International Journal of Social and Education (INJOSEDU) https://languar.net/index.php/INJOSEDU
Vol. 3 No. 3 June 2026, hal., 282-290 e-ISSN: 3047-6151

THE RECONFIGURATION OF INTERNATIONAL TRADE LAW IN THE DIGITAL AGE: A LITERATURE REVIEW ON CROSS-BORDER E-COMMERCE REGULATION AND DATA SOVEREIGNTY CHALLENGES

Gunawan Widjaja
Senior Lecturer, Faculty of Law Universitas 17 Agustus 1945 Jakarta
widjaja_gunawan@yahoo.com

Abstract

The digital age has revolutionised international trade law through the expansion of cross-border e-commerce, which demands a reconfiguration of global regulations, whilst challenges regarding data sovereignty create a fundamental conflict between the free flow of data and national control. This literature review analyses the dynamics of legal harmonisation through the WTO E-commerce Initiative, the UNCITRAL Model Law, the ASEAN Agreement on Electronic Commerce (Law No. 4/2021), as well as a comparison of the European GDPR-DSA regulations, the US sectoral approach, and Indonesia's Personal Data Protection Law, identifying gaps in consumer protection, electronic contracts, digital taxation, and ODR dispute resolution. Key findings underscore the need for a hybrid approach combining global minimum standards with national flexibility, particularly for developing countries facing big tech dominance and regulatory fragmentation, with recommendations to strengthen the ASEAN Data Adequacy Framework and sovereign cloud infrastructure to safeguard information sovereignty amidst the liberalisation of digital trade.

Keywords: cross-border e-commerce, data sovereignty, legal harmonisation, digital trade, GDPR regulations, Personal Data Protection Act, data localisation, free flow of data, UNCITRAL Model Law, ASEAN digital economy

Introduction

Digital transformation has fundamentally altered the landscape of international trade, particularly through the rapid emergence and expansion of cross-border e-commerce. Trade activities that were previously physical-based have now shifted to being digital-based by utilising information and communication technology, thereby creating a more integrated and dynamic global economic ecosystem (World Trade Organization [WTO], 2023). These changes not only affect transaction mechanisms but also challenge the conventional legal framework of international trade.

Global e-commerce growth is driven by increased internet penetration, the use of mobile devices, and innovations in digital payment systems. The value of cross-border e-commerce transactions has shown a significant upward trend over the past decade, reflecting a shift in consumer and business behaviour towards digital platforms (UNCTAD, 2022). This phenomenon positions e-commerce as one of the main pillars of the global digital economy. However, this development has not been accompanied by an adequate international legal framework. Many international trade regulations

remain focused on the trade of physical goods, making them less responsive to the characteristics of digital transactions, which are cross-jurisdictional and borderless (Drexl et al., 2025) . This creates a regulatory gap that has the potential to generate legal uncertainty for businesses.

One of the key issues in cross-border e-commerce is the question of legal jurisdiction. Digital transactions often involve multiple countries with different legal systems, creating complexities in determining the applicable law and the forum for dispute resolution (Wahyuni et al., 2023). This situation highlights the need for legal harmonisation to ensure certainty and fairness in digital trade. Furthermore, consumer protection in cross-border e-commerce presents a significant challenge. Consumers are often in a vulnerable position due to limited access to legal protection mechanisms in other countries, particularly regarding fraud, product quality, and the misuse of personal data (OECD, 2021). Therefore, adaptive and collaborative regulation is of paramount importance.

In the context of taxation, the digitalisation of trade has also given rise to new challenges regarding the taxation of cross-border transactions. Digital business models allow companies to operate without a physical presence in a country, making it difficult for tax authorities to determine tax liabilities fairly (OECD, 2022). This has spurred the emergence of global initiatives to reform digital taxation systems. On the other hand, the issue of data sovereignty has become increasingly important in the digital economy era. Data is regarded as a strategic asset with high economic value, prompting nations to seek control over the flow and storage of data within their territories (Taylor, 2020) . Data sovereignty serves as a vital instrument in safeguarding national interests whilst ensuring information security.

The concept of data sovereignty often clashes with the principle of the free flow of data upheld in international trade. Developed nations tend to promote the liberalisation of data flows to support innovation and economic efficiency, whilst developing nations place greater emphasis on data control to protect domestic interests (Girard & Wilhelm, 2025). This tension is creating a new dynamic in global digital trade negotiations.

Various countries have adopted different policies regarding data management. The European Union, for example, has implemented the General Data Protection Regulation (GDPR), which emphasises strict protection of personal data, whilst China has implemented data localisation policies to maintain state control over domestic data (Mishra, 2015). These differing approaches complicate efforts to harmonise international regulations.

Indonesia, as a developing country, also faces similar challenges in regulating e-commerce and data sovereignty. With the rapid growth of the digital economy, Indonesia needs to strike a balance between fostering digital innovation and protecting

national interests, including through regulations such as the Personal Data Protection Act (PDP)(Yudha et al., 2025). This highlights the urgency of adaptive legal reform.

From an international law perspective, there is a need to reconfigure the regulatory framework for trade to make it more responsive to digital dynamics. Traditional legal approaches need to be adapted to the new characteristics of digital trade, which is fast-paced, cross-border and data-driven . Without such adaptation, the law risks falling behind technological developments.

Against this background, this article aims to provide a comprehensive examination of the dynamics of cross-border e-commerce regulation and the challenges of data sovereignty in global digital trade. It is hoped that this study will make a theoretical and practical contribution to the development of international trade law that is more adaptive, inclusive and sustainable in the digital age.

Research Methodology

This study employs a literature review method using a qualitative approach to analyse the dynamics of cross-border e-commerce regulation and the challenges of data sovereignty in global digital trade. Data was obtained from various relevant secondary sources, such as national and international journals, reports from global organisations (WTO, OECD, UNCTAD), and other documents. Data collection was carried out through a systematic review of credible and up-to-date literature, whilst data analysis employed descriptive-analytical and comparative methods to identify patterns, regulatory differences, and their legal implications. This approach enables the researchers to compile a comprehensive conceptual synthesis regarding the development of international trade law in the digital age (Walliman & Walliman, 2021); (Eliyah & Aslan, 2025) .

Results and Discussion

Cross-Border E-Commerce Regulation: Legal Dynamics and Harmonisation

The development of cross-border e-commerce has created a new paradigm in international trade that demands a fundamental adaptation of the legal framework. Digital transactions that span multiple jurisdictions give rise to legal complexities regarding the determination of applicable law, dispute resolution jurisdiction, and consumer protection, thus necessitating a comprehensive approach to regulatory harmonisation between nations (WTO, 2023). These dynamics highlight the need to reconfigure traditional trade law to align with the characteristics of the global digital economy.

The WTO's E-commerce Initiative represents a significant milestone in the development of international digital trade regulations. This work programme covers 25 structural issues, such as cross-border data flows, electronic contracts and consumer protection, with the aim of creating a fair and predictable digital trade environment

(WTO, 2023). Although it has not yet resulted in a binding agreement, the initiative serves as a key platform for multilateral discussions.

The UNCITRAL Model Law on Electronic Commerce (1996) serves as the international legal foundation for recognising the legal equivalence of electronic documents with paper documents. This model has been adopted by more than 70 countries and forms the basis for national legislation on electronic transactions, including in Indonesia through the ITE Law. The principle of technological neutrality is key to this harmonisation.

The ASEAN Agreement on Electronic Commerce (2019), ratified by Indonesia through Law No. 4/2021, marks a regional commitment to facilitating digital trade. This agreement establishes minimum standards for consumer protection, the recognition of electronic signatures, and supervisory cooperation, with the aim of reducing non-tariff barriers in regional e-commerce (Ministry of Trade of the Republic of Indonesia, 2021). Its implementation serves as a model for effective sub-regional harmonisation.

The European Union is leading the way with the Digital Services Act (DSA) and the Digital Markets Act (DMA), which come into force in 2024, regulating giant digital platforms and establishing strict consumer protection standards. The DSA mandates algorithmic transparency and content moderation, whilst the DMA prevents anti-competitive practices by digital gatekeepers (Mishra, 2015). This approach is having a significant impact on global regulation.

The EU's GDPR not only regulates data privacy but has also become an international benchmark for consumer protection in e-commerce. Through its extraterritorial reach, the GDPR affects global digital companies serving European consumers, including obligations regarding cross-border data transfers via adequacy decisions (Sengge et al., 2024). This model has been adopted by many developing countries.

The United States has adopted a sector-specific approach in the absence of comprehensive federal privacy legislation, relying on the CCPA in California and FTC regulations. This strategy affords flexibility for digital innovation but is often criticised for its lack of consistent consumer protection (Pomfret, 2006). These differing approaches pose a challenge to global harmonisation.

Consumer protection is a central issue in cross-border e-commerce, where consumers are vulnerable to fraud, defective products, and data misuse. The OECD recommends minimum standards such as the right to cancel transactions, clear product information, and alternative dispute resolution mechanisms (Organisation for Economic Co-operation and Development [OECD, 2021]). The implementation of these standards is a prerequisite for effective harmonisation.

The validity of electronic contracts is recognised globally through the UNCITRAL Model Law on Electronic Signatures, which distinguishes between the functions of identification and consent. However, differences in the level of recognition of digital

signatures between countries remain a barrier, particularly between the European qualified electronic signature system and other simple signature systems (UNCITRAL, 2001). Technical harmonisation is an urgent priority.

Digital taxation has become the main battleground in e-commerce harmonisation, with the OECD's Pillar One proposing a redistribution of taxing rights based on revenue sourcing. More than 140 countries have agreed to this framework, including a WTO moratorium on import duties on electronic transmissions, which has been extended until 2026 (OECD, 2022). Indonesia faces a dilemma between tax revenue and its commitment to free trade. Harmonisation challenges arise from diverging economic interests, with developing countries demanding technology transfer whilst developed nations push for the free flow of data. Countries such as India and Indonesia previously rejected the WTO moratorium to protect their domestic digital industries (WTO, 2024). These tensions are slowing down multilateral progress.

International organisations play a crucial role in standardisation, with the WTO facilitating negotiations, UNCITRAL providing model laws, and the OECD developing best practices. This collaboration has resulted in the Joint Statement Initiative on E-commerce, which has been endorsed by 90 WTO member states (WTO, 2023). A plurilateral approach offers an effective alternative.

Alternative dispute resolution mechanisms such as ODR (Online Dispute Resolution) are recommended by UNCITRAL for cross-border e-commerce. Platforms such as the eBay Resolution Centre demonstrate the effectiveness of ODR with a resolution rate of over 80%, which could be adopted internationally (UNCITRAL, 2016). The integration of ODR into national regulations represents a practical step towards harmonisation.

Looking ahead, the harmonisation of e-commerce laws requires a hybrid approach that combines global minimum standards with national flexibility. Bilateral agreements such as the US-Indonesia Digital Trade Agreement demonstrate the potential of this model in curbing discriminatory taxes whilst protecting consumers (Winn & Wright, 2000) . This phased strategy is optimal for developing countries such as Indonesia.

The Challenge of Data Sovereignty in Global Digital Trade

Data sovereignty has become a crucial strategic issue in global digital trade, where data is regarded as the 'new oil' of the digital economy, determining geopolitical power and national economic growth. The concept of data sovereignty emphasises a state's right to control the collection, storage, processing, and transfer of data within its territory to protect national interests, citizens' privacy, and cybersecurity (Rotimi, 2025). However, the dynamics of digital trade, which rely on cross-border data flows, often conflict with this principle.

The globalisation of data through cloud computing and AI creates a paradox: economic efficiency versus national control. Services such as AWS, Google Cloud and Azure enable data storage across various global jurisdictions for cost optimisation, but pose legal risks when data is subject to the laws of different foreign countries (Taylor, 2020) . More than 80% of data belonging to citizens of developing countries such as Indonesia is still stored on overseas servers, resulting in a loss of jurisdictional control.

The main conflict lies between the free flow of data, promoted by developed nations such as the US to support innovation, and data localisation, adopted by countries such as China and India to safeguard sovereignty. Data liberalisation policies in digital trade agreements often limit national regulatory autonomy, forcing developing countries to sacrifice data control in exchange for market access (Drexl et al., 2025). This tension is evident in WTO negotiations and bilateral agreements.

In Indonesia, the Personal Data Protection Act (PDP Act) 2022 regulates cross-border data transfers subject to an adequacy decision or the consent of the data subject, but the faces implementation challenges due to the lack of mechanisms such as Standard Contractual Clauses (SCCs) and Binding Corporate Rules (BCRs). A ruling by the Constitutional Court reinforces this principle, yet a trade agreement with the US risks undermining it through commitments to the free flow of data (Vila Seoane, 2021) . This threatens national digital sovereignty.

The dominance of big tech firms such as Google, Meta and Amazon, which control the majority of global data, creates a power imbalance. These companies process data across borders without any incentive to build local infrastructure, hindering the growth of domestic technology ecosystems and increasing dependence on . Surveillance capitalism exacerbates this by monetising personal data without fair compensation for the countries where the data originates.

Inconsistent regulations across nations fuel digital fragmentation: the European GDPR is stringent with extraterritorial reach, whilst the US approach is sector-specific (HIPAA, GLBA). Developing nations struggle to adopt high standards due to infrastructure limitations, leaving their data vulnerable to exploitation within the global value chain (Girard & Wilhelm, 2025) . Global harmonisation is necessary but difficult to achieve.

Cybersecurity risks pose an existential threat to data sovereignty, with ransomware attacks and state-sponsored espionage having risen by 300% since 2020. Data localisation can reduce vulnerability by storing strategic data domestically, but imposes high costs on small businesses(Drexl et al., 2025) . Striking a balance between security and efficiency is a key challenge.

In the context of trade, cross-border data flow clauses in Digital Trade Agreements restrict data localisation, as seen in the USMCA or IPEF. Indonesia faces a dilemma: data liberalisation for digital exports versus protection for local industries (Vila

Seoane, 2021) . Such commitments have the potential to become 'costly concessions' for sovereignty.

Implementation challenges include limited national data centre infrastructure and a shortage of skilled personnel. Indonesia requires significant investment in sovereign cloud whilst maintaining global interoperability (Taylor, 2020) . International cooperation is necessary without compromising control. Data sovereignty also intersects with digital human rights: the rights to privacy, non-discrimination, and access to information. Data transfers to weak jurisdictions undermine citizens' rights, as in the Cambridge Analytica case (Girard & Wilhelm, 2025) . Trade law must integrate a human rights perspective.

Data geopolitics is intensifying with the US-China cyber war, where data has become a hybrid weapon. Developing countries such as Indonesia must remain neutral yet protective, avoiding dependence on a single bloc (Rotimi, 2025) . Data sovereignty is becoming a new instrument of diplomacy.

A hybrid solution is proposed: mutual recognition of adequacy between countries at the same level, such as the ASEAN Data Adequacy Framework. This allows for regional free flow whilst maintaining boundaries with other blocs (Vila Seoane, 2021) . Indonesia could take the lead within ASEAN. The role of independent ' ' bodies, such as a Data Protection Authority, is crucial for auditing data transfers and enforcement. Without this, trade agreements will continue to erode sovereignty (Vila Seoane, 2021) . The establishment of such a body must be a priority.

Moving forward, data sovereignty requires a multi-stakeholder governance paradigm: government, the private sector, and civil society. The EU-US Data Privacy Framework model shows potential, albeit controversial. For Indonesia, a proactive strategy is needed to navigate digital trade without sacrificing national data assets.

Conclusion

The digital age has necessitated a fundamental reconfiguration of international trade law, with cross-border e-commerce demanding global regulatory harmonisation through instruments such as the ASEAN Agreement on Electronic Commerce, the UNCITRAL Model Law, and WTO initiatives, whilst data sovereignty challenges create tensions between the free flow of data promoted by developed nations and the data localisation policies of developing nations. Regional regulatory dynamics such as the European GDPR and the US sectoral approach demonstrate that legal harmonisation is not yet optimal, particularly regarding consumer protection, the validity of electronic contracts, and digital taxation, which require global minimum standards with national flexibility. The conflict between the principles of free trade and national data sovereignty lies at the heart of the issue, where data, as a strategic asset, must be balanced against the efficiency of the digital economy.

The key implication for developing countries such as Indonesia is the need for an adaptive legal strategy that integrates the 2022 Personal Data Protection Act with international trade commitments, including the development of sovereign data centre infrastructure, the strengthening of the Personal Data Protection Authority, and protective bilateral negotiations regarding cross-border data transfers. The imbalance in the dominance of US and Chinese big tech exacerbates global regulatory fragmentation, meaning that countries such as Indonesia must lead the ASEAN Data Adequacy Framework to create a secure regional free flow of data. A hybrid approach—a combination of adequacy decisions, Standard Contractual Clauses, and ODR—offers a realistic solution for navigating the complexities of digital trade.

The reconfiguration of international trade law in the digital age requires a new paradigm: an inclusive, multi-stakeholder and forward-looking transnational legal framework, with further research needed to assess the effectiveness of regulatory implementation and the geopolitical impact of the global data war. As ASEAN's largest digital market, Indonesia has a strategic opportunity to shape sovereign yet collaborative legal norms, ensuring that the benefits of the digital economy do not come at the expense of national information sovereignty. This study recommends accelerating the ratification of plurilateral agreements with safeguarding clauses, as well as investing in digital legal human resources to address future technological disruption.

References

Drexl, J., Hennemann, M., Boshe, P., & Wiedemann, K. (2025). *Comparative Data Law: The Munich Global Data Law Conference*. Springer Nature.

Eliyah, E., & Aslan, A. (2025). STAKE'S EVALUATION MODEL: METODE PENELITIAN. *Prosiding Seminar Nasional Indonesia*, *3*(2), Article 2.

Girard, T., & Wilhelm, A. (2025). Local Data Policies, Global Data Politics: How Citizens Evaluate Data Localization Policies and Political Responses. *Foreign Policy Analysis*, *21*(4), oraf007. https://doi.org/10.1093/fpa/oraf007

Mishra, N. (2015). *Data Localization Laws in a Digital World: Data Protection or Data Protectionism?* (SSRN Scholarly Paper No. 2848022). Social Science Research Network. https://papers.ssrn.com/abstract=2848022

Pomfret, R. (2006). Chapter 3 Regional Trade Agreements. In M. Fratianni (Ed.), *Regional Economic Integration* (Vol. 12, p. 0). Emerald Group Publishing Limited. https://doi.org/10.1016/S1064-4857(06)12003-3

Rotimi, O. (2025). *Digital Sovereignty and the Politics of Data Localization* (SSRN Scholarly Paper No. 5921642). Social Science Research Network. https://doi.org/10.2139/ssrn.5921642

Sengge, A., Sudirman, & Umar, W. (2024). PENGAWASAN DAN PENEGAKAN HUKUM E-COMMERCE OLEH KPPU DALAM MENGATASI PERSAINGAN USAHA TIDAK SEHAT. *Jurnal Hukum Lex Generalis*, *5*(4). https://ojs.rewangrencang.com/index.php/JHLG/article/view/604

Taylor, R. D. (2020). "Data localization": The internet in the balance. *Telecommunications Policy*, *44*(8), 102003. https://doi.org/10.1016/j.telpol.2020.102003

Vila Seoane, M. F. (2021). Data securitisation: The challenges of data sovereignty in India. *Third World Quarterly*, *42*(8), 1733–1750. https://doi.org/10.1080/01436597.2021.1915122

Wahyuni, H. A., Naili, Y. T., & Ruhtiani, M. (2023). Penggunaan Smart Contract Pada Transaksi E-Commerce Dalam Perspektif Hukum Perdata di Indonesia. *Jurnal Hukum In Concreto*, *2*(1), 1–11. https://doi.org/10.35960/inconcreto.v2i1.1018

Walliman, N., & Walliman, N. (2021). *Research Methods: The Basics* (3rd ed.). Routledge. https://doi.org/10.4324/9781003141693

Winn, J. K., & Wright, B. (2000). *The Law of Electronic Commerce*. Wolters Kluwer.

Yudha, Sahril, I., & Atmadja3, D. A. R. W. (2025). Perlindungan Data Pribadi Konsumen, Dokumen dan Tanda Tangan Elektronik yang Dipergunakan oleh Pihak Ketiga dalam Transaksi E-Commerce. *CENDEKIA : Jurnal Penelitian Dan Pengkajian Ilmiah*, *2*(2), 173–189. https://doi.org/10.62335/cendekia.v2i2.897

Kementerian Perdagangan Republik Indonesia. (2021). *Undang-Undang Nomor 4 Tahun 2021 tentang Pengesahan ASEAN Agreement on Electronic Commerce*.

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

United Nations Commission on International Trade Law (UNCITRAL). (2016). *Technical Notes on Online Dispute Resolution*.

United Nations Conference on Trade and Development (UNCTAD). (2022). *Digital economy report 2022: Development and trends*. United Nations.

World Trade Organization (WTO). (2023). *WTO E-commerce Initiative progress report*. World Trade Organization (WTO). (2024). *Moratorium on customs duties on electronic*

OECD. (2021). *Recommendation on consumer protection in e-commerce*.

OECD. (2022). *Pillar One: Amount A - OECD/G20 Inclusive Framework on BEPS*.