

PERSONAL DATA PROTECTION ON INTERNATIONAL DIGITAL TRADE: HARMONIZING STATE REGULATIONS THROUGH A COMMON STANDARD

Gita Venolita Valentina Gea
Fakultas Hukum, Universitas Surabaya
email: gitavenolita@staff.ubaya.ac.id

Jill Grezelda Wijaya
Fakultas Hukum, Universitas Surabaya
email: jillgrezeldaw@gmail.com

Olivia Clarissa
Fakultas Hukum, Universitas Surabaya
email: oliviaclarissa2@gmail.com

Aurelia Kimberley Clarence Witanto
Fakultas Hukum, Universitas Surabaya
email: veronicaaurelia18@gmail.com

disampaikan 19/02/2025 – di-review 11/04/2025 – diterima 28/06/2025
DOI: 10.25123/zbea9p38

Abstract

The advancement of digital trade has brought considerable benefits, yet it also presents significant challenges, particularly in protecting users' personal data. Digital trade platforms commonly require users to share personal information, raising concerns over data security and accountability. Current regulations governing personal data protection are primarily limited to national or regional legal systems, resulting in a lack of harmonization that impedes the seamless flow of international trade. This paper explores the pressing need for a standardized global framework for personal data protection within the digital trade landscape. Using a normative juridical approach, the study examines various regional legal regimes and assesses the relevance of international trade principles in addressing data protection issues. The analysis highlights the absence of a globally recognized standard for personal data protection in digital trade and finds that existing international instruments are inadequate for meeting current challenges. Given UNCITRAL's role in shaping international trade law, the development of a new legal framework, such as a Model Law, should be pursued. As a form of soft law, a Model Law offers a practical and adaptable tool for harmonizing legal standards across jurisdictions. Its adoption would enhance legal certainty and ensure the protection of personal data in international digital trade transactions, thereby upholding the rights of all parties involved.

Keywords:

digital trade; model law; personal data protection

Abstrak

Perkembangan perdagangan digital, di satu sisi membawa kemajuan signifikan, namun di sisi lain juga menimbulkan risiko terhadap perlindungan data pribadi para penggunanya. Platform perdagangan digital kerap mensyaratkan penyediaan data pribadi tertentu, yang kemudian memunculkan kekhawatiran konsumen terkait tanggung jawab atas pengelolaan dan perlindungan data tersebut. Regulasi mengenai perlindungan data pribadi saat ini masih terbatas pada lingkup hukum nasional atau regional. Ketidakteraturan pendekatan negara dalam mengatur perlindungan data pribadi menimbulkan hambatan dalam pelaksanaan perdagangan internasional. Tulisan ini

bertujuan mengkaji urgensi keseragaman pengaturan perlindungan data pribadi pada tingkat internasional dalam konteks perdagangan digital. Penelitian ini menggunakan metode yuridis normatif dengan menganalisis perbandingan kerangka hukum regional serta menelaah bagaimana prinsip-prinsip perdagangan internasional dapat diterapkan dalam merespons isu perlindungan data pribadi. Hasil kajian menunjukkan belum adanya standar internasional yang bersifat universal terkait perlindungan data pribadi, khususnya dalam sektor perdagangan digital. Instrumen internasional yang ada saat ini belum memadai untuk mengakomodasi permasalahan tersebut secara menyeluruh. Oleh karena itu, mengingat UNCITRAL memiliki mandat untuk mengembangkan kerangka hukum dalam bidang perdagangan internasional, penting untuk mendorong pembentukan suatu kerangka hukum baru yang berfungsi sebagai standar bersama dalam perlindungan data pribadi pada transaksi perdagangan digital. Kerangka tersebut dapat diwujudkan dalam bentuk *Model Law*, yakni *soft law* yang dirancang dengan pendekatan yang aplikatif guna mendorong harmonisasi antarnegara. Keberadaan standar bersama dalam *Model Law* ini diharapkan dapat memberikan kepastian hukum terkait perlindungan data pribadi dalam perdagangan digital internasional, serta menjamin hak-hak para pihak yang terlibat di dalamnya.

Kata Kunci:

model law; perdagangan digital; perlindungan data pribadi

Introduction

Technological change has always presented a significant challenge to existing regulatory structures.¹ The growth of technology in the last few decades has caused digitalization in various aspects of our lives. Digitalization which is a process of changing from conventional activities to technology based activities has brought significant changes to people's lives and behaviours.² Trade and business are two aspects that can not be separated from digitalization as the growth of technology has brought unprecedented global economic changes³ also with its competitiveness.⁴ Due to the digitalization, companies that engaged in trade activities have started to shift their business model to a digital based business. Form of digitalization in trade and business is the emergence of electronic commerce. The internet indeed become an important trading tool for companies as it allows them to conduct saving on the cost of expensive trading platforms and helps them to optimize and reduce logistic costs.⁵

¹ Renuad Sorieue, Jennifer R. Clift, and Jose Angelo Estrella-Faria, Establishing a Legal Framework for Electronic Commerce: The Work of the United Nations Commission on International Trade Law (UNCITRAL), International Lawyer Vol. 35, No. 1, 2001.

² Joseph Amankwah-Amoah et al., COVID-19 and Digitalization: The Great Acceleration, Journal of Business Research Vol. 136, No. July, 2021, p. 602–11.

³ Taufiq Adiyanto, The Analysis of Indonesian Electronic Transaction Tax (ETT) Under WTO Law, Law Development Journal Vol. 5, No. 225, 2023, p. 209–31.

⁴ Dolores Añón Higón and Daniel Bonvin, Digitalization and Trade Participation of SMEs, Small Business Economics, Vol. 62 No.3, 2024.

⁵ Ikrom Ahmedov, The Impact Of Digital Economy On International Trade, European Journal of Business and Management Research Vol. 5, No. 4, 2020.

As a subset of digital trade, electronic commerce brought various advantages for all parties involved, which is electronic commerce companies, sellers, and consumers. Nevertheless, digital trade in the context of electronic commerce also brought disadvantages related to personal data protection. Personal data protection is related to the risks of the growth of cyber security as a minus point of digitalization in trade and business which has been a critical challenge.⁶ Meltzer reports that the global expansion of the internet is transforming international trade. As digital connectivity grows, the risks of cyberattacks are also increased.⁷ Additionally, Oddenino examines that cyber security plays a paradoxical role in international trade and each state has adopted domestic measures to ensure cyber security at a national level.⁸

Electronic commerce companies generally require its users as consumers to submit their personal data before conducting a transaction. Personal data, referring to the General Data Protection Regulation 2016/679 issued by The European Union (GDPR), particularly in Article 4 paragraph 1, defined it as:

“any information relating to an identified or identifiable natural person, an identifiable natural person is one who can be identified directly or indirectly, in particular by reference to an identifier such as name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, cultural or social identity of that natural person.”

This personal data protection, where electronic commerce companies often require some personal data of its user, raises consumers' concerns about the responsibility of the electronic commerce companies being accountable for the consumers' or users' personal data. Throwing back into 2020 when Indonesia was flabbergasted by the breach of up to 91 million of Tokopedia users' personal data that were traded in the black market.⁹ This triggered the government to accelerate the discussion of Indonesia's regulation on personal data protection.

⁶ Rahmonov Jaloliddin, Digitalization in Global Trade: Opportunities and Challenges for Investment, *Global Trade and Customs Journal* Vol. 18, No. 10, 2023, p. 391–95.

⁷ Joshua P Meltzer, *Cybersecurity, Digital Trade, and Data Flows: Re-Thinking a Role for International Trade Rules*, *Global Economy & Development*, 2020.

⁸ Alberto Oddenino, Digital Standardization, Cybersecurity Issues and International Trade Law, *Questions of International Law* Vol 51, No. 2018, 2021, p. 31–51.

⁹ Alvansa Vickya and Reshina Kusumadewi, Kewajiban Data Controller Dan Data Processor Dalam DAta Breach Terkait Perlindungan Data Pribadi Berdasarkan Hukum Indonesia Dan Hukum Singapura: Studi Kasus Data Breach Tokopedia, *Padjajaran Law Review*, Vol. 9, No. 1, 2021.

Some large-known e-commerce also have experienced data breaches such as e-Bay in 2014 and Alibaba in 2022 which raise a concern in the sector of data protection of e-commerce users. In order to overcome these concerns and also to provide personal data security for consumers, states have established its own regulations related to personal data protection. Up until now, there are several states that already issued a legal basis relating to electronic commerce and personal data protection including Indonesia. Several domestic regulations on concerning the personal data protection include China's Personal Information Protection Law (PIPL), United States with its state-based approach regulation such as the California Consumer Privacy Act of 2018 (CCPA), and The European Union which issued the GDPR in 2016. Apart from that, Indonesia has also followed by issuing the Law No. 27 of 2022 on Personal Data Protection (UU PDP).

Each state has developed and issued their own regulations regarding personal data protection which have been adapted according to the criteria, characteristics, and the objectives of each state. Those regulations have its own approach and main focus, just as China with its sovereignty-focused regulation which focused on strict data localization¹⁰ or the GDPR with its strong and right-based approach and provide extraterritorial jurisdiction.¹¹ This will lead to regulations differences between each state regarding the same concern, moreover, according to the United Nations Trade and Development (UNCTAD) that only 137 from 194 countries that had establish or processing the legislation of the protection of personal data and privacy.¹²

The state's partiality in regulating personal data protection brought obstacles to the process of transaction activities through electronic commerce globally. These obstacles are becoming trade barriers which cause most electronic commerce companies struggle in the area of digital trade. Diverse and fragmented approaches to personal data protection created by states create significant

¹⁰ Liming Liu and Yiming Chen, A Triple-Layered Comparative Approach to Understanding New Privacy Policy Practices of Digital Platforms and Users in China After Implementation of the PIPL, *Social Media + Society*, No. 111, 2024, p. 1–14, <https://doi.org/10.1177/20563051241301265>.

¹¹ Cedric Ryngaert and Mistale Taylor, The GDPR as Global Data Protection Regulation?, *AJIL Unbound* 114, 2020, p. 5–9, <https://doi.org/10.1017/aju.2019.80>.

¹² UNCTAD, Data and Privacy Unprotected in One Third of Countries, Despite Progress, <https://unctad.org/news/data-and-privacy-unprotected-one-third-countries-despite-progress>, 2020.

challenges for digital trade especially in cross-border electronic commerce.¹³ This impacted the practices of digital trade particularly towards electronic commerce as it intensifies the compliance complexity of business where the companies shall comply with various domestic laws that would increase their legal and operational costs as it should adjust with fragmented focus or requirements of states.¹⁴ Various domestic laws that apply such as the PIPL which requires domestic data localization would also lead to limited service offerings and also the increase of legal risk such as the GDPR that has extraterritorial power that will cause companies to face liabilities even outside the region. Non-compliance to the regulations would lead into restrictions to market access which later understood as a barrier to the practice of digital trade of electronic commerce.

While electronic commerce companies rely on cross border data flows for payments, logistics, and customer analytics the diverse and fragmented rules limit the companies to be able to scale globally because of such adjustments to navigate various patchworks of data laws. A survey conducted by Greenleaf over 145 national privacy laws also showed that there is a global trend toward regulating personal data protection but it is deep in legal fragmentation also there is divergence in standards and enforcement.¹⁵ Some recognition by international trade institutions also stated that diverse and fragmented data regulations become a barrier to digital trade, the Organisation for Economic Cooperation and Development (OECD) confirmed that regulatory diversity in personal data protection is a top trade concern that affects digital trade growth.¹⁶ UNCTAD also explained that national and regional data governance regimes such as the GDPR, CCPA, and PIPL complicate the digital trade practices especially in electronic commerce and increase the risk of data divide between states.¹⁷ Cooper and Kuner concluded that these data

¹³ Paul M. Schwartz and Anupam Chander, Resolving the Conflict Between Trade and Data Protection Law, *European Data Protection Law Review*, Vol. 9, No. 3, 2023, p. 296-304, <https://doi.org/https://doi.org/10.21552/edpl/2023/3/6>.

¹⁴ Zerui Zhao, The Dilemma of Cross-Border Data Flow and the Construction of Mutual Trust Platform in Asia, *Asian Journal of Law and Society*, Vol. 11, No. 4, 2024, p. 488-506, <https://doi.org/10.1017/als.2024.31>.

¹⁵ Graham Greenleaf, *Global Data Privacy Laws 2021: Despite COVID Delays, 145 Laws Show GDPR Dominance*, *Privacy Laws & Business International Report* 169, No. 1, 2021, p. 3-5, <https://doi.org/https://doi.org/10.2139/ssrn.3836348>.

¹⁶ Francesca Casalini and Javier López González, *Trade and Cross-Border Data Flows*, 2019.

¹⁷ UNCTAD, *Cross-Border Data Flows and Development: For Whom the Data Flow*, 2021.

protection regimes function as non-tariff trade barriers that also undermining market access in the digital economy.¹⁸ Partiality of states in governing the personal data protection issue with diverse focus and priorities are the main legal tension which urge the creation of a harmonization of universal common standard.¹⁹

Harmonization itself has been proved as a success in creating clarity, as happened through the creation of the United Nations Convention on Contracts for the International Sale of Goods (CISG) that harmonized the laws of sale of goods, driven by the need to simplify and unify international trade laws caused by the diversity in domestic contract laws that were uncertain and inefficient for cross-border transactions.²⁰ Therefore, this paper aims to understand and examine further on how a unified and harmonized common standards on governing the issue of personal data protection would ease the digital trade barriers. Thus, this paper aims to explores the following research question: How the harmonization of state regulations on personal data protection would help to ease barriers on digital trade practices? In doing so, this paper aims to furnish comprehensive insights into viable solutions that the international community, through international organizations can adopt to mitigate the risk of personal data security issues. This paper examines the existing legal framework on personal data protection both at the national level and at the international level and how it creates barriers to the practise of digital trade through electronic commerce. Later this paper will also discuss on various pathways to harmonization and which is the most ideally applicable to the issue.

This paper applies juridical normative as the research method. Through this type of method, study and examination towards bibliographical data is performed including positive international laws, literatures, and experts' opinions related to the issue discussed. All of the primary legal source will be examined thoroughly, compared to another, and analyzed to understand and obtain any possible solutions.

¹⁸ Daniel Cooper and Christopher Kuner, *Data Protection Law and International Dispute Resolution*, *Recueil Des Cours de l'Academie de La Haye En Ligne*, Vol. 382, Brill, Nijhoff, 2017, https://doi.org/https://doi.org/10.1163/1875-8096_pplrdc_A9789004338302_01.

¹⁹ Maarja Saluste, *Cross-Border 'Data Adequacy' Frameworks under GATS Article VII : Aligning WTO Members 'Rights to Protect Personal Data with Their International Commitments*, *World Trade Review*, Vol. 23, 2025, p. 1–27, <https://doi.org/10.1017/S1474745625000047>.

²⁰ Troy Keily, *Harmonisation and The United Nations Convention on Contract For The International Sale of Goods*, *Nordic Journal of Commercial Law*, Vol. 1, 2003, p. 1–21.

The approaches used on this research are, statute approach which examines regulations associated with the issue, such as regulations under the legal framework, and the second approach is conceptual approach based on conceptual theories related with the discussed issue.²¹ The analysis of various legal frameworks ranging from international and domestic laws related to personal data protection supported on understanding of how it later created a trade barrier in digital trade practices. Several cases and examples ranging from various countries also portrayed to help dive into deeper understanding of trade barriers are affecting digital trade. Legal theories related to trade barriers and importance of harmonization strengthened the analysis and helped to obtain a more comprehensive explanation on how this issue shall be resolved Data sources obtained from the approaches later will be analyzed using the method of descriptive and qualitative analysis to provide a comprehensive understanding and the correlation of each variable and will guide to a proper conclusion of the issue.

Analysis

Digital Trade and Personal Data Protection

The existence of internet has supported the establishment of trade digitalization, where digital trade is covering various aspects ranging from pure exchange of digital assets until its subsets including electronic commerce which is a digitally enabled trade.²² In a very dynamic circumstances, digital trade has become a primary channel for digital trade practices that includes buying and selling goods or services through online platforms which connect sellers and buyers to be able to conduct a cross-border digital transactions.²³ Several major worldwide electronic commerce like Amazon, Alibaba, E-bay, Shopee, and Tokopedia have played its important role to contribute on economic growth and supported massive amount of Small and Medium Enterprises (SMEs) across the world.²⁴ Even though digital trade on the context of electronic commerce may brings many conveniences to society,

²¹ Peter Mahmud Marzuki, *Penelitian Hukum*, Kencana Prenada Media Group, Jakarta, 2011.

²² Wolfgang Alschner, *E-Commerce or Digital Trade? Why the Difference Should Matter To Trade Lawyers*, in *Handbook on Digital Trade*, ed. Edward Elgar, 2022, <https://ssrn.com/abstract=4321743>.

²³ IMF et al., *Handbook on Measuring Digital Trade*, United Nations, 2021.

²⁴ World Internet Conference, *Cross-Border E-Commerce Competitiveness Research Report*, 2024.

digital trade also has drawbacks where one of them is regarding security issues, especially regarding the protection of consumers personal data.

Burri explained that data has become an essential element to economic process where everything is centralized. Data becomes very valuable for companies to gather information about their customers, suppliers, and operations which will support them in the process of trade.²⁵ In addition to their commercial value, data are involved in the protection of personal privacy and human rights, shaping consensus on decision-making and maintaining important national security interests.²⁶ Data is an important variable of digital transaction process, it plays important role on the development of electronic commerce practices including: (i) users profiling and personalization to build a detailed customer personalization in order to be able to receive personalized product recommendation and promotion²⁷, (ii) to facilitate transaction processing through an accurate and secure ways of payment, billing or shipping, (iii) to help companies conduct forecast of demand and inventory levels which help them in managing their supply chain worldwide, (iv) to help companies analyze marketing strategies and targeting customers in a correct market, (v) to avoid any fraud and for security monitoring by detecting any suspicious behavior or transactions, (vi) to assist users with effective and efficient customer service supports in addressing struggles during transactions.²⁸

Collecting data has been conducted by platforms like Amazon, Tokopedia, and JD.Id to collect data such as reviews, browsing patterns, in order to understand its users preferences.²⁹ Alibaba even provide its top selling sellers with access to its users behavior data to adjust their personalized recommendation.³⁰ Based on this, international trade and the protection of personal data have a very close

²⁵ Mira Burri, The Impact of Digitalization on Global Trade Law, German Law Journal Vol. 24, No. 3, 2023, p. 551–73.

²⁶ Yik Chan Chin and Jingwu Zhao, Governing Cross-Border Data Flows: International Trade Agreements and Their Limits, Laws Vol. 11, No. 4, 2022, p. 1–22.

²⁷ Rahayu Damayanti and Zaldy Adrianto, Machine Learning for E-Commerce Fraud Detection, Jurnal Riset Akuntansi Dan Bisnis Airlangga, Vol. 8, No. 2, 2023, p. 1562–77, <https://doi.org/https://doi.org/10.20473/jraba.v8i2.48559>.

²⁸ Swapnil Patil, Vikesh Dudhankar, and Pradyumna Shukla, Securing Digital Transactions: The Role of Identity Verification in Reducing E-Commerce Fraud, Journal of Artificial Intelligence Research, Vol. 3, No. 1, 2023, p. 358–85.

²⁹ Siti Asiyah, Tokopedia E-Commerce Retail Business Innovation in the Transformation Retail Industrial Era 4.0, Widya Cipta: Jurnal Sekretari Dan Manajemen, Vol. 7, No. 2, 2023, p. 145–50, <https://doi.org/10.31294/widyacipta.v7i2.16141>.

³⁰ Erica Pandey, Up for Grabs: Alibaba's Secret Sauce for Winning Chinese Retail, Axios, 2018, <https://www.axios.com/2018/10/16/alibaba-china-consumer-data-ecommerce>.

relationship, where in cross-border digital trade, it is important to collect data of its worldwide users yet it is also necessary to protect personal data which is used to ensure that unwanted things do not occur, such as data leaks or other cases.

Coupled with many cases of fraud or data leakage caused by a lack of security regarding consumer personal data. Where then, the data can be used to identify the person, namely the owner of the data. One example of a data leak case resulting from a lack of personal data protection in digital trade is the data leakage on Lazada, an international trading application based in Singapore. Where as many as 1.1 million user data of Lazada's online supermarket, namely RedMart, were reported to have been hacked in 2020.³¹ Following on the same year, it was reported that 91 million Tokopedia user data was allegedly leaked too.³² This led into global concern regarding the importance of personal data protection particularly in digital trade through electronic commerce platforms as the users retreating from online transactions worrying of their privacy, starting to lose trust with the electronic commerce companies. States began to establish their personalized regulation regarding personal data protection. The arrangements regarding the protection of privacy and personal data above have been regulated in several countries in the world without the exception of Indonesia's UU PDP.

Protection of privacy and personal data greatly influences economic development in a country. This protection is one of the determining factors for trust in online transactions, which is an important element in digital transactions. Personal data itself could be considered as the DNA of a person, and because of it this matter is a subject to human rights.³³ To realize establishment which properly starts with a general law regarding it.³⁴ Indonesia's UU PDP defines the personal data as individuals' data who are identified or combined with other information, through the electronic or non-electronic systems, both directly or indirectly.

³¹ Tubagus Muhammad Ali Ridho Azhari and Maria Grasia Sari Soetopo, Protection of Personal Data in Transactions Using ECommerce in the Perspective of Indonesian Law (An Overview), *International Journal of Research and Innovation in Social Science* Vol. 6, No. 12, 2022, p. 370–75.

³² Edy Santoso, Opportunities and Challenges: E-Commerce in Indonesia from a Legal Perspective, *Jurnal Penelitian Hukum De Jure* Vol. 22, No. 3, 2022, p. 395.

³³ Itzayana Tlacuilo Fuentes, Legal Recognition of The Digital Trade in Personal Data, *Mexican Law Review* Vol. 12, No. 2, 2020, p. 87–117.

³⁴ Azharuddin, Legal Protection for Users of Internet Banking Customers Following Changes in Information and Electronic Transaction Law, *Jurnal Pembaharuan Hukum* Vol. 6, No. 1, 2019.

Meanwhile, protection of personal data is the overall effort to protect personal data in every process particularly in digital trade activities that evolve it. In this case, personal data becomes an important matter for users, because users will not carry out digital trading without certainty in the security of the data.

Other arrangements regarding personal data protection can be seen in The European Union Charter of Fundamental Rights which explains the recognition of personal data protection and privacy as basic rights.³⁵ This is made to be a step to strengthen the fulfilment of the basic rights of European Union people in the digital era and can directly impact the impetus for business development in the digital era. The European Union itself has had The European Union Data Privacy Directive in 1995 which is a form of harmonization of national regulations regarding the protection of personal data among European Union countries. In addition, Hong Kong also has the Personal Data Privacy Ordinance of 1995 and Singapore which is The Personal Data Protection Act No. 26 of 2012. Driven by the urgency to ensure the protection of personal data in its territories, states were paying more attention to the legislation of personal data protection legal frameworks. However, with diverse and fragmented approach conducted by each state unfortunately also lead into another issue on how those legal frameworks affecting the practices of digital trade through electronic commerce platforms as a barrier.

Personal Data Protection Legal Frameworks as Trade Barriers

With advances in technology and globalization, the capacity of businesses to collect, store, and exchange digitized data from any location around the world is getting stronger and bigger.³⁶ In relation to electronic commerce, the personal data are in the form of consumer identity such as names, passwords, debit and credit card numbers, conversations in email, as well as information related to consumer requests and browsing activities.³⁷ Consumers submit their personal data to obtain services, on the other side organizations need personal data to carry out their

³⁵ Sinta Dewi Rosadi and Garry Gumelar Pratama, Urgensi Perlindungan Data Privasi dalam Era Ekonomi Digital Di Indonesia, *Veritas et Justitia* Vol. 4, No. 1, 2018, p. 88-110.

³⁶ Gabriella Beaumont-smith, Digital Trade Brings the World to Your Fingertips, *Cato Policy Analysis*, 2024.

³⁷ Rahmi Ayunda, Personal Data Protection to E-Commerce Consumer: What Are the Legal Challenges and Certainties?, *Law Reform* Vol. 18, No. 2, 2022, p. 144-163.

business.³⁸ This shows that information privacy has become a more critical issue to be considered. If consumer data falls into the wrong hands, consumers could face the risk of identity theft, misuse of personal information, or other cyberattacks³⁹ as has been discussed on section above.

Speaking of protection of personal data is inseparable of it being a part of human rights. Article 12 of the Universal Declaration of Human Rights (UDHR) mandated that individual has the right to have legal protection without intrusion into his/her privacy, family, place of living, and correspondence or honor and reputation have not included personal data as the instance that necessarily need to be protected. In this modern age, the interpretaion of privacy have extended including the protection of personal data, as digital technologies development become challenges to privacy issues.⁴⁰ As part of human rights then it is a legal consequences for states as the main actor to guarantee the protection of personal data, therefore, the establishment of domestic laws related to personal data protection is a form of state's responsibility to protect the privacy of its people.

States started to create its own domestic law, with its own consideration and main focus causing diverse fragmentations and approaches of legal frameworks related to personal data protection. Many countries such as Brazil's Lei Geral de Proteção de Dados (LGPD), European Union's General Data Protection Regulation 2016/679 (GDPR), China's Personal Information Protection Law (PIPL), Singapore's Personal Data Protection Act No. 26 of 2012 (PDPA), and Indonesia's Undang-Undang Nomor 26 Tahun 2022 Tentang Perlindungan Data Pribadi (UU PDP) govern their own personal data regulations and they are likewise provided in detail.

The EU's GDPR focuses on comprehensive personal data protection with individual rights and organizational accountability approaches. As it also has characteristics that not every state has which applies extraterritorial jurisdiction that would be able to cover entities outside the teritorry of the EU.⁴¹ The main

³⁸ Norjihhan Abdul Ghani and Zailani Mohamed Sidek, Personal Information Privacy Protection in E-Commerce, WSEAS Transactions on Information Science and Applications Vol. 6, No. 3, 2009, p. 407-16.

³⁹ Wiwik Sri Widiarty and Aartje Tehupeiory, THE ROLE OF BUSINESS LAW IN IMPROVING CONSUMER PROTECTION IN THE DIGITAL AGE, Journal of Law and Sustainable Development Vol. 12, No. 2, 2024, p. 1-12.

⁴⁰ Lorna Woods, *The Right to Privacy*, Routledge, United Kingdom, 2018).

⁴¹ Oskar Josef Gstrein and Andrej Janko Zwitter, Extraterritorial Application of the Gdpr: Promoting European Values or Power?, Internet Policy Review, Vol. 10, No. 3, 2021, <https://doi.org/10.14763/2021.3.1576>.

regulation of GDPR includes the requirement of explicit consent for processing data and it mandates the Data Protection Impact Assessments or the DPIAs also the sanctions for non-compliance in the form of penalties.⁴² While it has a strong normative regulation as it has influenced other states to have similar regulation, the GDPR creates a higher possibility of trade barrier especially to electronic commerce companies which operating in multiple countries.⁴³ The extraterritorial jurisdiction of GDPR creates de facto trade barriers in digital markets, it triggered foreign businesses that collect personal data from the EU residents with some consequences. Therefore, this caused several major news and media websites from the US such as the Los Angeles Times and New York Daily News in May 2018 decided to block access to their users from the region of the EU.⁴⁴ Thinking that refraining themselves from complying to the GDPR and withdrawing to the market is a better decision and would benefit them more.

While China's PIPL has different approach in regulating personal data protection. It emphasized on state's sovereignty and control over data. It required data localization domestically for certain types of data and mandated access to the government to the data processed by electronic commerce companies upon their request, this later called as data sovereignty act and become a non-tariff barrier to digital trade. Many foreign electronic commerce companies outside China were discouraged to enter China's digital market and it affected the global supply chains.⁴⁵ Domestic electronic commerce companies also face the same hurdles, such as Alibaba that must comply with the PIPL, strong intervention of the government to the business operations is another form of trade barrier faced by the companies.⁴⁶

⁴² Abdulah M. Aseri, The Implication of the European Union's General Data Protection Regulation (GDPR) on the Global Data Privacy, *Journal of Theoretical and Applied Information Technology* Vol. 98, No. 4, 2020, p. 692–702.

⁴³ Hannes Berggren, The GDPR and International Trade. *Kommerskollegium National Board of Trade Sweden*, 2025, <https://doi.org/10.1017/aju.2019.78>.

⁴⁴ Neil Thurman et al., Forbidden Fruit or Soured Grapes? Long-Term Effects of the Temporary Unavailability and Rationing of US News Websites on Their Consumption from the European Union, *International Communication Gazette* Vol. 84, No. 7–8, 2022, p. 698–720, <https://doi.org/10.1177/1748048522111312>.

⁴⁵ Wenlong Li and Jiahong Chen, From Brussels Effect to Gravity Assists: Understanding the Evolution of the GDPR-Inspired Personal Information Protection Law in China, *Computer Law and Security Review* Vol. 54, 2024, <https://doi.org/10.1016/j.clsr.2024.105994>.

⁴⁶ Danni Zhang, Understanding the Evolution of China's Approach to Digital Trade: Interests, Ideas, and Institutions, *Asian Review of Political Economy* Vol. 3, No. 1, 2024, <https://doi.org/10.1007/s44216-024-00026-4>.

Singapore’s PDPA has a more business friendly approach where it balances data protection and business needs, it governs the consent requirement for data collection and processing, also providing guidelines to data retention and transfer.⁴⁷ It also establishes a special commission called the Personal Data Protection Commision. Brazil’s LGPD focuses more on individual rights on the protection of personal data, the special characteristic of this regulation is that it mandates data protection officers for related organizations including the electronic commerce companies, this would contribute on the increase of business operation costs.⁴⁸ Lastly, Indonesia’s UU PDP with its focus on the protection of personal data both in public and private sectors, regulates data access, correction, deletion, and strict administration and criminal sanctions.⁴⁹ Key gaps on those regulations could be summarized into this table below:

Table 1. Key Gaps on Personal Data Protection Legal Frameworks

Regulation	Main Focus	Government Involvement	Cross-border Data Transfer
GDPR	Rights-centered, specific on lawful bases such as consent, legal obligation, etc.	Strong enforcement, cooperation between EU states by independent authorities in each state	Restrictive, requires standard contractual clauses
PIPL	Similar as GDPR with additional state access, focuses on national security and public interest	Strong state control, centralized enforcement, Cyberspace Administration of China (CAC)	Highly restrictive, sensitive data must be localized
PDPA	Business-friendly framework, consent-driven regulations	Advisory and enforcement roles, Personal Data Protection Commission (PDPC)	Allowed with reasonable data protection assurance
LGPD	Based on GDPR model, focuses on consent and transparency	Evolving authority which is the National Data Protection Authority (ANPD)	Same standard as GDPR
UU PDP	User consent as primary legal basis, requires domestic data localization	To be established on 2025	Allowed with subject consent

Source: compiled by authors

⁴⁷ Kah Leng Ter, Singapore’s Personal Data Protection Legislation: Business Perspective, *Computer Law and Security Review*, Vol. 29, No. 3, 2013, p. 264–73, <https://doi.org/https://doi.org/10.1016/j.clsr.2013.03.007>.

⁴⁸ Mohsin Ali Farhad, Consumer Data Protection Laws and Their Impact on Business Models in the Tech Industry, *Telecommunications Policy*, Vol. 48, No. 9, 2024, <https://doi.org/https://doi.org/10.1016/j.telpol.2024.102836>.

⁴⁹ Nofie Iman, The Fight for Our Personal Data: Analyzing the Economics of Data and Privacy on Digital Platforms, *International Journal of Law and Management*, Vol. 66, No. 6, 2024, p. 774–91, <https://doi.org/https://doi.org/10.1108/IJLMA-12-2022-0258>.

The GDPR and LGPD focuses on rights and offer more flexibility while PDPA and UU PDP heavily emphasize on consent, and China with the strictest regulation with government involvement. It is understandable that these gaps exist based on the differences on legal, cultural, political, and economic situation and interest in each state. Thus, fragmented legal frameworks also caused diverse obligations, rights, enforcement, and state involvement, that would be challenging to electronic commerce companies. The barrier on digital trade is escalated by the obligation to adjust with various regulations with different treatments and approach that might affect the business core of each company. The divergence of regulations leads into operational complexity which increase compliance costs and legal uncertainty. GDPR and PIPL impose strict regulations on data transfer and data localization while PDPA adopts a more business-friendly framework.

While domestic regulations on personal data protection play an essential role to safeguarding individual privacy, however these measures can also be perceived as non-tariff barriers, particularly under the World Trade Organization (WTO) legal framework, when cross-border data flows is restricted and additional compliance burdens are imposed towards foreign business.⁵⁰ From the perspective of the WTO law, a non-tariff barrier refers to any measure other than a tariff that restricts international trade which include domestic laws, regulations, technical standards, or licensing requirements that create obstacles for foreign business actors.⁵¹ According to this, such regulations may conflict with core principles of international trade which also shall be applied to digital trade, including principles of market access, national treatment, and transparency.⁵²

Data localization requirements, cross-border data transfer restrictions, and government access mandates embedded in personal data protection laws can function as de facto trade barriers by increasing the cost of doing business and limiting access to digital markets. When a data protection regulation imposes data

⁵⁰ Magdalena Słok-Wódkowska and Joanna Mazur, *Between Commodification and Data Protection: Regulatory Models Governing Cross-Border Information Transfers in Regional Trade Agreements*, *Leiden Journal of International Law*, Vol. 37 No. 1, 2024, p. 111–138.

⁵¹ Peter Van den Bossche and Werner Zdouc, *Non-Tariff Barriers*, in *The Law and Policy of the World Trade Organization*, Cambridge University Press, 2017, p.478–543.

⁵² World Trade Organization, *Principles of the Trading System*, n.d., https://www.wto.org/english/thewto_e/whatis_e/tif_e/fact2_e.htm.

localization only on foreign companies or restricts the transfer of data out of the country, it may violate the market access (Art. XVI General Agreement on Trade in Services/GATS) or national treatment (Art. XVII GATS) obligations, unless it falls under a justified exception.⁵³ In this light, some provisions of GDPR or PIPL, such as extraterritorial application or broad data localization mandates, are potentially challengeable under WTO rules if they unduly hinder foreign access without sufficient justification or transparency. Consequently, while personal data protection serves a vital public policy goal, its design and implementation need to strike a balance between protecting privacy and avoiding unnecessary trade restrictions. Failure to do so risks transforming legitimate regulation into protectionist tools that distort international digital trade, thereby undermining the principles of free and fair trade upheld by the WTO framework.

Besides the GATS framework, domestic personal data protection measures may also fall under the scope of the WTO Agreement on Technical Barriers to Trade (TBT Agreement), particularly when such measures take the form of technical regulations, standards, or conformity assessment procedures that affect trade in goods. Many aspects of personal data protection laws can fall within the scope of the TBT Agreement, particularly when they impose requirements on goods that collect, store, or transmit data. Under the TBT Agreement, it is mandated to ensure non-discrimination between imported and domestic products (Art. 2.1), it requires that technical regulations not create unnecessary obstacles to trade and be no more trade-restrictive than necessary to fulfill a legitimate objective, such as protecting privacy (Art. 2.2), and encourages the use of international standards (Art 2.4).⁵⁴

Failure to adopt or align with globally accepted frameworks (such as ISO/IEC 27701 or OECD Privacy Guidelines) may expose a country to WTO scrutiny. For example, mandatory data localization provisions or government access requirements, as seen in China's PIPL, may exceed what is necessary to protect privacy and function instead as disguised trade barriers. Likewise, compliance

⁵³ Eugene Tseng, Data Localization: The Compatibility with GATS and Its Outlook, *Michigan Journal of International Law*, Vol. 43, 2021, p.5–6.

⁵⁴ Mira Burri, Interfacing Privacy and Trade, *Case Western Reserve Journal of International Law*, Vol. 53 No. 1, 2021, p.35–71.

burdens under the GDPR's extraterritorial application may disadvantage exporters of data-intensive goods from non-EU countries. While protecting privacy is a legitimate policy objective, WTO members must design personal data regulations that are transparent, non-discriminatory, and no more trade-restrictive than necessary to balance privacy rights and free trade principles according to international economic law. Encouraging regulatory cooperation and convergence through mutual recognition agreements or global data protection standards may help reduce friction and strengthen trust in cross-border digital trade.

Various standards, definitions, and severity of penalties are inconsistencies that force companies to adjust and adapt their data processing practices with specific infrastructures and legal frameworks. This results on substantial barriers such as delayed market access, increase on operational costs, and limited mobility to scale globally. The absence of harmonization in data protection regulations disrupts the digital trade and is needed, but a unified or harmonized legal framework would reduce risk or non-compliance and the legal certainty would help the companies to settle better in managing the operations. Harmonized laws would also boost users' trust on a cross-border transaction, as the standard to the data protection is established, it would also put the users at ease knowing that their data is secured in regardless jurisdiction it is processed.

The Need of Harmonization and the Creation of Common Standard

Law has the characteristic to predict and facilitate various technological and information developments to maintain society order.⁵⁵ The legal challenges associated with consumer protection have become a growing concern, particularly when consumers engage in electronic commerce transactions with merchants across multiple countries. Such fraudulent activities can involve various aspects, including the legitimacy of business entities, the quality of purchased goods, issues related to laws and regulations, pricing discrepancies, consumer payments, and safeguarding personal data.⁵⁶ According to data released by the Indonesian

⁵⁵ I Gede Agus Kurniawan, Digitalization of Business Law : Urgency and Orientation of the Industrial, *Volkgeist* Vol. V, No. 40, 2022, p. 253–65.

⁵⁶ Rahmi Ayunda, *supra* note 26.

Consumer Foundation (YLKI), online shopping is among the top five sectors that are most frequently reported by consumers. The first place is still occupied by the banking sector, followed by online loans or fintech in the second place. Housing ranks third, online shopping is fourth, and leasing is fifth. To reduce the potential misuse of personal data then strong yet strict regulation is needed for the benefit of both consumers and businesses.

However, it creates another challenge on how it would affect the practices of electronic commerce itself, when accessibility and operating in digital market is becoming a hurdle to the companies. While speaking of ensuring personal data protection is a part of rights that must be guaranteed, it is also important to ensure that the businesses' needs and interests are covered too in performing their activities. As the existence of electronic commerce is much needed, it is also important to provide the companies with certainty and sustainability without ruling out the essence of personal data protection. Current existing international instruments related to electronic commerce

Electronic commerce transcends national borders, enabling businesses to operate and consumers to engage in transactions worldwide. In the absence of common standards, there is a lack of consistency and harmonization in protecting personal data across different jurisdictions. In e-commerce, personal data is frequently transferred across borders. However, the absence of common standards results in a lack of clarity and consistency in governing these data transfers. This situation can lead to conflicting regulations and insufficient protection measures. Implementing common standards would enable smooth cross-border data flows while prioritizing the privacy and security of personal data.

Currently, there are some existing regulations in the international level that govern matters related to personal data protection, although a fully universal law does not exist yet. There are several treaties, guidelines, and regional laws that contribute on the shaping of global data protection while most of them are influential enough to become a model law. Some of the regulations include the OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data established on 1980 and was updated on 2013. It is a non-binding regulation but has

global influence that inspired many national laws on data protection. Some of the key points regulated under the guidelines are principles such as purpose limitation, data quality, security safeguards and individual participation.⁵⁷

There is also Asia-Pacific Economic Cooperation (APEC) Privacy Framework that applies regionally to the members of the organization and mainly governs on cross-border data flow, accountability, and consumer protection.⁵⁸ Both the OECD's Guidelines and the APEC Privacy Framework have actually designed with harmonization purposes including in the context of digital trade and electronic commerce.⁵⁹ The principle of trans-border data flow that is found under the OECD Guidelines, which affirms that data transfers should not be restricted accross borders if the destination country offers adequate protection is one of preliminary steps of harmonization in data protection in digital trade. Even the APEC Privacy Framework has clear focus on electronic commerce with its main goal to maintain data protection balanced with unhindered data flow and provide a system called the Cross-Border Privacy Rules (CBPR) System that would help companies of electronic commerece with data protection standards. It also has been collaborating with the EU to align the CBPR and GDPR system, a proof of another step of harmonization.⁶⁰

Various initiatives at the international level have attempted to address legal uncertainty in digital trade, particularly through trade agreements. One such initiative is the WTO Work Programme on Electronic Commerce, which since 1998 has introduced a moratorium on customs duties for electronic transmissions. This moratorium, extended most recently in 2024, is a significant step toward maintaining a free flow of digital goods and services. However, it only covers tariff-based restrictions and does not address regulatory barriers such as data localization, divergent privacy requirements, or cross-border transfer prohibitions,

⁵⁷ Zhurabaev Bekzod and Latifjon Ugli, *Regulating E-Commerce: International Legal Perspectives and Challenges*, International Journal of Cyber Law, Vol. 1, No. 6, 2023, p. 1–13.

⁵⁸ Jamael Jacob, *APEC 's Cross Border Data Transfer Rules : An Unfulfilled Potential , An Uncertain Future*, DTA Alliance, 2023.

⁵⁹ Tobias Naef, *Data Protection without Data Protectionism*, in *European Yearbook of International Economic Law* Springer, 2023, p. 367–420, <https://link.springer.com/content/pdf/10.1007/978-3-031-19893-9.pdf?pdf=button>.

⁶⁰ Rowena Rodrigues and Vagelis Papakonstantinou, *Privacy and Data Protection Seals*, T.M.C. Asser Press The Hague, 2018, <https://link.springer.com/book/10.1007/978-94-6265-228-6>.

which can function as non-tariff barriers in practice.⁶¹ On the other hand, regional trade agreements like the Comprehensive and Progressive Agreement for Trans-Pacific Partnership (CPTPP) have taken a more comprehensive approach. Chapter 14 of the CPTPP explicitly requires members to allow cross-border data flows and to avoid forced data localization, while still permitting personal data protection as long as it is not used as a disguised restriction on trade. Despite this, the lack of uniform enforcement mechanisms and the discretionary nature of its privacy provisions continue to permit fragmentation across jurisdictions.⁶²

However, the harmonization of global framework for personal data protection in electronic commerce practices still does not exist yet as current existing international instruments only promote partial harmonization. Although complete harmonization would be very vague to achieve, a greater harmonization is still needed to answer challenges occurred in the development of personal data protection in the context of electronic commerce. The absence of a common standard in personal data protection in electronic commerce will also affect consumer confidence and trust in electronic commerce. When consumers have confidence that their personal information is being effectively protected, they are more inclined to participate in online transactions and willingly share their data with businesses.⁶³ Considering the need to establish common standards for the protection of personal data in e-commerce, it is imperative for countries around the world to promptly agree on the formation of such common standards. The impact of these standards would not only benefit consumers but also greatly benefit all electronic commerce businesses.⁶⁴

Establishing a common standard lead, us into the understanding of creating a standarization of law on certain issue which in this discussion is on the issue of personal data protection and digital trade. The aim of standarization is to minimize

⁶¹ Neha Mishra, Privacy, Cybersecurity, and GATS Article XIV: A New Frontier for Trade and Internet Regulation? *World Trade Review*, Vol. 19 No. 3, 2020, p.341–64.

⁶² Stephanie Honey, Modernizing the CPTPP's e-Commerce Chapter, *Hinrich Foundation*, 2025, <https://www.hinrichfoundation.com/research/article/ftas/modernizing-the-cptpp-e-commerce-chapter/>.

⁶³ Zlatan Morić et al., Protection of Personal Data in the Context of E-Commerce, *Journal of Cybersecurity and Privacy*, Vol. 4, No. 3, 2024, p. 731–61, <https://doi.org/10.3390/jcp4030034>.

⁶⁴ Panagiotis Delimatsis, *International Trade Law and Technical Standardization*, J. Contreras (Ed.), *The Cambridge Handbook of Technical Standardization Law: Further Intersections of Public and Private Law*, Cambridge University Press (CUP), United Kingdom, 2019.

deviations from the standards and later on it will be harmonized across states jurisdictions by providing opportunities to state to receipt and adopt these standards and transform it into their domestic law.⁶⁵ The creation of standards is an important vehicle for the practice of international trade, however different standards apply in different countries may serve as trade barriers. Trade barriers caused by differences in standards tend to be higher than traditional tariff barriers thus it is important to harmonize the standards.⁶⁶ Therefore, international common standards on international trade is becoming essential for countries to harmonize their standards and rely whenever possible on international standards as a basis for domestic policies.⁶⁷ International standard, is a norm for market-based activity and has two essential attributes: prescribed or recommended by an institution set up for that purpose and the institution must be international in the sense that it involves participation from more than two states.⁶⁸ Therefore, international coordination is needed to create an integration of legal and policy on digital trade.⁶⁹

To address these challenges, it can be resolved through the comparative method as proposed by Schmitthoff, which recognizes three methods, (1) international conventions/agreements (this involves the establishment of international agreements or conventions that govern the protection of personal data in e-commerce), (2) uniform laws (this method entails the adoption of uniform laws that are applied consistently across multiple countries to regulate the protection of personal data in electronic commerce), (3) uniform rules (this method involves the implementation of uniform rules that provide standardized guidelines for the protection of personal data in electronic commerce). By employing these comparative methods, the challenges related to unification and harmonization can be addressed effectively. It is necessary right now to establish a legislation that will

⁶⁵ Katharina Pistor, *The Standardization of Law and Its Effect on Developing Economies*, G-24 Discussion Paper Series, New York, 2000.

⁶⁶ Yasushi Kawabata and Yasuhiro Takarada, *Deep Trade Agreements and Harmonization of Standards*, *Southern Economic Journal* Vol. 88, No. 1, 2021, p. 118–143.

⁶⁷ Cary Coglianese, *Standards and the Law*, *Standardization: Journal of Research and Innovation* Vol. 2, No. 2, 2023, p. 15–20.

⁶⁸ Steve Charnovitz, *International Standards and the WTO*, *SSRN Electronic Journal*, 2005.

⁶⁹ Neha Mishra and Ana Maria Palacio Valencia, *Digital Services and Digital Trade in the Asia Pacific: An Alternative Model for Digital Integration?*, *Asia Pacific Law Review* Vol. 31, No. 2, 2023, p. 489–513.

regulates all digital changes particularly towards trade which put uniformity between countries as the main consideration.⁷⁰

In relation to the method explained above, the establishment of common standards for the protection of personal data in electronic commerce is carried out using the second method, namely uniform laws. The operationalization of this method is achieved by creating a model law, which contains recommended legal provisions to be adopted into the national laws of a country. This allows countries to adapt the rules to their specific conditions while maintaining the common standards applicable across any country. The flexible nature of model laws makes them easier to negotiate compared to conventions, as their text can be modified, and they have the potential to be more readily accepted or agreed upon by countries.⁷¹

The Model Law proposed is intended to be a soft law to standardize the concept and regulation of personal data protection. Soft law itself is a form of agreement in international law which is not legally binding.⁷² Soft law could play the role and act as a means of coordinating norms or policy in the context of international law.⁷³ It is been proved that soft law is more effective to hard law, it is measured as continuity of active participation and involvement instead of agreement accession or ratification.⁷⁴ Soft law has been applied for quite a long time in international trade, for example UNCITRAL Model Law on Electronic Commerce issued in 1996. This Model Law issued by UNCITRAL has become a minimum standard regarding electronic commerce arrangements. This can be emulated to form a new Model Law on Personal Data Protection. Since soft law is not legally binding, therefore, the process of forming and enacting the Model Law can be carried out in a relatively short time.

⁷⁰ Ricardo Francisco Reier Forradellas and Luis Miguel Garay Gallastegui, *Digital Transformation and Artificial Intelligence Applied to Business: Legal Regulations, Economic Impact and Perspective*, Laws Vol. 10, No. 3, 2021.

⁷¹ Subianta Mandala, *Harmonisasi Hukum Perdagangan Internasional: Sejarah, Latar Belakang Dan Model Pendekatannya*, Jurnal Bina Mulia Hukum Vol. 1, No. 1, 2016, p. 53–61.

⁷² Gita Venolita Valentina Gea, *Eksistensi UPICC Sebagai Instrumen Soft Law Dalam Praktik Perdagangan Internasional*, Jurnal Panorama Hukum Vol. 4, No. 1, 2020, p. 93–103.

⁷³ Stephen Daly, *The Rule of (Soft) Law*, King's Law Journal Vol. 32, No. 1, 2021, p. 3–13.

⁷⁴ Maximilian S.T. Wanner, *The Effectiveness of Soft Law in International Environmental Regimes: Participation and Compliance in the Hyogo Framework for Action*, International Environmental Agreements: Politics, Law and Economics Vol. 21, No. 1, 2021, p. 113–32.

The new Model Law on Personal Data Protection is ideally proposed to be established by the UNCITRAL, too. UNCITRAL has mandates, credibility, and past success with establishing model laws and it has the potential to align with existing regional frameworks such as GDPR, PIPL, or PDPA. UNCITRAL Model Law would provide legal certainty, trade facilitation, and capacity-building for developing countries.⁷⁵ Although the UNCITRAL Model Law would be in a form of soft law such as the OECD Guidelines and the APEC Privacy Framework, however, UNCITRAL Model Laws are designed to be able to transform into hard law through voluntary national adoption. While UNCITRAL Model Laws are not binding per se, their deliberate design for legislative adoption makes them uniquely positioned among soft law instruments to catalyze global legal harmonization, particularly in the context of cross-border electronic commerce and data governance. Matters that should be governed under the UNCITRAL Model Law on Personal Data Protection in E-Commerce shall include privacy principles such as transparency and purpose limitation, cross-border data transfer rules, business obligations and individual rights, also on dispute resolutions and enforcement mechanisms.

Another challenge on creating a harmonization on personal data protection standard is when it faces the sovereignty of states especially with powerful jurisdictions. However, soft law in a form of model law would not force the states to strictly comply with the regulation, but somehow may align or adjust the standards with their trade interests.⁷⁶ While state sovereignty presents a significant challenge to full legal harmonization, UNCITRAL's model law mechanism respects national autonomy by offering adaptable frameworks rather than binding obligations. This flexibility allows even strongly sovereign states, such as China, to engage in partial harmonization that supports their commercial interests. UNCITRAL's approach to model laws balances the goals of global harmonization with the reality of national sovereignty. While full legal convergence may be unattainable, a UNCITRAL Model

⁷⁵ Jenny Clift, Regional and Global Initiatives and Lessons: UNCITRAL Global Insolvency Standards, in *Global Insolvency and Bankruptcy Practice for Sustainable Economic Development*, ed. Tarek M. Hajjiri and Adrian Cohen, Palgrave Macmillan, London, 2016, p. 19–58, https://doi.org/https://doi.org/10.1057/9781137515759_2.

⁷⁶ Henry Deeb Gabriel, The Use of Soft Law in the Creation of Legal Norms in International Commercial Law: How Successful Has It Been?, *Michigan Journal of International Law*, Vol. 40, No. 3, 2019, p. 413, <https://doi.org/10.36642/mjil.40.3.use>.

Law on Personal Data Protection in E-Commerce offers a flexible blueprint for countries to align key principles, enable data flows, and build interoperability even without sacrificing regulatory autonomy.

The creation of a standard with harmonization purpose on personal data protection in electronic commerce, would help to eliminate digital trade barriers. Even in a legally pluralistic world, the strategic adoption of a UNCITRAL Model Law on Personal Data Protection in E-Commerce can substantially reduce regulatory fragmentation, promote legal interoperability, and unlock cross-border digital trade opportunities particularly for small and medium enterprises disproportionately affected by data localization and compliance burdens. The establishment of a harmonized model law such as that proposed by UNCITRAL empowers not only governments, but also electronic commerce actors, by giving them a clear legal standard to align with and advocate for. As digital trade becomes essential to national economies, states that impose excessive restrictions risk isolation both legally and commercially. In this context, a standardized model law functions as a bargaining tool, enabling companies to call for legal alignment in the name of interoperability, innovation, and mutual economic benefit. With an UNCITRAL Model Law on Personal Data Protection in E-Commerce, electronic commerce companies could request regulatory alignment or recognition and use the model law as a baseline for digital trade practices. Once a standard is set and widely accepted, it would encourage compliance and would create a better circumstance for all stakeholders in the digital trade development.

Conclusion

The significant development of digital trade particularly through electronic commerce undoubtedly brought pathways to new economic opportunities while also exposing critical vulnerabilities in personal data protection. Diverse regulations on national levels ranging from right-based approaches like the GDPR to sovereignty-focused models such as China's PIPL has created a fragmentation on legal frameworks that contributes to the complexity of cross-border transactions and compliance burdens on electronic commerce companies. These later acts as

non-tariff barriers with impacts such as market access limitation due to regulations, operational costs increasement, and uncertainty for legal aspects. Harmonization of personal data protection regulation at international level is essential to facilitate digital trade and protecting interest of all parties involved. While complete legal unification remains difficult but the establishment of a soft law in a form of UNCITRAL Model Law on Personal Data Protection in E-Commerce might be a viable solution. This model law would provide a flexible yet effective framework that can align with diverse legal systems without compromising regulatory autonomy, serve as catalyst to build trust among business actors and users, enhance legal certainty, reduce regulatory fragmentation, and enable a smoother implementation on personal data protection.

BIBLIOGRAPHY

Books:

- IMF, OECD, United Nations and WTO, Handbook on Measuring Digital Trade, United Nations, 2021.
- Jenny Clift, Regional and Global Initiatives and Lessons: UNCITRAL Global Insolvency Standards, in *Global Insolvency and Bankruptcy Practice for Sustainable Economic Development*, ed. Tarek M. Hajjiri and Adrian Cohen, London, Palgrave Macmillan, 2016.
- Lorna Woods, *The Right to Privacy*, United Kingdom, Routledge, 2018.
- Panagiotis Delimatsis, International Trade Law and Technical Standardization, J. Contreras (Ed.), *The Cambridge Handbook of Technical Standardization Law: Further Intersections of Public and Private Law*, United Kingdom, Cambridge University Press (CUP), 2019.
- Peter Mahmud Marzuki, *Penelitian Hukum*, Jakarta, Kencana Prenada Media Group, 2011.
- Peter Van den Bossche and Werner Zdouc, Non-Tariff Barriers, in *The Law and Policy of the World Trade Organization*, Cambridge University Press, 2017.
- Rowena Rodrigues and Vagelis Papakonstantinou, *Privacy and Data Protection Seals*, The Hague, T.M.C. Asser Press, 2018.
- Tobias Naef, Data Protection without Data Protectionism, in *European Yearbook of International Economic Law* Springer, 2023.
- Wolfgang Alschner, E-Commerce or Digital Trade? Why the Difference Should Matter To Trade Lawyers, in *Handbook on Digital Trade*, ed. Edward Elgar, 2022.

Journals:

- Abdulah M. Aseri, "The Implication of the European Union's General Data Protection Regulation (GDPR) on the Global Data Privacy", *Journal of Theoretical and Applied Information Technology* Vol. 98, No. 4, 2020.
- Alberto Oddenino, "Digital Standardization, Cybersecurity Issues and International Trade Law", *Questions of International Law*, Vol 51, No. 2018, 2021.
- Alvansa Vickya and Reshina Kusumadewi, "Kewajiban Data Controller Dan Data Processor Dalam DATA Breach Terkait Perlindungan Data Pribadi Berdasarkan Hukum Indonesia Dan Hukum Singapura: Studi Kasus Data Breach Tokopedia", *Padjajaran Law Review*, Vol. 9, No. 1, 2021.
- Azharuddin, "Legal Protection for Users of Internet Banking Customers Following Changes in Information and Electronic Transaction Law", *Jurnal Pembaharuan Hukum*, Vol. 6, No. 1, 2019.
- Cary Coglianese, "Standards and the Law, Standardization: Journal of Research and Innovation", Vol. 2, No. 2, 2023.
- Cedric Ryngaert and Mistale Taylor, "The GDPR as Global Data Protection Regulation?", *AJIL Unbound* 114, 2020.
- Daniel Cooper and Christopher Kuner, "Data Protection Law and International Dispute Resolution", *Recueil Des Cours de l'Academie de La Haye En Ligne*, Vol. 382, Brill, Nijhoff, 2017.
- Danni Zhang, "Understanding the Evolution of China's Approach to Digital Trade: Interests, Ideas, and Institutions", *Asian Review of Political Economy*, Vol. 3, No. 1, 2024.
- Dolores Añón Higón and Daniel Bonvin, "Digitalization and Trade Participation of SMEs", *Small Business Economics*, Vol. 62, No.3, 2024.
- Edy Santoso, "Opportunities and Challenges: E-Commerce in Indonesia from a Legal Perspective", *Jurnal Penelitian Hukum De Jure*, Vol. 22, No. 3, 2022.
- Eugene Tseng, "Data Localization: The Compatibility with GATS and Its Outlook", *Michigan Journal of International Law* Vol. 43, 2021.
- Gita Venolita Valentina Gea, "Eksistensi UPICC Sebagai Instrumen Soft Law Dalam Praktik Perdagangan Internasional", *Jurnal Panorama Hukum*, Vol. 4, No. 1, 2020.
- Henry Deeb Gabriel, "The Use of Soft Law in the Creation of Legal Norms in International Commercial Law: How Successful Has It Been?", *Michigan Journal of International Law*, Vol. 40, No. 3, 2019.
- I Gede Agus Kurniawan, "Digitalization of Business Law : Urgency and Orientation of the Industrial", *Volkgeist*, Vol. V, No. 40, 2022.
- Ikrom Ahmedov, "The Impact Of Digital Economy On International Trade, European Journal of Business and Management Research", Vol. 5, No. 4, 2020.
- Itzayana Tlacuilo Fuentes, "Legal Recognition of The Digital Trade in Personal Data, Mexican Law Review", Vol. 12, No. 2, 2020.
- Joseph Amankwah-Amoah et al., "COVID-19 and Digitalization: The Great Acceleration", *Journal of Business Research*, Vol. 136, July, 2021.
- Joshua P. Meltzer, "Cybersecurity, Digital Trade, and Data Flows: Re-Thinking a Role for International Trade Rules", *Global Economy & Development*, 2020.

- Kah Leng Ter, "Singapore's Personal Data Protection Legislation: Business Perspective", *Computer Law and Security Review*, Vol. 29, No. 3, 2013.
- Liming Liu and Yiming Chen, "A Triple-Layered Comparative Approach to Understanding New Privacy Policy Practices of Digital Platforms and Users in China After Implementation of the PIPL", *Social Media + Society*, No. 111, 2024.
- Maarja Saluste, "Cross-Border 'Data Adequacy' Frameworks under GATS Article VII: Aligning WTO Members' Rights to Protect Personal Data with Their International Commitments", *World Trade Review*, Vol. 23, 2025.
- Magdalena Słok-Wódkowska and Joanna Mazur, "Between Commodification and Data Protection: Regulatory Models Governing Cross-Border Information Transfers in Regional Trade Agreements", *Leiden Journal of International Law*, Vol. 37, No. 1, 2024.
- Maximilian S. T. Wanner, "The Effectiveness of Soft Law in International Environmental Regimes: Participation and Compliance in the Hyogo Framework for Action", *International Environmental Agreements: Politics, Law and Economics*, Vol. 21, No. 1, 2021.
- Mira Burri, "The Impact of Digitalization on Global Trade Law", *German Law Journal*, Vol. 24, No. 3, 2023.
- Mira Burri, "Interfacing Privacy and Trade", *Case Western Reserve of International Law Journal*, Vol. 53, No. 1, 2021.
- Mohsin Ali Farhad, "Consumer Data Protection Laws and Their Impact on Business Models in the Tech Industry", *Telecommunications Policy*, Vol. 48, No. 9, 2024.
- Neil Thurman et al., "Forbidden Fruit or Soured Grapes? Long-Term Effects of the Temporary Unavailability and Rationing of US News Websites on Their Consumption from the European Union", *International Communication Gazette*, Vol. 84, No. 7–8, 2022.
- Neha Mishra, "Privacy, Cybersecurity, and GATS Article XIV: A New Frontier for Trade and Internet Regulation?", *World Trade Review*, Vol. 19, No. 3, 2020.
- Neha Mishra and Ana Maria Palacio Valencia, "Digital Services and Digital Trade in the Asia Pacific: An Alternative Model for Digital Integration?", *Asia Pacific Law Review*, Vol. 31, No. 2, 2023.
- Nofie Iman, "The Fight for Our Personal Data: Analyzing the Economics of Data and Privacy on Digital Platforms", *International Journal of Law and Management*, Vol. 66, No. 6, 2024.
- Norjihan Abdul Ghani and Zailani Mohamed Sidek, "Personal Information Privacy Protection in E-Commerce", *WSEAS Transactions on Information Science and Applications*, Vol. 6, No. 3, 2009.
- Oskar Josef Gstrein and Andrej Janko Zwitter, "Extraterritorial Application of the Gdpr: Promoting European Values or Power?", *Internet Policy Review*, Vol. 10, No. 3, 2021.
- Paul M. Schwartz and Anupam Chander, "Resolving the Conflict Between Trade and Data Protection Law", *European Data Protection Law Review*, Vol. 9, No. 3, 2023.
- Rahayu Damayanti and Zaldy Adrianto, "Machine Learning for E-Commerce Fraud Detection", *Jurnal Riset Akuntansi Dan Bisnis Airlangga*, Vol. 8, No. 2, 2023.

- Rahmi Ayunda, "Personal Data Protection to E-Commerce Consumer: What Are the Legal Challenges and Certainties?", *Law Reform*, Vol. 18, No. 2, 2022.
- Rahmonov Jaloliddin, "Digitalization in Global Trade: Opportunities and Challenges for Investment", *Global Trade and Customs Journal*, Vol. 18, No. 10, 2023.
- Renuad Sorieau, Jennifer R. Clift, and Jose Angelo Estrella-Faria, "Establishing a Legal Framework for Electronic Commerce: The Work of the United Nations Commission on International Trade Law (UNCITRAL)", *International Lawyer*, Vol. 35, No. 1, 2001.
- Ricardo Francisco Reier Forradellas and Luis Miguel Garay Gallastegui, "Digital Transformation and Artificial Intelligence Applied to Business: Legal Regulations, Economic Impact and Perspective", *Laws*, Vol. 10, No. 3, 2021.
- Sinta Dewi Rosadi and Garry Gumelar Pratama, "Urgensi Perlindungan Data Privasi dalam Era Ekonomi Digital Di Indonesia", *Veritas et Justitia*, Vol. 4, No. 1, 2018.
- Siti Asiyah, "Tokopedia E-Commerce Retail Business Innovation in the Transformation Retail Industrial Era 4.0", *Widya Cipta: Jurnal Sekretari Dan Manajemen*, Vol. 7, No. 2, 2023.
- Stephen Daly, "The Rule of (Soft) Law", *King's Law Journal*, Vol. 32, No. 1, 2021.
- Steve Charnovitz, "International Standards and the WTO", *SSRN Electronic Journal*, 2005.
- Subianta Mandala, "Harmonisasi Hukum Perdagangan Internasional: Sejarah, Latar Belakang Dan Model Pendekatannya", *Jurnal Bina Mulia Hukum*, Vol. 1, No. 1, 2016.
- Swapnil Patil, Vikesh Dudhankar, and Pradyumna Shukla, "Securing Digital Transactions: The Role of Identity Verification in Reducing E-Commerce Fraud, *Journal of Artificial Intelligence Research*", Vol. 3, No. 1, 2023.
- Taufiq Adiyanto, "The Analysis of Indonesian Electronic Transaction Tax (ETT) Under WTO Law", *Law Development Journal*, Vol. 5, No. 225, 2023.
- Troy Keily, "Harmonisation and The United Nations Convention on Contract For The International Sale of Goods", *Nordic Journal of Commercial Law*, Vol. 1, 2003.
- Tubagus Muhammad Ali Ridho Azhari and Maria Grasia Sari Soetopo, "Protection of Personal Data in Transactions Using ECommerce in the Perspective of Indonesian Law (An Overview)", *International Journal of Research and Innovation in Social Science*, Vol. 6, No. 12, 2022.
- Wenlong Li and Jiahong Chen, "From Brussels Effect to Gravity Assists: Understanding the Evolution of the GDPR-Inspired Personal Information Protection Law in China", *Computer Law and Security Review*, Vol. 54, 2024.
- Wiwik Sri Widiarty and Aartje Tehupeiory, "The Role of Business Law on Improving Consumer Protection in the Digital Age", *Journal of Law and Sustainable Development*, Vol. 12, No. 2, 2024.
- Yasushi Kawabata and Yasuhiro Takarada, "Deep Trade Agreements and Harmonization of Standards", *Southern Economic Journal*, Vol. 88, No. 1, 2021.
- Yik Chan Chin and Jingwu Zhao, "Governing Cross-Border Data Flows: International Trade Agreements and Their Limits", *Laws*, Vol. 11, No. 4, 2022.
- Zerui Zhao, "The Dilemma of Cross-Border Data Flow and the Construction of Mutual Trust Platform in Asia", *Asian Journal of Law and Society*, Vol. 11, No. 4, 2024.

Zhurabaev Bekzod and Latifjon Ugli, "Regulating E-Commerce: International Legal Perspectives and Challenges", *International Journal of Cyber Law*, Vol. 1, No. 6, 2023.

Zlatan Morić, Vedran Dakic, Daniela Djekic, and Damir Regvart, "Protection of Personal Data in the Context of E-Commerce", *Journal of Cybersecurity and Privacy*, Vol. 4, No. 3, 2024.

Reports:

Francesca Casalini and Javier López González, "Trade and Cross-Border Data Flows", 2019.

Gabriella Beaumont-smith, "Digital Trade Brings the World to Your Fingertips", *Cato Policy Analysis*, 2024.

Graham Greenleaf, "Global Data Privacy Laws 2021: Despite COVID Delays, 145 Laws Show GDPR Dominance", *Privacy Laws & Business International Report* 169, No. 1, 2021.

Hannes Berggren, "The GDPR and International Trade", *Kommerskollegium National Board of Trade Sweden*, 2025.

Jamael Jacob, "APEC 's Cross Border Data Transfer Rules : An Unfulfilled Potential , An Uncertain Future", *DTA Alliance*, 2023.

Katharina Pistor, "The Standardization of Law and Its Effect on Developing Economies", *G-24 Discussion Paper Series*, New York, 2000.

UNCTAD, "Cross-Border Data Flows and Development: For Whom the Data Flow", 2021.

World Internet Conference, *Cross-Border E-Commerce Competitiveness Research Report*, 2024.

Websites:

Erica Pandey, "Up for Grabs: Alibaba's Secret Sauce for Winning Chinese Retail, Axios", 2018, <https://www.axios.com/2018/10/16/alibaba-china-consumer-data-ecommerce>.

Stephanie Honey, "Modernizing the CPTPP's E-Commerce Chapter", *Hinrich Foundation*, 2025, <https://www.hinrichfoundation.com/research/article/ftas/modernizing-the-cptpp-e-commerce-chapter/>.

UNCTAD, "Data and Privacy Unprotected in One Third of Countries, Despite Progress", 2020, <https://unctad.org/news/data-and-privacy-unprotected-one-third-countries-despite-progress>

World Trade Organization, "Principles of the Trading System", n.d., https://www.wto.org/english/thewto_e/whatis_e/tif_e/fact2_e.htm