerging technologies (Burri et al., 2024; Jones, 2024). Indonesia–Thailand harmonization should be directed toward the establishment of minimum principles, rather than total uniformity, so that legal certainty, consumer protection, and ASEAN digital economic integration can develop in a balanced manner.

This article offers the idea of a legal bridge in digital trade, namely a concept that seeks to connect differences between legal systems through principles of harmonization. This legal bridge is directed at strengthening the certainty of electronic transactions, digital consumer protection, personal data security, and cross-border dispute settlement. Bilateral harmonization between Indonesia and Thailand is also positioned as part of strengthening ASEAN digital economic integration. Thus, the protection of digital society becomes an important element of modern business law that is fair, adaptive, and sustainable. Based on the above explanation, how can the harmonization of digital trade law between Indonesia and Thailand be formulated based on the development, similarities, and differences in the national regulations of both countries in order to support legal certainty, digital consumer protection, and ASEAN regional digital economic integratio?

METHODS

This study applies normative legal research to examine rules, principles, doctrines, and institutional arrangements governing digital commerce in Indonesia and Thailand. Normative inquiry is appropriate because the principal research question concerns the coherence, comparability, and prospective harmonization of legal frameworks rather than the measurement of individual behavior. The unit of analysis is therefore the legal norm as expressed in legislation, implementing regulation, regional instruments, and authoritative interpretation. The analysis nevertheless treats law as an institutional practice: formal similarity is distinguished from operational equivalence, since identical terminology may produce different outcomes when supervisory mandates, remedies, administrative capacity, or access to justice differ.

Three complementary approaches are used. First, the statutory approach identifies the positive-law architecture in each jurisdiction. Indonesian materials include the Electronic Information and Transactions regime, Government Regulation Number 80 of 2019 on Trading Through Electronic Systems, Law Number 27 of 2022 on Personal Data Protection, consumer-protection legislation, and related implementing measures. Thai materials include the Electronic Transactions Act, the Personal Data Protection Act B.E. 2562 (2019), and the Royal Decree on the Operation of Digital Platform Service Businesses B.E. 2565 (2022). Regional and international benchmarks include the ASEAN Agreement on Electronic Commerce, the emerging ASEAN Digital Economy Framework Agreement agenda, the UNCITRAL Model Law on Electronic Commerce, and the UNCITRAL Model Law on Electronic Signatures. These instruments were selected because they directly regulate, or provide model principles for, the validity of electronic communications, platform governance, privacy, consumer confidence, and cross-border transactions.

Second, the conceptual approach develops the notions of functional equivalence, interoperability, regulatory fragmentation, legal certainty, digital trust, platform accountability, and access to justice. Functional equivalence is particularly important: harmonization need not require identical statutory language if different rules recognize electronic records and signatures with comparable legal effects (UNCITRAL, 1996, 2001). The analysis also draws on scholarship showing that digital trade regulation is a hybrid field in which trade facilitation, privacy, cybersecurity, competition, and consumer law interact (Burri, 2023; Burri et al., 2024). This conceptual framework prevents harmonization from being reduced to deregulation and preserves the state's legitimate authority to protect public interests.

Third, the comparative approach uses a functional matrix covering six dimensions: (1) legal recognition of electronic transactions and signatures; (2) digital consumer rights and remedies; (3) personal-data processing and cross-border transfers; (4) duties and supervision of digital platforms; (5) jurisdiction, evidence, and enforcement; and (6) online dispute resolution. For each dimension, the study identifies convergence, divergence, implementation risks, and opportunities for interoperability. Primary legal materials are interpreted textually and systematically, while secondary materials are used to explain doctrine, regulatory context, and institutional implications. The study does not claim to measure enforcement outcomes empirically. Its contribution is prescriptive: it formulates a legally feasible architecture for bilateral cooperation that complements, rather than displaces, ASEAN processes.

RESULTS AND DISCUSSION

Conceptual Foundations: From Uniformity to Interoperability

The central difficulty in regulating digital commerce is the mismatch between borderless technical infrastructures and territorially bounded legal authority. A marketplace interface may be accessible in Jakarta, operated from Bangkok, use cloud infrastructure in another jurisdiction, process payments through a multinational intermediary, and transfer personal data through several locations. Traditional conflict-of-laws rules remain relevant, but they are often too slow and uncertain to provide routine governance for high-volume, low-value transactions. Digital trade law consequently performs two tasks at once: it facilitates transactions by recognizing electronic acts and it disciplines the risks created by data-intensive, platform-mediated markets.

The first organizing principle is functional equivalence. The UNCITRAL Model Law on Electronic Commerce rejects discrimination merely because information takes electronic form and asks whether an electronic method performs the relevant function of writing, an original, or a signature (UNCITRAL, 1996). The Model Law on Electronic Signatures similarly adopts technology neutrality and reliability criteria rather than privileging one technical design (UNCITRAL, 2001). These ideas matter for Indonesia–Thailand relations because mutual confidence can be built around legal effect and reliability without requiring identical certification systems. If each jurisdiction can determine that a foreign method adequately identifies the signatory, expresses intention, and preserves document integrity, cross-border recognition becomes possible while domestic supervisory structures remain intact.

The second principle is regulatory interoperability. Interoperability is narrower and more practical than unification. It requires rules and institutions to communicate across borders through compatible definitions, minimum safeguards, points of contact, and procedures for recognition and cooperation. Deane et al. (2024) explain that digital trade agreements increasingly respond to fragmentation, while Burri et al. (2024) show that modern digital trade instruments extend far beyond tariff questions to data flows, paperless trading, digital identity, consumer protection, and emerging technologies. The implication is that a legal bridge must connect multiple regulatory domains rather than concentrate exclusively on electronic contracts.

The third principle is protected openness. Cross-border data flows are economically important, but openness cannot be treated as an absolute norm. Privacy, cybersecurity, public order, and regulatory autonomy remain legitimate public interests. Burri (2024) demonstrates that contemporary digital trade agreements employ exceptions, safeguards, transition periods, and rights to regulate to reconcile data-flow commitments with domestic values. Similarly, data-localization measures may constitute trade barriers in some circumstances but may also respond to genuine regulatory concerns, depending on their design, proportionality, and alternatives (Selby, 2017). A defensible Indonesia–Thailand framework should therefore enable transfers subject to accountable processing, security, effective remedies, and justified restrictions.

The fourth principle is substantive digital justice. Formal recognition of electronic contracts has limited value when consumers cannot identify a trader, contest an automated decision, recover a small loss, or enforce a remedy against a foreign platform. Platform markets redistribute power through control over ranking, access, data, payment, and contractual terms. As Riefa (2020) argues, online marketplaces cannot always be understood as neutral noticeboards; their architecture and economic role may justify differentiated responsibility. Harmonization must consequently address transparency, trader traceability, complaint handling, evidence preservation, and proportionate platform duties. These principles guide the following comparison of Indonesian and Thai law.

Development of Digital Trade Regulation in Indonesia

Indonesia’s legal framework concerning electronic transactions and digital trade has developed through a combination of information and electronic transaction law, trade law, consumer protection law, personal data protection law, and dispute settlement mechanisms. Conceptually, this framework demonstrates that digital transactions are no longer viewed as informal economic relations, but as legal relations that give rise to rights, obligations, responsibilities, and legal consequences for the parties involved. The development of global digital trade law also shows a similar tendency, namely the strengthening of regulations concerning e-commerce, electronic contracts, data flows, electronic signatures, and platform governance within modern legal regimes (Burri et al., 2024).

In the area of electronic transactions, Indonesia has established its legal foundation through the Electronic Information and Transactions Law, which has subsequently been amended, including through Law Number 1 of 2024. This regulation is important because it provides legitimacy for electronic information, electronic documents, electronic contracts, and the operation of electronic systems as part of legal activities. With such recognition, legal acts no longer have to be proven solely through physical documents, but may also be proven through electronic records, documents, and systems that meet the requirements of reliability and information integrity (Republic of Indonesia, 2024).

In the field of trading through electronic systems, Indonesia regulates e-commerce activities through Government Regulation Number 80 of 2019 concerning Trading Through Electronic Systems (PMSE). This regulation expands the scope of regulation by covering the parties involved in PMSE, business requirements, obligations of business actors, transaction evidence, electronic advertisements, electronic offers and acceptance, electronic contracts, personal data protection, payments, delivery of goods and services, exchange or cancellation of purchases, and dispute settlement (Republic of Indonesia, 2019). PMSE is therefore not merely understood as online buying and selling activity, but as a legal ecosystem that connects business actors, consumers, platforms, payment systems, and logistics service providers.

Consumer protection is an important part of this framework because digital consumers are often in a weaker position. In electronic transactions, consumers cannot always inspect goods directly, have limited room to negotiate standard clauses, and are highly dependent on information provided by business actors or platforms. The study by Rosidah and Karjoko shows that although Indonesian law has provided a basis for protection through the Consumer Protection Law, the Electronic Information and Transactions Law, the PMSE Regulation, the Regulation on the Operation of Electronic Systems and Transactions, and the latest trade regulations, the restoration of consumer rights in electronic transactions remains far from simple. They emphasize the need for business actor validation and a more efficient compensation mechanism for consumers (Rosidah & Karjoko, 2025).

The issue of digital consumers is also closely related to personal data protection. Digital transactions almost always require the collection, processing, storage, and transfer of personal data, such as identity information, addresses, telephone numbers, payment data, and transaction histories. Law Number 27 of 2022 concerning Personal Data Protection is an important instrument because it regulates principles, types of personal data, the rights of data subjects, the obligations of data controllers and processors, personal data transfers, administrative sanctions, institutional arrangements, international cooperation, and dispute settlement (Republic of Indonesia, 2022). Syailendra, Lie, and Sudiro emphasize that the Personal Data Protection Law is an important step in strengthening personal data protection, although its implementation still faces institutional and law enforcement challenges (Syailendra et al., 2024).

Electronic signatures have a strategic function in strengthening the validity of digital transactions. In modern business transactions, electronic signatures do not merely replace handwritten signatures, but also serve as instruments for identity authentication, consent, document integrity, and evidentiary purposes. Therefore, regulations concerning electronic certification providers, electronic certificates, and digital trust services form an important part of legal certainty. Without strong regulation of electronic signatures, digital contracts may face evidentiary problems, particularly when there is a denial of a transaction or a dispute concerning the authenticity of a document.

Ultimately, Indonesia's legal framework also needs to be strengthened through digital dispute settlement. E-commerce disputes are usually relatively small in value but large in number, and therefore require settlement mechanisms that are fast, inexpensive, and easily accessible. Subagyono and his colleagues show that disputes over online purchases are often more appropriately understood within the framework of the Electronic Information and Transactions Law rather than solely under the Consumer Protection Law, indicating the need for legal reform to address the complexity of modern e-commerce (Subagyono et al., 2024). Online dispute resolution needs to be developed as a dispute settlement mechanism that corresponds to the characteristics of digital trade. Obi-Farinde emphasizes that ODR can expand access to justice in consumer and cross-border e-commerce disputes because conventional court mechanisms are often disproportionate to the value of the dispute (Obi-Farinde, 2021).

Thus, Indonesia's legal framework has provided a foundation for electronic transactions, PMSE, consumer protection, personal data protection, electronic signatures, and digital dispute settlement. However, the main challenge is to build cross-sectoral integration so that regulations do not operate separately. Indonesian digital trade law should be directed toward a balance between business innovation, transaction certainty, data security, consumer protection, and effective access to dispute settlement.

Development of Digital Trade Regulation in Thailand

Thailand's regulation of digital trade shows an increasingly directed development toward the formation of an electronic transaction ecosystem that is secure, trustworthy, and subject to supervision. Its basic framework rests on the Electronic Transactions Act, which provides legal recognition for electronic transactions, electronic documents, electronic signatures, digital identity, and digital trust services. This regulation is important because business relations in the digital economy no longer depend on physical documents or direct meetings between the parties. In the context of global digital trade law, recognition of the electronic form of contracts, documents, and signatures is a fundamental requirement for cross-jurisdictional transactions to have legal certainty (Burri et al., 2024).

In addition to electronic transactions, Thailand has begun to strengthen the regulation of digital platform services. Through the Royal Decree on the Operation of Digital Platform Service Businesses B.E. 2565 (2022), Thailand regulates digital platform service providers that function as intermediaries between business actors, consumers, and users. This regulation includes notification obligations to the authorities, operational transparency, platform classification based on characteristics and risk levels, and supervision of both domestic platforms and foreign platforms that provide services to users in Thailand. This approach shows that platforms are no longer positioned as passive intermediaries, but as actors in the digital economy that bear legal responsibility within the transaction ecosystem (Electronic Transactions Development Agency [ETDA], 2022).

In the field of consumer protection, Thailand faces increasingly complex challenges due to the rise of online transactions, social commerce, and the use of cross-border platforms. Digital consumers are vulnerable to incomplete product information, misleading advertisements, fraud, non-conforming goods, and difficulties in obtaining compensation. Recent studies on digital platform operators in Thailand indicate the need to strengthen platform responsibility because consumer losses do not always arise from direct sellers, but also from weaknesses in platform systems in verifying business actors, monitoring content, and addressing digital fraud (ETDA, 2022).

Personal data protection is also an important pillar of Thailand's digital regulation. The Personal Data Protection Act B.E. 2562 (2019) positions personal data as an object of legal protection through provisions on consent, processing purposes, data subject rights, obligations of data controllers and data processors, cross-border data transfers, and sanctions. The study by Chatsuwan and colleagues shows that compliance with the PDPA remains a challenge, particularly for small and medium-sized enterprises that must adjust their privacy policies, data processing procedures, and accountability mechanisms (Chatsuwan et al., 2023).

In the field of cybersecurity, Thailand links digital security with public trust in electronic services and the digital economy. Threats such as data breaches, online fraud, identity theft, and cyberattacks demonstrate that digital trade regulation cannot be separated from cybersecurity governance. Comparative studies on digital development in ASEAN emphasize that cybersecurity law and data protection are essential prerequisites for building trust in digital platforms and electronic government services (Suranto et al., 2025).

Overall, Thailand's digital economy supervision is moving toward a regulatory model that combines recognition of electronic transactions, platform supervision, consumer protection, personal data protection, and cybersecurity. However, its main challenges lie in the effectiveness of implementation, institutional coordination, law enforcement capacity, and supervision of cross-border platform activities. Thus, Thailand's regulation reflects an effort to build a digital economy that is not only oriented toward innovation, but also toward transparency, security, platform responsibility, and user protection.

Convergence and Divergence in Indonesia–Thailand Digital Trade Law

The similarities and differences in digital trade regulation between Indonesia and Thailand can be examined through five main aspects: the legality of electronic transactions, data security, consumer protection, platform responsibility, and cross-jurisdictional law enforcement. In terms of the legality of electronic transactions, both countries share common ground because they recognize that legal relations in modern trade can be established through electronic means. Electronic contracts, electronic documents, electronic signatures, and digital communications are no longer positioned as secondary evidence, but as legitimate elements of business legal activities. This tendency is in line with the development of global digital trade law, which increasingly integrates e-commerce, paperless trading, electronic authentication, and data flows into contemporary trade regimes (Burri et al., 2024).

Nevertheless, differences emerge in the way the two countries construct their regulatory structures. Indonesia tends to develop digital regulation through dispersed legal instruments, such as information and electronic transaction law, trading through electronic systems, consumer protection, personal data protection, digital taxation, and platform supervision. Thailand also has a framework for electronic transactions and digital platform regulation, but its approach shows a stronger emphasis on supervising platform services as part of digital economy governance. This difference indicates that normative convergence does not always produce the same institutional model.

In the areas of data security and personal data protection, Indonesia and Thailand both face the need to balance data flows with privacy protection. Data has become a central element in digital trade because every transaction involves the collection, processing, storage, and transfer of consumer information. Indonesia has established a foundation through the Personal Data Protection Law, but its implementation still faces institutional challenges, business compliance issues, and questions concerning enforcement effectiveness (Syailendra et al., 2024). Thailand has implemented the Personal Data Protection Act; however, studies on small and medium-sized enterprises' compliance in Thailand show that data protection implementation continues to face technical issues, compliance costs, and organizational readiness challenges (Chatsuwan et al., 2023). The main difference, therefore, does not lie in the recognition of the importance of personal data, but in the level of operational readiness and supervision.

In terms of consumer protection, both countries face relatively similar problems. Digital consumers are in a vulnerable position because they cannot directly inspect products, must deal with standard clauses, and depend on information provided by business actors or platforms. Comparative studies on Indonesia and Thailand show that the main risks in e-commerce include information asymmetry, fraud, non-conforming goods, and limited consumer access to effective remedies (Dewi & Siregar, 2026). In Indonesia, weaknesses in digital consumer protection are also linked to the suboptimal dispute settlement mechanism and the need for legal reform to better suit the nature of electronic transactions (Subagyono et al., 2024).

Sharper differences can be seen in platform supervision. Indonesia still faces challenges in positioning platforms as actors that not only facilitate transactions, but also bear responsibility for information transparency, system security, data protection, and the prevention of practices that harm consumers. Thailand also faces similar issues, particularly in ensuring that digital platform operators are responsible for risks arising from online trading activities. However, Thailand's approach to regulating digital platform services shows a tendency to clarify the position of platforms as specific subjects of supervision within the digital economy.

In cross-jurisdictional law enforcement, Indonesia and Thailand both face the limits of national legal capacity. Digital transactions may involve consumers, sellers, platforms, servers, and payment systems located in different countries. This situation raises issues concerning the applicable law, dispute settlement forum, recognition of electronic evidence, and enforcement of judgments. Digital trade literature emphasizes that regulatory fragmentation in data governance and differences in national standards may create new barriers to cross-border trade, particularly for MSMEs and consumers in developing countries (Deane et al., 2024). The similarities and differences between Indonesia and Thailand should therefore be directed toward the formation of shared minimum principles, rather than total uniformity. Harmonization in the legality of electronic transactions, data protection, digital consumer protection, platform accountability, and cross-jurisdictional dispute settlement will strengthen legal certainty while supporting ASEAN digital economic integration.

Indonesia–Thailand Legal Cooperation in Supporting ASEAN Digital Economic Integration

The challenge of bridging the legal systems of Indonesia and Thailand in digital trade lies in the lack of uniformity in the regulatory structures and law enforcement mechanisms of the two countries. Cross-border digital trade does not only involve buying and selling relations, but also data transfers, the use of platforms, electronic payments, digital contracts, and consumer protection across different jurisdictions. This condition increases the risk of regulatory fragmentation because a single transaction may be subject to various national rules that do not necessarily share the same standards (Burri et al., 2024).

The differences in the legal approaches of Indonesia and Thailand also raise issues in determining the applicable law, the dispute settlement forum, and the responsibility of business actors and digital platforms. Cross-border data protection becomes an important issue because data flows are the backbone of digital trade, while at the same time creating risks of misuse, leakage, and unclear accountability (Deane et al., 2024). The capacity gap between large platforms, small business actors, MSMEs, and consumers means that legal protection does not always operate in a balanced manner. Efforts to bridge the legal systems of Indonesia and Thailand require common principles concerning electronic transactions, consumer protection, data security, platform accountability, and cross-border dispute settlement. Such harmonization is important so that regional digital trade not only promotes economic growth, but also ensures legal certainty, justice, and the protection of digital society (Dewi & Siregar, 2026).

The direction of Indonesia–Thailand digital trade law harmonization should be placed on the formation of shared minimum principles, rather than the unification of all national legal systems. First, harmonization may be directed toward the recognition of electronic transactions, including electronic contracts, electronic signatures, electronic documents, and digital authentication. Such recognition is important so that cross-border transactions have a clear legal basis and can be proven in the event of a dispute (Burri et al., 2024). Second, harmonization needs to strengthen personal data protection standards. Digital trade depends on cross-border data flows, but differences in security and accountability standards may create regulatory fragmentation and weaken consumer trust (Deane et al., 2024).

Third, the responsibility of digital platforms must be clarified, particularly in relation to information transparency, consumer protection, transaction security, and the prevention of data misuse. Fourth, Indonesia and Thailand need to establish a cross-border consumer complaint mechanism that is accessible, fast, and inexpensive. This mechanism should be connected to digital dispute settlement, including online dispute resolution, so that consumers and MSMEs are not burdened by conventional litigation processes (Obi-Farinde, 2021). Digital trade law harmonization should be directed toward a balance between innovation, legal certainty, data protection, platform responsibility, and access to justice within the ASEAN digital economy ecosystem (Lee, 2025).

Indonesia–Thailand cooperation has strategic significance in supporting ASEAN digital economic integration because both countries are important markets in the region and both are facing structural changes in trade due to digitalization. Digital trade is no longer limited to the exchange of goods and services through platforms, but also includes data flows, digital identity, electronic payments, electronic signatures, cross-border logistics, and the use of technology in business relations. In global developments, digital trade law is advancing rapidly through preferential trade agreements and digital economy agreements that incorporate issues of e-commerce, data, cybersecurity, consumer protection, and platform governance as part of modern economic law (Burri et al., 2024). Indonesia–Thailand cooperation should therefore be viewed as part of an effort to build regional legal connectivity, rather than merely an ordinary bilateral relationship.

One important foundation of such cooperation is regulatory interoperability. Interoperability does not mean that Indonesia and Thailand must have absolutely identical rules, but rather that both countries need to establish principles, standards, and procedures that can be mutually recognized in cross-border digital transactions. Without interoperability, business actors will face higher compliance costs because they must adjust to differences in rules concerning electronic contracts, data protection, digital payments, platform responsibility, and dispute settlement. In the ASEAN context, digital regulatory fragmentation may hinder regional trade because national legal systems operate under different standards. Deane, Woolmer, Cao, and Tranter emphasize that regulatory fragmentation in digital trade, particularly in relation to data flows and national policies, can become a serious obstacle to cross-border economic integration (Deane et al., 2024).

Digital trade depends on the collection, processing, storage, and transfer of both personal data and business data. Consumer data, transaction histories, payment information, and logistics data can move across national borders within a very short time. If data security standards are not balanced, consumers and business actors may face risks of data breaches, misuse of personal information, identity theft, and unclear responsibility when violations occur. Studies on ASEAN data governance show that strengthening transparency, regulatory alignment, and mechanisms that support the smooth flow of cross-border data are necessary to promote regional digital integration (Watanabe, 2025). Indonesia and Thailand need to establish minimum standards concerning data security, consent of data owners, cross-border data transfers, obligations of data controllers, and response mechanisms for cyber incidents.

In addition to data security, consumer protection is a major reason for the need for legal cooperation. Digital consumers in cross-border transactions are in a more vulnerable position because they deal with business actors, platforms, payment systems, and logistics providers that may be located in different countries. The problems that arise are not limited to non-conforming goods or delivery delays, but also include non-transparent product information, digital fraud, unfair standard clauses, and difficulties in obtaining compensation. Comparative studies on e-commerce consumer protection in Indonesia and Thailand show that both countries need to strengthen consumer protection in digital transactions, particularly through clearer regulation of consumer rights, business actor obligations, and remedy mechanisms (Dewi & Siregar, 2026). Cooperation between the two countries should therefore be directed toward cross-border consumer complaint mechanisms, information exchange among authorities, and the strengthening of platform responsibility for transactions occurring within their ecosystems.

Digital trade facilitation is also an important agenda. Indonesia and Thailand need to encourage mutual recognition of electronic documents, electronic signatures, digital authentication, and electronic contracts. Such recognition would make it easier for business actors, especially MSMEs, to conduct cross-border transactions without being burdened by excessive administrative procedures. Within the ASEAN framework, the Digital Economy Framework Agreement is viewed as an important instrument for addressing regulatory and digital infrastructure fragmentation while strengthening regional economic cohesion (Lee, 2025). If Indonesia–Thailand cooperation can be aligned with the direction of DEFA, their bilateral relationship could become a practical model for digital legal interoperability in ASEAN.

Large platforms possess legal, technological, and data resources that are far stronger than those of small business actors. Without adequate protection standards, digital integration may widen market inequality and weaken the position of consumers. Therefore, Indonesia–Thailand cooperation should not be oriented merely toward accelerating transactions, but also toward access justice, platform responsibility, digital literacy, and protection mechanisms that are easy to use. Legal cooperation between Indonesia and Thailand within the ASEAN framework should be directed toward four main agendas: regulatory interoperability, data security standardization, cross-border consumer protection, and digital trade facilitation. These four agendas are interconnected because digital trade can only develop sustainably when there is legal trust. Interoperability provides certainty for business actors, data security protects the foundation of digital transactions, consumer protection preserves market fairness, and trade facilitation strengthens regional economic integration.

CONCLUSIONS AND RECOMMENDATIONS

Conclusion

Digital commerce has transformed legal relations between Indonesia and Thailand by combining electronic contracts, platform intermediation, payment services, data processing, and cross-border delivery within a single transaction. Both jurisdictions have moved beyond the assumption that online activity is legally exceptional. They recognize electronic information and signatures, protect personal data, regulate aspects of digital consumer relations, and increasingly subject platforms to public oversight. This study nevertheless finds that normative convergence does not eliminate practical fragmentation. Differences persist in institutional design, platform obligations, transfer safeguards, supervision, and the accessibility of remedies. These differences can raise compliance costs for businesses and leave consumers uncertain about applicable law, responsible institutions, evidence, and enforcement. The appropriate response is functional harmonization rather than complete legal unification.

Indonesia and Thailand can preserve constitutional and regulatory autonomy while establishing interoperable minimum standards. The proposed legal bridge rests on five connected elements: mutual recognition of reliable electronic transactions; compatible principles for lawful, secure, and accountable data processing; risk-based platform duties linked to control and capacity; cross-border cooperation among consumer, data-protection, and digital-economy authorities; and accessible online dispute resolution supported by enforceable outcomes. This model treats legal certainty and rights protection as mutually reinforcing. Trustworthy data governance and effective remedies facilitate trade because they reduce uncertainty and make participation safer for consumers and MSMEs. Bilateral cooperation should also operate as a building block for ASEAN integration. The ASEAN Agreement on Electronic Commerce already supplies common commitments regarding electronic transactions and consumer confidence, while the DEFA process offers a broader setting for regulatory interoperability. An Indonesia–Thailand pilot could translate regional principles into operational protocols and generate lessons for wider adoption. Ultimately, the legitimacy of digital integration depends not only on transaction volume but on whether law distributes risks fairly, preserves regulatory space, and gives individuals meaningful control and redress in markets shaped by platforms and data.

Recommendations

First, Indonesia and Thailand should establish a bilateral working group connected to relevant ASEAN bodies. Its mandate should be technical and outcome-oriented: map equivalent rules, identify gaps, publish common terminology, designate institutional contact points, and develop a phased interoperability roadmap. Participation should include authorities responsible for electronic transactions, trade, consumer protection, personal data, cybersecurity, competition, payments, customs, and justice. Regulatory cooperation will remain incomplete if it is confined to only one ministry or one branch of digital law. Second, both states should adopt a mutual-recognition protocol for electronic signatures, seals, time stamps, transferable records, and trusted digital identities. Recognition should be based on demonstrable reliability, identity assurance, integrity, auditability, and security rather than nationality of the technology provider. A conformity-assessment process and a public list of recognized trust services could reduce uncertainty for courts, businesses, and public agencies. The protocol should remain technologically neutral and be reviewed periodically to accommodate new authentication methods.

Third, data governance should be aligned through a shared baseline incorporating lawfulness, fairness, transparency, purpose limitation, data minimization, accuracy, security, storage limitation, accountability, and enforceable data-subject rights. Cross-border transfers should be permitted through comparable protection, approved contractual safeguards, binding corporate rules, certification, or narrowly defined statutory derogations. Authorities should create a secure procedure for breach notification and regulatory assistance. Restrictions on transfers should be necessary, proportionate, and transparent so that privacy protection is not converted into disguised protectionism. Fourth, platform responsibility should follow a risk-based and function-sensitive model. Obligations should increase where a platform controls trader admission, ranking, advertising, payment, fulfillment, or dispute handling. Core duties should include verification and traceability of traders, clear disclosure of commercial identity and ranking parameters, preservation of transactional evidence, accessible complaint channels, prompt action against fraud, transparent suspension procedures, and periodic systemic-risk assessment for very large services. Safe-harbor protection should be conditional on diligence rather than absolute immunity.

Fifth, Indonesia and Thailand should build a cross-border consumer redress network with a multilingual single-entry portal. Consumers should be able to submit complaints, upload electronic evidence, receive status updates, and proceed to mediation or adjudication without physical presence. Low-value disputes require simplified timelines and costs; platform participation should be mandatory where the dispute arose within its ecosystem. Settlements and determinations should have clear rules for recognition and enforcement. The design should draw on online dispute-resolution principles of accessibility, procedural fairness, data security, and human review (Obi-Farinde, 2021). Finally, harmonization should include capacity building and periodic evaluation. MSMEs need model privacy notices, standard contractual clauses, cybersecurity guidance, and affordable trust services. Consumers need practical digital-literacy support. Independent evaluation should measure complaint resolution, fraud response, data-breach cooperation, compliance costs, and MSME participation. These indicators would ensure that harmonization remains a living process directed toward inclusion and justice rather than a one-time legislative exercise.

REFERENCES

Association of Southeast Asian Nations. (2019). *ASEAN Agreement on Electronic Commerce*.

Ayob, A. H. (2021). E-commerce adoption in ASEAN: Who and where? *Future Business Journal, 7*(1), Article 4. https://doi.org/10.1186/s43093-020-00051-8

Burri, M. (2023). What are digital trade and digital trade law? *American Journal of International Law Unbound, 117*, 99–103. https://doi.org/10.1017/aju.2023.15

Burri, M. (2024). Regulatory autonomy in digital trade agreements. *Journal of International Economic Law, 27*(3), 397–423. https://doi.org/10.1093/jiel/jgae030

Burri, M., Callo-Müller, M. V., & Kugler, K. (2024). The evolution of digital trade law: Insights from TAPED. *World Trade Review, 23*(2), 190–207. https://doi.org/10.1017/S1474745623000472

Chatsuwan, P., Phimoltares, S., Phankokkruad, M., & Kwanmuang, P. (2023). Personal data protection compliance assessment: A privacy policy scoring model for SMEs in Thailand. *Heliyon, 9*(11), e22495. https://doi.org/10.1016/j.heliyon.2023.e22495

Deane, F., Woolmer, E., Cao, S., & Tranter, K. (2024). Trade in the digital age: Agreements to mitigate fragmentation. *Asian Journal of International Law, 14*(1), 154–179. https://doi.org/10.1017/S204425132300036X

Dewi, I. Y., & Siregar, P. A. S. (2026). Legal protection for consumers in e-commerce transactions: Comparative study of Indonesia and Thailand. *Awang Long Law Review, 8*(2). https://doi.org/10.56301/awl.v8i2.2047

Electronic Transactions Development Agency. (2022). *Royal Decree on the Operation of Digital Platform Service Businesses That Are Subject to Prior Notification, B.E. 2565 (2022).*

Gao, X., & Chen, X. (2025). The regime complex for digital trade in Asia and China's engagement. *Asia Europe Journal, 23*, 393–413. https://doi.org/10.1007/s10308-024-00705-0

Jones, E. (2024). Norm entrepreneurship in digital trade: The Singapore-led wave of digital trade agreements. *World Trade Review*. Advance online publication. https://doi.org/10.1017/S1474745624000196

Kuner, C. (2013). *Transborder data flows and data privacy law*. Oxford University Press.

Lee, B. T. H. (2025). ASEAN Digital Economy Framework Agreement. *Journal of Strategic and Global Studies, 8*(1), Article 5.

Mishra, N., & Kugler, K. (2024). International community in the global digital economy: A case study on the African digital trade framework. *International & Comparative Law Quarterly, 73*(4), 853–888. https://doi.org/10.1017/S0020589324000307

Obi-Farinde, M. (2021). A solution for consumer disputes and cross-border e-commerce disputes. *BCDR International Arbitration Review, 8*(1), 133–160.

Republic of Indonesia. (2019). *Government Regulation Number 80 of 2019 concerning Trading Through Electronic Systems*.

Republic of Indonesia. (2022). *Law Number 27 of 2022 concerning Personal Data Protection*.

Republic of Indonesia. (2024). *Law Number 1 of 2024 concerning the Second Amendment to Law Number 11 of 2008 concerning Electronic Information and Transactions*.

Riefa, C. (2020). *Consumer protection and online auction platforms: Towards a safer legal framework*. Routledge.

Rosidah, Z. N., & Karjoko, L. (2025). Enhancing consumer protection in electronic transactions in Indonesia. *Sriwijaya Law Review, 9*(1), 194–207. https://doi.org/10.28946/slrev.Vol9.Iss1.3942.pp194-207

Selby, J. (2017). Data localization laws: Trade barriers or legitimate responses to cybersecurity risks, or both? *International Journal of Law and Information Technology, 25*(3), 213–232. https://doi.org/10.1093/ijlit/eax010

Subagyono, B. S. A., Romadhona, M. K., Chumaida, Z. V., Suheryadi, B., & Elkhasha, N. S. (2024). Can Indonesia's laws keep up? Protecting consumer rights in digital transactions. *Journal of Law and Legal Reform, 5*(3), 869–890. https://doi.org/10.15294/jllr.v5i3.4202

Suranto, B., et al. (2025). State of digitalization in the Southeast Asia region. *Quality & Quantity*. Advance online publication.

Syailendra, M. R., Lie, G., & Sudiro, A. (2024). Personal data protection law in Indonesia: Challenges and opportunities. *Indonesia Law Review*, *14*(2), Article 4. https://doi.org/10.15742/ilrev.v14n2.4

Thailand. (2001). *Electronic Transactions Act B.E. 2544 (2001)*.

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

United Nations Commission on International Trade Law. (1996). *UNCITRAL Model Law on Electronic Commerce with Guide to Enactment*.

United Nations Commission on International Trade Law. (2001). *UNCITRAL Model Law on Electronic Signatures with Guide to Enactment*.

Watanabe, S. (2025). *Current status of ASEAN data governance and its implications for the Digital Economy Framework Agreement*. Economic Research Institute for ASEAN and East Asia.