Master's Thesis of International Studies

Towards a Global Privacy Protection Mechanism

- Balancing between the Cross-border Data Flows and Privacy Protection -

개인정보보호의 글로벌 메커니즘 모색
- 국경 간 데이터 이동과 개인정보보호의 균형을 중심으로 -

August 2023

Graduate School of International Studies
Seoul National University
International Commerce Major

Gun Young PARK

Towards a Global Privacy Protection Mechanism

- Balancing between the Cross-border Data Flows and Privacy Protection -

Examiner 이영섭

Submitting a master's thesis of
International Studies

August 2023

Graduate School of International Studies
Seoul National University
International Commerce Major

Gun Young PARK

Confirming the master's thesis written by
Gun Young PARK
August 2023

Chair	신성호	(Seal)
Vice Chair	유명희	(Seal)
Examiner	이영섭	(Seal)

Abstract

Data constitute a valuable resource for economic and social transactions in today's interconnected, data-driven digital economy. However, the widespread sharing of data, particularly personal data, has raised concerns regarding appropriate data usage and possible exploitation across borders, thereby escalating concerns regarding privacy and personal data protection. In response, countries have implemented and modified data regulations, enforcing measures restricting data transfer across borders or mandating data storage and processing within specific locations. Owing to the absence of an international legal framework at the multilateral level, the proliferation of diverse regulations has resulted in a fragmented regulatory landscape, posing significant challenges in effectively enforcing public policy objectives such as privacy and data protection. Consequently, businesses encounter obstacles in operating seamlessly across different jurisdictions, limiting their potential for global expansion and hampering the anticipated benefits of digitalization.

In this regard, this study aims to enhance the understanding of the policy landscape surrounding cross-border data flows and privacy protection and contribute to ongoing discussions on practical approaches and mechanisms that countries can adopt to reconcile increasingly complicated and fragmented regulatory regimes. This study examines three existing regulatory mechanisms and explores avenues for enhancing their effectiveness and the interoperability of regional and international data protection regulations to establish a comprehensive global mechanism for privacy protection. Furthermore, this study recommends two-sided efforts: first, a vertical approach of developing a compatibility mechanism built on the two pillars of the APEC CBPR and European Union

GDPR, which could elevate the level of privacy protection regulation; and second, a horizontal approach of fostering consensus on cross-border data flows and privacy protection through preferential trade agreements to increase inclusiveness. Such a compatibility mechanism, along with PTAs, can serve as an experimental domain for governance, thereby paving the way for a more effective and harmonious international regulatory framework for digital trade and the potential establishment of a global privacy protection mechanism.

Keyword: Personal Data Protection; Privacy Protection; OECD Privacy Guidelines; APEC Privacy Framework; General Data Protection Regulation; Preferential Trade Agreements

Student Number: 2020-23901

Table of Contents

Introduction

The rapid expansion of digital technology and the subsequent surge in global data exchange have brought about profound economic and trade transformations in the global landscape. The advent of modern technology has ushered in a new era of convenience and connectivity, granting unprecedented access to information and simplifying interpersonal communication. Moreover, the recent coronavirus disease (COVID-19) pandemic has acted as a catalyst, propelling the growth of the global digital economy and instigating a paradigm shift in global commerce, commonly known as digital trade. This innovative model of international trade has significantly reduced trade costs[1] and established a framework for borderless trade, revolutionizing traditional transactions of goods and services (OECD, 2020). While there has been a decline in other services, the value of digitally delivered services in global exports has experienced nearly fourfold growth since 2005, reaching US$3.82 trillion in 2022, constituting a significant 54% proportion of total global service exports (WTO, 2023).

Parallelly, digital trade expansion and prevalence necessitate data collection in various forms. In contemporary business practices, data have become integral in production, and they constitute tradable assets, forming the building blocks of global value chains (GVCs) and facilitating trade (Susan & Patrick, 2018). The application of data is crucial for emerging and rapidly growing service delivery models, such as the Internet of Things (IoT), cloud computing, and artificial intelligence (AI). The ability to

[1] Technological development reduced international trade costs by 15% between 1995 and 2014. See World Trade Organization, *The future of world trade: How digital technologies are transforming global commerce*, World Trade Report 2018.

collect, utilize, and analyze data has become a powerful maneuver in the global political economy, serving as a critical asset for companies and countries seeking competitive advantage (Burri, 2021c). The ongoing dispute between the United States and China vying for supremacy in the 5G technology domain, exemplifies the vital role of data management (Sender, 2019).

Although data exchange between countries has become an integral component of international trade, new challenges have surfaced, particularly in privacy protection, as there is an ongoing escalation in the unauthorized leakage of personal information. Governments have expressed growing concerns about the ethical utilization and exploitation of data. However, the current framework provided by the World Trade Organization (WTO) fails to deliver comprehensive guidelines for cross-border data transfer and privacy protection. Consequently, owing to the disparity in trade regulations and the proliferation of digital trade, governments have turned to national regulations and bilateral and regional agreements to achieve an equilibrium between the free flow of data and privacy protection. To address data governance issues, many countries have implemented and adjusted data regulations, enforcing measures that either condition cross-border data transfer or mandate the storage and processing of data within specific locations.

The proliferation of diverse regulations has led to a fragmented regulatory landscape, presenting significant challenges for enforcing public policy objectives such as privacy and data protection. Consequently, businesses face obstacles in effectively operating across different jurisdictions, limiting their potential for global expansion and the expected benefits derived from digitalization (Casalini, González, & Nemoto, 2021).

Erecting barriers to transnational data also undermines the efficacy of digital technologies (Kim, 2021), which play a pivotal role in driving innovation and facilitating the data-driven economy across various industries. The seamless functioning of digital technologies relies heavily on the free flow of data, which enables the utilization of vast quantities of data for transformative purposes. Therefore, despite global privacy concerns, countries have demonstrated varying stances and approaches to cross-border data flows and privacy protection, influenced by their respective political and economic considerations.

For instance, the United States has traditionally supported the liberalization of cross-border data flows as a pioneer in the legal regulation of digital trade. It aims to achieve unrestricted trade in digital services through preferential trade agreements (PTAs). The Comprehensive and Progressive Agreement for Trans-Pacific Partnership (CPTPP) Electronic Commerce Rules [2] and the United States-Mexico-Canada Agreement (USMCA) Digital Trade Rules [3] outline progressive trade policies that leverage the advanced digital infrastructure of participating countries to facilitate cross-border data transfers. In contrast, the European Union (EU) has adopted a more cautious approach to cross-border data flows, especially those concerning personal data. The EU's General Data Protection Regulation (GDPR) refers to privacy as a fundamental human right and values privacy protection over trade. Furthermore, countries such as China advocate "internet sovereignty" and impose restrictions on the free flow of data. Regarding the cross-border transfer of personal information directly related to national security, they mandate storing personal and critical data generated within their borders (Fefer, 2020).

[2] Chapter 14 of the CPTPP.
[3] Chapter 19 of the USMCA.

Although China's influence in shaping global digital regimes is not extensive, a similar approach is being shared by other countries such as India, Russia, Indonesia, and Vietnam (Kim, 2017; Lee, 2019), further complicating the development of a global privacy protection mechanism.

This study aims to enhance knowledge of the policy landscape surrounding cross-border data flows and privacy protection while fostering ongoing discussion on practical approaches and mechanisms countries can adopt to reconcile increasingly complicated and fragmented regulatory regimes. The remainder of this paper is organized as follows. Chapter I provides an introductory overview of the significance of the data, defines the key terms, and presents the rationale behind the data protection regulations. Chapter II scrutinizes the construction and evolutionary trends of data protection and the challenges posed by the current regulatory landscape. Furthermore, the Trade Agreement Provisions on Electronic Commerce and Data (TAPED), a database encompassing an illustrated delineation and categorizing all PTAs completed since 2000, is referred to in this chapter to analyze recent trends in data regulations. Chapter III examines the transnational rules for personal data protection, including organizational and geographically-based approaches. Chapter IV demonstrates the application of the General Agreement on Trade in Services (GATS) provisions to privacy protection and data-related frameworks in recent PTAs. Chapter V examines the three existing regulatory mechanisms and explores avenues for enhancing their effectiveness, as well as the interoperability and compatibility of data protection regulations to establish a comprehensive global mechanism for privacy protection. Finally, the paper concludes with a summary of key findings.

I. The Role of Data and the Need for Data Governance

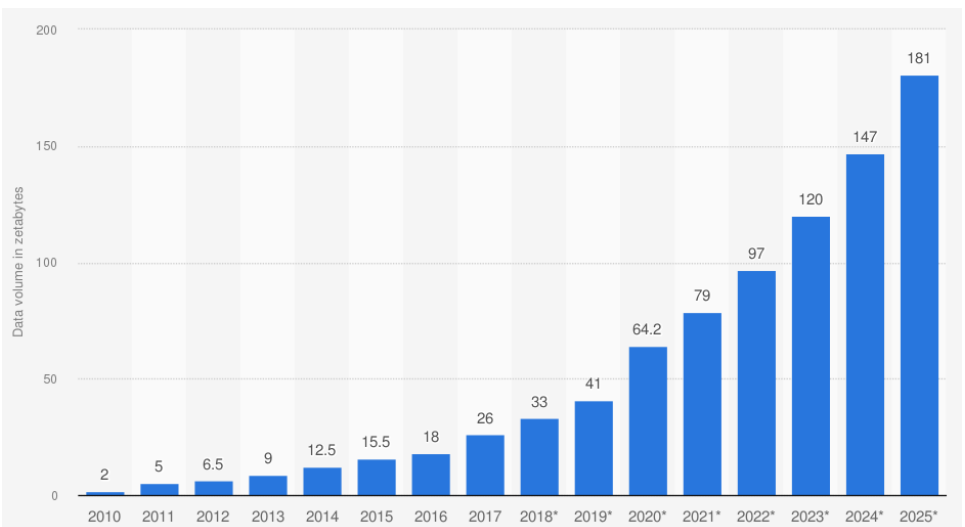
The pervasive penetration of digital technologies across all facets of economic activity has brought about a digital revolution that has caused an unparalleled surge in data exchange, both domestically and internationally. With the acceleration of the COVID-19 outbreak, the amount of data circulated worldwide, which was only 41 ZB in 2019, is expected to increase to 181 ZB by 2025 (see **Graph 1**). In contemporary times, the cross-border transfer, storage, and utilization of data have become essential components of global trade transactions, and it is anticipated that the scale and significance of data will continue to expand with the proliferation of the IoT and data-driven businesses adopted on a global scale.

Currently, firms of all sizes and industries rely heavily on data for routine operations (National Board of Trade, 2015). The impact of data is especially significant for micro-, small-, and medium-sized enterprises (MSMEs). Data flow facilitates IT services, including cloud computing and blockchain, through cross-border data flow, thereby curbing the need for costly upfront capital investments in digital infrastructure. This grants the enterprises greater agility, enabling the prompt expansion of IT capabilities in line with demand fluctuations. In addition, enhanced and expedited availability of crucial knowledge and information not only allows them to surmount informational deficiencies vis-à-vis bigger firms but also mitigates entry barriers for international trade, rendering them better prepared to vie with their larger counterparts. Multinational enterprises also rely heavily on cross-border data flow as they leverage the data gathered by their affiliates

globally to perform various internal functions relating to daily operations, including personnel data management, transfer of data to overseas research and development centers, effective management of manufacturing processes, and efficient after-sales client services.

There are numerous instances in which personal data are collected to generate economic value. Social media platforms, such as Facebook and Instagram, collect user data to provide targeted advertising opportunities for businesses. Advertisers can leverage these data to reach specific demographics, thereby increasing the effectiveness of their campaigns and maximizing the return on investment. Another example is Google Health, a platform for gathering essential patient characteristics, diagnostic records, and medication information while providing telemedicine services. Telemedicine services can enhance diagnostic intelligence capabilities by analyzing and processing these data.

Graph 1. Volume of data/information created, captured, copied, and consumed worldwide from 2010 to 2020, with forecasts from 2021 to 2025 (in zettabytes)



Source: IDC, & Statista. (June 7, 2021). Retrieved from https://www.statista.com/statistics/871513/worldwide-data-created/

1. Definition of Key Terms

Data utilization has become integral to decision-making, production processes, management, and transactions across diverse service sectors (UNCTAD, 2019). Despite the pivotal role of data in the rapidly advancing digital economy, a lack of consensus persists regarding the explicit definitions or attributes of the term "data." Data are distinct in nature and possess unique features that distinguish them from goods and services. Data exhibit intangibility and non-rivalry, making them feasible for numerous individuals to access and draw benefits from concurrently and repeatedly, without depletion (UNCTAD, 2021). Diverse interpretations can be drawn by examining alternative sources. According to the OECD, data refers to "characteristics or information, usually numerical, that are collected through observation."[4] Leblond and Aaronson (2018) define the term "data" as units serving as a means of production and inherently constituting tradable assets, thus constructing the GVCs and enabling trade facilitation.

Discussions concerning data in the realm of trade frequently center on the transmission of three distinct categories of data: personally identifiable data or personal data; industry-specific data (including financial, business, and health-related data); and the emerging trend of an ambiguous, all-encompassing data classification known as "important" data (Casalini & González, 2019). "Personal data" and "personal information" are frequently used interchangeably. However, without a standard definition for personal

[4] The OECD references the Oxford Dictionary of the International Statistical Institute.

data and personal information in international regulations, their precise meanings are subject to divergent interpretations across different jurisdictions. The OECD Privacy Guidelines (2013) define the term "personal data" as "any information relating to identified or identifiable individual." Owing to the rather ambiguous nature of this definition, the linkage of a singular aspect of a dataset to an individual is likely to render the entire collection of data "personal." Moreover, technological advancements have increased the possibility of re-identifying previously de-identified data (Schwartz & Solove, 2014). Consequently, what may be classified as non-personal data now can be recognized as personal data in the future (Casalini & González, 2019). In practice, variations in the interpretations of terms may harm the compatibility of diverse measures on cross-border transfers and the protection of data and could impact companies that conduct operations in multiple nations, as they face difficulties in evaluating whether specific types of data are classified as personal data within a particular jurisdiction. Nevertheless, based on the definitions provided by international organizations[5], this study did not strictly distinguish between "personal information" and "personal data."

Additionally, there is a lack of consensus regarding a universally accepted definition of privacy. Over the past 150 years, scholars have dedicated their research to exploring the concept of privacy and its protective nature, taking into account cultural and geographical contexts. The EU's privacy law focuses primarily on upholding individuals' dignity, whereas the United States prioritizes safeguarding autonomy and liberty (James,

[5] The APF defines "personal information" as "any information about an identified or identified individual." See Cooperation, A. P. E. (2005). APEC privacy framework. Asia Pacific Economic Cooperation Secretariat, 81.

2004). Consequently, this study involved a broad examination of privacy, which serves as a fundamental right to personal information.

2. Rationale Behind Data Protection Regulations

Governments may enforce limitations or stipulations on cross-border data flows, such as local storage requirements, to achieve various objectives and influence various types of data. Different countries have varying priorities when it comes to reconsidering their data policies, with some favoring more liberal approaches while others tend to lean toward increased state intervention. The OECD (2020) generally classifies them into five distinct categories.

First, governments must revise or establish data regulations for *privacy and personal data protection*. The intrinsic value of raw data obtained from individuals is limited, but it gains significance when the data are integrated with supplementary data, aggregated, analyzed, and processed into data products, such as in statistical analysis and databases (UNCTAD, 2021). Personal data serve as the fundamental data source that drives contemporary digital trade. The proliferation of digital services and IoT products has resulted in the significant tradability of personal information and facilitates the potential for multiple actors to amass personal data along the supply chain, rendering it susceptible to exploitation (Aaditya & Joshua, 2018). Privacy concerns encompass a spectrum of data-related activities, including collection, storage, analysis, and utilization. Therefore, it is imperative that governments safeguard personal data through regulatory measures. However, diversity in cultural perspectives regarding privacy and personal data protection necessitates varying regulatory measures, as well as definitions of privacy and

personal data. This means that what is deemed as personal data in one country may not necessarily be recognized as such in another jurisdiction (Casalini & González, 2019). Determining which data fall under the data governance framework is a multifaceted matter that is further complicated when the data traverse foreign boundaries. Various governments have been revising and introducing data policies with the emergence of regulatory challenges. Consequently, an increasing number of countries have imposed restrictions on transferring data across borders or mandated data storage within their territorial boundaries, resulting in a highly fragmented landscape of the current international regulatory framework for data protection.

Second, certain measures implemented to regulate data flow are intended to safeguard information accessibility in order to *comply with regulations or facilitate auditing procedures*. Sector-specific measures can be adopted to comply with regulatory requirements and focus on specific data types such as business accounts, telecommunications, and banking data. Third, additional measures pertain to safeguarding *national security*, allowing for extensive accessibility to and the containment of "important" and "strategic" data, particularly personal data. Fourth, governments advocate the adoption of local storage and processing solutions to fortify *digital security* measures. The reason for adopting a country-specific approach is that domestic storage and processing offer the highest assurance of digital security. Finally, there may be additional motivations for regulating the transfer and storage of data, such as promoting domestic capacity in digitally intensive industries by utilizing a centralized pool of data. This can be viewed as a form of *digital industrial policy or digital protectionism* (Casalini & González, 2019). One perspective that may be held is that data

are valuable assets that should be primarily accessible to domestic manufacturers or providers. The methodologies utilized may cater to a particular industry or have broader applicability across multiple datasets. For example, China's decision to enforce stringent internet regulations by limiting its citizens' access to foreign websites such as Google, Facebook, and Netflix has contributed to the swift expansion of its domestic digital platforms, including Baidu, Tencent, and Alibaba (이효영, 2021).

Overall, the rationales behind data protection regulations limit cross-border data flows, which function as a novel form of non-tariff trade barriers that impede digital trade and undermine trust within the digital economy.

II. Construction and Evolutionary Trend of Data Regulations

Several nations have adopted measures to address data governance issues. These manifestations can vary according to political, economic, social, and cultural circumstances and norms. This section explores three aspects of the construction and evolutionary trend of data regulations. First, the absence of international legal frameworks that can effectively deter trade barriers and enforce uniformity in cross-border data flow and protection, such as the WTO, continues to perpetuate the challenges raised by emerging digital trade. Additionally, the establishment of domestic control measures that hinder trade is increasing aggressively, thereby highlighting the detrimental effects of disparate legal regulations across nations. Lastly, as countries seek to preempt and reflect on their stances toward data through recent PTAs, there is an increasing number of data- and privacy-related provisions worldwide. This chapter provides a comprehensive overview of the current status of data regulation, emphasizing the distinctions that cause fragmentations in the global digital realm, which may cause apprehension among MSMEs and emerging economies.

1. Absence of a Legal Framework at the Multilateral Level

Thus far, WTO rules are yet to successfully govern cross-border data flows and data protection within digital trade. This is not only because the WTO establishes no data regulation but, more importantly, because the regulation of trade activities that falls under the purview of the current WTO rules is predicated on the specific commitments made

by member states. This implies that implementing the WTO rules for regulating corresponding trade activities is contingent on member countries making particular commitments to those activities. The WTO regulatory framework encompasses the exchange of goods and services between member countries. The General Agreement on Tariffs and Trade (GATT) regulates trade in goods based on the Harmonized System (HS), while the GATS regulates trade in services based on the Service Sectoral Classification List. Notwithstanding, the HS encompasses only tangible traded goods, and intangible entities such as virtual data and digital products that go beyond traditional product classifications are excluded. The Service Sectoral Classification List features a limited array of digital services, especially data-driven activities. Hence, the efficacy of the current WTO rules in regulating digital trade is limited.

2. Growing Number of Data Regulations

The expansion of data-driven businesses has prompted numerous countries to reinforce domestic regulations and accommodate them in the contemporary digital landscape (see **Figure 1**). Restrictions hindering cross-border data flow are important as they constitute one of the most specific barriers to digital trade. The growing number of these measures manifests in various forms, notably as data localization requirements, clauses that restrict access to specific online content, and conditional stipulations that necessitate adequacy assessments or discretionary authorizations for a total prohibition of data exports, as exemplified by the EU's GDPR (Andrew & Jarrod, 2018).

Among them, the data localization requirement is the most prominent one taken by various countries, typically justified on the grounds of privacy protection and national

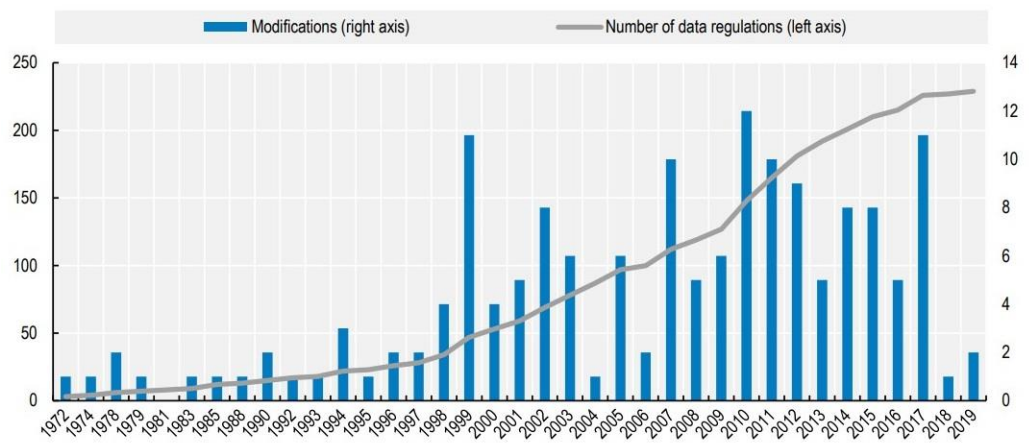
security concerns. It mandates that internet content providers maintain the data of online users within the geographical confines of their respective host countries. This typically involves using localized data-hosting servers that remain subject to the jurisdiction of the host government. The data residing in a local jurisdiction can be either an exclusive copy of the data or a mandatory local copy of data dispatched for storage or processing in another jurisdiction. Therefore, foreign businesses are mandated to construct or lease data centers within a designated jurisdiction rather than be permitted to select the most optimized location for their data centers in terms of economic feasibility (Selby, 2017). Unsurprisingly, a recent study on U.S. companies identified data localization regulations as the main non-tariff trade barrier to the digital economy (U.S. International Trade Commission, 2017). Overall, there has been a discernible increase in the implementation of explicit measures for data localization (see **Figure 2**). As of 2021, 92 provisions across 39 countries have stipulated explicit legal requirements for domestic data storage or processing. Notably, the trade regulations are progressively imposing stricter measures, wherein, by the year 2021, approximately 66% of identified measures entailed the need for storage coupled with a prohibition on data flow (López et al., 2022).

Countries worldwide have used various approaches for data localization. While many countries, notably the U.S., oppose data localization policies, others, such as Russia, Vietnam, and China, advocate facility localization or data localization requirements. The latter group also limits the free flow of personal and confidential business data, such as electronic transactions, beyond their territorial boundaries. For example, under the provisions of the Personal Information Protection Act (2011), the Republic of Korea prohibits the cross-border transfer of personal information unless the data subject

authorizes it through informed consent (Chung, 2018). China's Counterterrorism Law (2015) mandates that the international transmission of personal data is subject not only to the explicit consent of the individual concerned but also to the authorization of the government or the explicit approval of the relevant regulatory authorities (Martina & Lee, 2017). China's Cybersecurity Law (2016) restricts the transmission of data across borders by specifying that the personal data of Chinese citizens and any "important data" collected by "key infrastructure operators" must be retained within the boundaries of China (Martina & Lee, 2017).[6]

Overall, divergent national data regulations have created considerable barriers to digital trade, resulting in business outcomes falling short of expectations. Therefore, it is imperative to establish a harmonious equilibrium between facilitating the unrestricted movement of data and preserving the essential regulatory measures required to uphold various policy objectives.

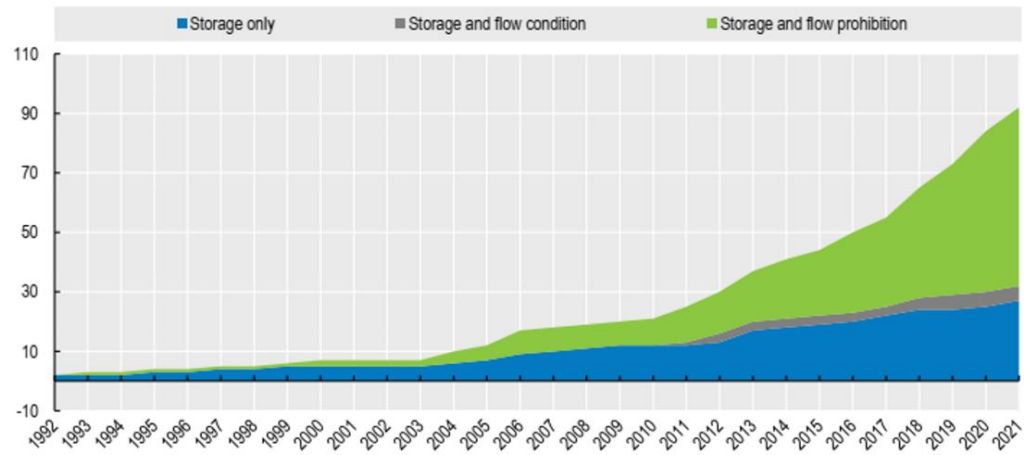
Figure 1. Growing number of regulations affecting cross-border data flows



[6] Article 37 of the Standing Committee of the National People's Congress, Cybersecurity Law of the People's Republic of China, Order No. 53 of the President of the People's Republic of China, 7 November 2016 (2016 Cybersecurity Law).

Source: Casalini & González (2019).

Figure 2. Data localization trends: Growth and increased restrictions



Source: López et al. (2022)

3. Proliferation of PTAs with Data Regulations

Ensuring the movement of data for business conduct does not preclude governments from regulating the use and transfer of data for legitimate objectives such as privacy and national security protection. Owing to the absence of universally adopted digital trade agreements, governments are resorting to bilateral and regional agreements to establish an equilibrium between cross-border data flow and privacy protection (Casalini & López, 2019). Recently, PTAs have incorporated stipulations relating to data localization, which involve restricting or prohibiting mandatory data localization or usage, and the U.S. has significantly contributed to the development of new templates by facilitating agreements such as the CPTPP, USMCA, and the United States-Japan Digital Trade Agreement (USJDTA). All these treaties encompass essential commitments in the realm of digital trade that are not only in line with WTO standards but also transcend them to address

emerging issues. Both the CPTPP and USMCA incorporated a distinct prohibition on the implementation of data localization. The dissemination of this norm was distinctly noticeable in subsequent PTAs. As of November 2022, it can be observed that 26 PTAs contained clauses that mandate the limitation or prohibition of data localization as a prerequisite for carrying out business activities. The recent Regional Comprehensive Economic Partnership (RCEP), which marks China's initial commitments on data-related issues, incorporates conditional data flows and data localization while allowing significant flexibility for domestic policies, some of which could potentially be oriented toward data protectionism.[7]

To date, 120 PTAs have included provisions for data protection. Although there are significant discrepancies between binding and non-binding provisions, it is worth noting that there is an increasing trend in data protection, especially in binding privacy-related provisions (see **Table 1**).

Table 1. Overview of privacy-related provisions in PTAs (2000-2022)

	November, 2019	November, 2022
Total number of provisions	98	120
Soft commitments	81	94
Hard commitments	17	26

Source: Own from TAPED database; See Mira Burri, Maria Vasquez Callo-Müller and Kholofelo Kugler, TAPED: Trade Agreement Provisions on Electronic Commerce and Data, available at: https://unilu.ch/taped (date of retrieval: 29.04.23).

[7] Articles 12.14 and 12.15, RCEP.

4. Issues Raised by Emerging Data Regulations

The growing proliferation of restrictive measures presents considerable challenges for companies, intensifying commercial uncertainty and escalating data regulation compliance costs in multiple jurisdictions. Companies increasingly depend on data transfer to facilitate their daily business operations. While telecommunications, information and communication technologies, and financial services rely significantly on personal data, the ubiquity of data utilization encompasses all phases of the manufacturing industry, including product design, sourcing of materials and parts, manufacturing, distribution, and final delivery to global consumers. As an increasing number of industries rely heavily on data, the related regulations present significant impediments to both traditional and digital trade by contradicting the borderless environment established by modern digital technologies (Javier & Janos, 2018). Although mutual concerns exist regarding protecting consumer privacy, businesses have raised concerns over the emerging personal data regulations. Specifically, identifying and segregating personal and non-personal data entails significant expenses that are overwhelming for most firms. Most MSMEs find this highly burdensome, and regulations concerning cross-border transfers of personal data may impact all types of data if firms cannot segregate them (Casalini & López, 2019). Data localization requirements can potentially burden local companies with additional taxes while adversely affecting the gross domestic product, exports, and foreign direct investments (Matthias et al., 2014). Furthermore, regulatory heterogeneity can give rise to ineffective barriers and undermine the efficacy of government enforcement efforts and resource allocation, posing a

significant risk of irreparable fragmentation in digital markets, undermining the effectiveness of GVCs, and ultimately eroding business competitiveness.

Furthermore, identifying an appropriate degree of "legitimate public policy objectives ('LPPO')" exceptions pertaining to data regulations poses a significant challenge. In addition to the general exceptions and security exceptions clauses of the GATS, newly established PTAs feature diverse forms of LPPO exceptions to serve as a safety net when addressing emerging digital trade issues. The LPPO exceptions invoked in conjunction with the general exceptions clauses in digital trade agreements raise apprehensions about implementing these exceptions in digital trade. Dan (2020) notes that ambiguity exists regarding the distinction between legitimate and disguised protectionism. A state may undertake multiple actions, including protective and protectionist measures. These actions may encompass promoting domestic enterprises at the expense of foreign ones, safeguarding local populations from the risks posed by the Internet, and overseeing online activities within state boundaries (Chimène, 2019). For instance, various perspectives are apparent in discussions revolving around prohibiting Huawei, a prominent telecommunications corporation in China, from participating in 5G tenders and curtailing its ability to access equipment supplies.

Therefore, as the varying approaches to data regulations and diverse interpretations of exceptions provisions could potentially diminish the extent of trade liberalization accomplished thus far, it becomes crucial to increase compatibility and harmonize the data regulatory landscape.

III. Personal Data Protection in Transnational Rules

Chapters I and II demonstrate that despite recognizing the significance of cross-border data flows and personal data in modern trade, there are divergences in domestic and international regulations, creating a challenging regulatory environment and negative repercussions for businesses and emerging economies. With the advancement of the digital economy, several international mechanisms have been developed to enhance the interoperability of regulations for cross-border transfers and the protection of personal information. Kuner (2013) stated that international privacy protection mechanisms can be organizationally or geographically based. Organizationally based regulations, including the OECD Privacy Guidelines and APEC Privacy Framework, mandate data exporters to assume responsibility for safeguarding personal data transferred to other organizations, irrespective of geographical location. A data processing entity may voluntarily comply with these requirements concerning the transmission of personal data. Meanwhile, geographically based regulations are based on determining whether the importing nation provides adequate data protection, such as the EU's top-down assessment of a third country's adherence to its adequacy requirement. This chapter begins with the accountability approach of two international organizations, the OECD and APEC, and then applies the EU's GDPR and its adequacy requirement.

1. OECD

The OECD paved the way in endorsing privacy protection principles by introducing the *Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data* (OECD Guidelines) in 1980. Owing to the increasing privacy vulnerability caused

by the internet and advanced technology, the OECD Guidelines were updated in 2013, emphasizing the importance of privacy protection worldwide.

The OECD Guidelines (2013) encompass fundamental tenets for domestic adoption and international collaboration that promote interoperability among privacy frameworks by encouraging unrestricted data flow while permitting the necessary limitations. It outlines a minimum set of principles that applies to both the public and private sectors. Countries are encouraged to uphold these principles when developing privacy protection frameworks. These principles include: (i) collection limitations, (ii) data quality, (iii) purpose specification, (iv) use limitations, (v) security safeguards, (vi) openness, (vii) individual participation, and (viii) accountability. Since 1980, these regulations have been adopted by various nations through legislation, enforcement, and policy measures, and they have significantly impacted the evolution of privacy laws, principles, and practices not only within OECD member states but also across the world (e.g., the APEC Privacy Framework) (OECD, 2020).

2. APEC

The APEC Privacy Framework (APF) adopted in 2005 comprises a set of principles and implementation guidelines for APEC member economies to develop their privacy legislation, aiming to promote data transfer while ensuring robust privacy protection within the APEC regions. While the APF incorporates principles similar to those presented in the OECD Guidelines, it differs from the latter regarding the significance of obtaining consent for data collection and the conditions for permitting cross-border data transfer. For example, consent or notice for data collection is deemed necessary only

when appropriate. Furthermore, data utilization may extend beyond the objectives established during data collection with the assent of the individual concerned or when crucial for fulfilling a requested service or product (Mattoo & Meltzer, 2018).

2.1 APEC Cross-Border Privacy Rules

Following this step, APEC established the Cross-Border Privacy Rules (CBPR) system in 2011 as an extension of the APF to establish trust among stakeholders, including consumers, corporations, and regulatory authorities, concerning the cross-border transfer of personal data. The CBPR system represents a government-backed data privacy certification framework that organizations can reduce transactional expenses by formulating pre-approved principles that facilitate cross-border data transfer among CBPR-participating economies (Casalini et al., 2021). Implementing the CBPR system in APEC economies is voluntary, and companies can pursue certification even if their respective economies adhere to the system. The CBPR system mandates that companies seeking certification undertake a voluntary assessment of compliance with the personal information protection system that adheres to the APF standards and stipulates that all their policies and practices must undergo thorough scrutiny by APEC-recognized accountability agents of each country to obtain CBPR certification. Moreover, in 2015, the Privacy Recognition for Processor (PRP), a system to certify the qualifications of a processor, was introduced to establish a more systematic network within the CBPR system, targeting only the controller of personal information (KIEP, 2023). As of February 2023, nine APEC economies have joined the CBPR system, and 59 companies have been successfully certified (see **Table 2**).

Table 2. APEC CBPR Certified Companies

Country	Accountability Agent	Certified Companies
The United States (42)	TRUSTe, NCC, Schellman & Company, BBB National Program, HITRUST	247.ai, Apple, Assurant, Asurion, BitSight Technologies, Box, Cisco Systems, Computer Expert Group, Credly, Crowley Webb & Associates, Cvent, DoubleVerify, Electronic Arts, Expedia, General Electric Company, GoTo Group, Herbalife Nutrition, Hewlett Packard Enterprise Company, HP, Hyland Software, Infor (US), IBM, Johnson Controls, Kobre & Kim, Kyndryl, Mastercard, Medallia, Merck & Co., Organon & Co., PGA Tour, Rackspace Technology Global, Reltio, Rimini Street, Slack Technologies, Talkdesk, Twilio, UKG, Virgin Pulse, Workday, World Wrestling Entertainment, Yardi Systems, Yodlee, Ziff Davis
Singapore (10)	IMDA (Info-Communications Media Development Authority)	Alibaba Cloud, CrimsonLogic, Foris Asia, Foris DAX Asia, Lark Technologies, Midea Electric Trading (Singapore), Singapore Life, The Great Eastern Life Assurance, TRS Forensics, United Overseas Bank
Japan (8)	JIPDEC (Japan Institute for Promotion of Digital Economy and Community)	Intasect Communications, Internet Initiative Japan, Paidly, Paypay, Yahoo Japan
Republic of Korea (1)	KISA	Naver

Chinese Taipei	III (Institute for Information Industry)	None
Mexico	None	None
Canada	None	None
Philippine	None	None
Australia	None	None

Source: KIEP (2023).

To facilitate the widespread adoption of the CBPR system, it currently accepts applications from all countries that align with its principles and objectives. The U.S. is committed to expanding the scope of CBPR within the APEC region and aims to extend its reach beyond APEC. These efforts include aligning the CBPR with the EU's GDPR and establishing greater compatibility to enhance interoperability.

On April 21, 2022, a consortium comprising the U.S., Canada, Japan, the Republic of Korea, the Philippines, Singapore, and Chinese Taipei launched the Global CBPR Forum. Its primary objective is to promote and encourage the global adoption of the Global CBPR System (similar to Binding Corporate Rules (BCRs) for controllers) and Global PRP System (similar to BCRs for processors), thereby enabling data protection and facilitating the free flow of data while striving for interoperability with other data protection and privacy frameworks. The Forum intends to institute a global certification mechanism for data privacy based on the APEC CBPR and PRP Systems that adhere to globally accepted data privacy standards (US Department of Commerce, 2022).

3. GDPR

The geographically based approach governs the movement of data by adhering to the data protection standards of the importing country. One example is the EU's GDPR,

which requires an adequate level of protection for the legal system in the country in question.

3.1 EU Privacy as a Fundamental Right

European societies have long placed significant importance on safeguarding data, specifically, protecting oriented toward shielding citizens from any exploitation of their personal information and ensuring the preservation of their privacy (Freude et al., 2016). The EU has a broad range of privacy rights in all sectors. The Charter of Fundamental Rights of the EU (2016) recognizes the significance of privacy and data protection as indispensable rights for citizens. The provisions of Article 7 of the Charter highlight the fundamental principle of privacy protection by granting all Europeans "the right to respect for his or her private and family life, home and communications." Article 8 explicitly acknowledges the right to safeguard personal data, stating, "data must be processed fairly for specified purposes and on the basis of the consent of the person concerned or some other legitimate basis laid down by law." The 1995 Data Protection Directive marked the onset of regulations against transmitting personal data to non-EU nations without the assurance of adequate privacy protection standards. Given the significant shifts in the regulatory landscape, specifically concerning the importance of data within the economy and society, it has become imperative to revise the Directive promptly. Additional factors that prompted the reform process were a sequence of influential rulings by the Court of Justice of the EU (CJEU), resulting in notable modifications to established legal proceedings and a more comprehensive understanding of safeguards for preserving individuals' digital rights in Europe. Specifically, the *Google*

Spain case[8] introduced the concept of the "right to be forgotten," highlighting the supremacy of privacy over the principles of free expression and the economic interests of information intermediaries such as Google Search. The *Schrems I* ruling in 2015[9] is another noteworthy example; it annulled the EU-US Safe Harbor Agreement and demonstrated the significance of cross-border data transfers, as well as the intricacies in balancing such transfers with the fundamental right to privacy protection (Burri, 2021c). Consequently, the Directive was replaced by the GDPR, which came into effect in 2018.

3.2 GDPR

The GDPR is an international framework for safeguarding data privacy and ensuring the free flow of personal data within the EU. It is a comprehensive framework that mandates businesses in all industries to abide by a set of principles and regulations governing the processing, management, and cross-border transfers of personal data, which is defined as "any information relating to an identified or identifiable natural person ('data subject')."[10] However, as mentioned in Chapter I, distinguishing between personal and non-personal data poses challenges due to ambiguous terminology used in the provisions and the technological complexities involved in collecting and managing personal data. Consequently, it is expected that the scope of the GDPR will extend beyond explicitly identifiable personal data to include data that may not be inherently personal but can potentially identify an individual when combined with other datasets. Overall, the GDPR mandates increased accountability for data controllers and processors.

3.2.1 Adequacy Requirement

[8] Case C-131/12 *Google Spain*, EU:C:2014:317.
[9] Case C-362/14 Schrems, EU:C:2015:650 (*Schrems I*).
[10] Article 4(1), GDPR.

The underlying principle of the GDPR dictates that the transfer and processing of personal data beyond the jurisdiction of the EU is strictly limited to countries and territories with "an adequate level of data protection." The European Commission confirms that these regions have a data protection and privacy framework essentially equivalent to that of the EU. With this adequacy decision, a third country can transfer personal data to its own country without requiring additional authorization.[11] These adequacy decisions culminated in extensive bilateral discussions, during which the European Commission deliberated on various factors in foreign economies. These include their data protection and privacy frameworks, adherence to the rule of law, commitments to international standards of data protection, and the nature of their economic and political relationship with the EU.[12] As of May 2023, the European Commission has acknowledged Andorra, Argentina, Canada (commercial organizations), the Faroe Islands, Guernsey, Israel, Isle of Man, Japan, Jersey, New Zealand, the Republic of Korea, Switzerland, the United Kingdom under the GDPR and LED, and Uruguay as providing adequate protection (European Commission, 2022).

3.2.2 BCRs and Standard Contractual Clauses (SCCs)

When no adequacy decision is available, a more demanding yet feasible substitute would be for a controller or processor to transfer personal data to a third country only by providing "appropriate safeguards" and "on the conditions that enforceable data subject rights and effective legal remedies for data subjects are available."[13] Each mechanism

[11] Article 45(1), GDPR.
[12] Article 45(2), GDPR.
[13] Article 46(1), GDPR.

requires approval from either the European Commission or a member-state privacy authority.

Both BCRs and SCCs constitute the main mechanisms enabling international corporations to transfer the personal data of EU individuals to third-party recipients outside the EU. According to Article 47.2, BCRs must be legally applied and provide data subjects with enforceable rights. Establishing a BCR necessitates the appointment of a controller or processor who can be held accountable for potential violations by a Member State. SCCs require the same levels of protection, monitoring, and availability for individuals as would be warranted in the case of an adequacy decision.

However, both BCRs and SCCs have certain limitations. BCRs require comprehensive implementation and meticulous approval. These requirements may pose challenges for smaller businesses seeking to export digital services to the EU, as they may not have the resources or capacity to fulfill the extensive criteria set by BCRs. In addition, SCCs are complicated because they must be structured to accommodate all possible data transfers retrospectively. This can be a daunting task considering the evolving nature of data transfers and various scenarios that may arise.

3.2.3 Extraterritorial Effect

Although the GDPR is a regulation on personal data within the EU, its applicability extends beyond its territorial boundaries as it encompasses all the activities of the establishment of controllers or processors in the EU, irrespective of the location where such processing takes place.[14] Moreover, the term "controller" refers to an entity that determines "the purposes and means of the processing of personal data,"[15] while the term

[14] Article 3(1), GDPR.
[15] Article 4(7), GDPR.

"processor" refers to an entity "that processes personal data on behalf of the controller."[16] Based on these provisions, irrespective of the lack of a physical establishment within the EU, a company must adhere to the GDPR if its business operations encompass the offering of goods or services within the EU or involve monitoring the conduct of inhabitants in the region.[17] Additional context can be derived from Recitals 23 and 24 of the GDPR. Recital 23 states that the amalgamation of online offers, which include goods or services, accompanied by the use of an EU member's language and favorable purchase prospects, are highly likely to be categorized as an offering for sale under the regulation stipulated in the GDPR. According to Recital 24, "monitoring" refers to data processing methods to track individuals online, specifically through profiling, for decision-making regarding the person or analyzing and predicting their preferences, behaviors, or attitudes. Collectively, these observations encompass a significant portion of online user experience (Mattoo & Meltzer, 2018). Overall, the expansion of the scope of EU data protection legislation has had considerable repercussions on its enforcement, particularly for foreign companies operating within or directing their efforts toward the EU marketplace.

[16] Article 4(8), GDPR.
[17] Article 3(2), GDPR.

IV. Personal Data Protection in Trade Rules

Owing to the disjointed nature of transnational rules, addressing legal challenges in the digital economy is complex. While the ongoing discussions of the Joint Statement Initiative (JSI) on e-commerce at the WTO concern digital policy issues (e.g., cross-border data flows, data localization, privacy protection, and network neutrality), PTAs have emerged as primary platforms for exploring and resolving data governance issues. Although the current state of data regulations can be likened to a complex arrangement resembling a "spaghetti bowl,"[18] the progressive trade policies outlined in the CPTPP and USMCA set the standard for cross-border data flows and data protection regulations on a global scale. This chapter critically reviews and interprets the regulations concerning cross-border data and privacy protection in three representative trade rules: the GATS, CPTPP, and USMCA.

1. GATS

The regulatory framework governing data flows under the WTO is primarily outlined in the GATS. This sector encompasses two facets of the GATS regulations: the scope and

[18] The U.S. economist Jagdish Bhagwati first introduced the term "spaghetti bowl" phenomenon in his paper, "*US Trade Policy: The infatuation with free trade agreements.*" It pertains to the complex and intricate state of various preferential treatment mechanisms and country of origin regulations as established in bilateral free trade agreements (FTAs) and regional trade agreements (RTAs) (collectively referred to as Preferential Trade Agreements, PTAs), which resemble entangled spaghetti strands. As WTO negotiations have witnessed declarations since the 1990s, nations have turned to PTAs as an expedient and flexible means to promote free trade and globalization. The intricate trade regulations and safeguarding measures implemented by countries may have adverse effects on the multilateral trade structure, diminishing the economic gains derived from commerce.

commitment of digital flows under the GATS and the GATS exceptions provisions relating to privacy concerns.

1.1 Scope and Commitment of Digital Flows under the GATS

Although WTO rules have not fully adapted to advancements in the digital age, they remain relevant in regulating e-commerce.[19] The Appellate Body affirmed that electronic delivery falls within the scope of specific commitments to service. This aligns with the perspective that specific commitments maintain "technological neutrality." Consequently, a commitment to permit service transfer across borders can be reasonably interpreted as allowing delivery through any medium, including digital flow. Nonetheless, this commitment does not necessarily mean that it entails a mandate for the unrestricted transfer of personal data. For example, a commitment to facilitate the provision of life insurance services across borders does not require a nation to permit offshore insurers to export personal health-related information beyond its borders (Mattoo & Meltzer, 2018).

Therefore, the scope of coverage for new digital services under the existing GATS commitments is currently subject to some uncertainties. Most WTO members employed either the United Nations Central Product Classification (CPC) Systems or the Services Sectoral Classifications List (MTN/GNS/W/120), or a fusion of both, for scheduling their GATS commitments. The CPC was published in 1991 when the internet was still in its nascent stage. Although the CPC has been updated several times, it is important to note that the CPC Provisional (1991) serves as the foundation for members' GATS commitments (Mattoo & Meltzer, 2018). Two of the most pertinent CPCs for digital services are under the sub-category of CPC 84, "Computer and related services," which

[19] Panel Report, *US – Gambling*, adopted 10 November 2004; Appellate Body Report, *US – Gambling*, adopted 7 April 2005.

are CPC 843 “Data processing services” and CPC 844 “Data base services.” However, it remains debatable whether these categorizations encompass modern digital services, such as search engines and cloud computing, which were non-existent at the time of commitment scheduling.

1.2 GATS exceptions provisions relating to privacy concerns

In the event of violations of the GATS provisions, Article XIV in the General Exceptions of the GATS allows WTO members to justify maintaining and adopting data restrictions to safeguard privacy concerns. According to Article XIV(c)(ii) of the GATS, measures related to “the protection of the privacy of individuals in relation to the processing and dissemination of personal data and the protection of confidentiality of individual records and accounts” are considered under the general exceptions. Regarding the necessity test, the “weighing or balancing” test established in *Korea – Beef*[20], which requires a less trade-restrictive alternative measure that could effectively attain the objective of privacy protection, is not reasonably available. Additionally, such measures should not be applied in a discriminatory manner between countries where similar conditions prevail or constitute a disguised restriction on trade in services, as stipulated by the chapeau.

Overall, Article XIV of the GATS embraces a crucial equilibrium that enables the implementation of legitimate protections while disallowing illegitimate trade protectionism. Regarding the application of Article XIV of the GATS to privacy protection issues, scholarly discourse will persist, given the absence of pertinent legal precedents. Nonetheless, as several trade agreements and recent proposals under the

[20] Appellate Body Report, *Korea – Beef*, adopted 11 December 2000.

WTO JSI have incorporated these provisions exactly or with minimal modifications, the significance of construing Article XIV of the GATS must be maintained (Burri, 2021c).

2. CPTPP

The U.S. has generally favored unrestricted data transfers and prohibited practices, including data localization, motivated by the desire to promote first-mover advantages and endorse the competitive edge of their digital firms (UNCTAD, 2019). This is because its technology industry has been highly adept at creating data-driven products and services with an extensive reach in global markets, resulting in a "positive feedback loop": the accumulation of data by U.S. companies is positively correlated to their market competitiveness and strength of their data-driven products and services in global markets (Weber, 2017). To sustain its dominant position in the worldwide digital market, the U.S. has endeavored to integrate its digital trading regulations into bilateral and multilateral trade agreements to secure unfettered market access for its corporations in foreign markets. The CPTPP and USMCA are examples of the "American model" for data flows and privacy protection.

The CPTPP is a free trade agreement (FTA) agreed in 2017 between 11 Pacific Rim countries: Canada, Mexico, Peru, Chile, New Zealand, Australia, Brunei, Singapore, Malaysia, Vietnam, and Japan. Although the U.S. has withdrawn from the agreement, the CPTPP reflects its endeavors to secure obligations on digital trade. It offers a comprehensive strategy for facilitating cross-border data flows and enhancing the interoperability and harmonization of privacy protection regulations across participating countries.

An essential aspect of the CPTPP is the inclusion of a specific obligation outlined in Article 14.11.1 on Cross-Border Transfer of Information by Electronic Means, which mandates that "Each Party shall allow the cross-border transfer of information by electronic means, including personal information, when this activity is for the conduct of the business of a covered person." Notably, these obligations apply to all types of data flows and are not limited to those essential for providing the cross-border services outlined in the GATS.

Similarly, while it can be contended that data localization requirements may breach the national treatment commitment of the GATS due to their potentially discriminatory nature, Article 14.13.2 on the Location of Computing Facilities also explicitly prohibits obligating a covered person to utilize or establish computing facilities within a particular country's jurisdiction in exchange for engaging in commercial operations.

Measures restricting cross-border data flows or requiring local data storage are permitted under Article 14.11.3 as an exception as long as (a) they do not constitute "arbitrary or unjustifiable discrimination or a disguised restriction on trade"; and (b) do not "impose restrictions on transfers of information greater than are required to achieve the objective." While the provision resembles the criteria delineated in Article XIV of the GATS and Article XX of the GATT 1994, it extends beyond the scope of WTO exceptions by encompassing LPPOs. This effectively grants CPTPP signatories greater independence in regulatory decision-making. However, the integrity of legal certainty may be called into question.

Consequently, the approach taken by the CPTPP toward privacy involves a dedication to data flows, while also allowing parties to limit the transfer of personal information as

necessary for legitimate policy purposes, such as privacy protection. In practice, this also indicates that where cross-border data transfers possess the potential to jeopardize the fulfillment of domestic privacy objectives, the CPTPP offers sufficient provisions for restraining such data movements. If there are no adequate mechanisms to ensure consistent privacy protection standards, this exceptions provision will likely be heavily utilized to restrict the transfer of personal data.

Another important aspect of the CPTPP is to mandate data-recipient countries to protect personal information, while the terminology used in its provisions leads to some ambiguity. First, it should be noted that both the CPTPP and the USMCA align on their definition of "personal information," as stated in Article 14.1 and Article 19.1, respectively. This definition encompasses the information and data of an individual who can be identified instead of a legal entity. Hence, corporate data are protected under alternative legal frameworks such as intellectual property laws. Personally identifiable information includes both direct and indirect data. Data that allow the identification of the data subject fall under personal information and warrant adequate protection.

Article 14.8.2 stipulates that "each Party shall adopt or maintain a legal framework that provides for the protection of the personal information of the users of electronic commerce." However, no specific standards or benchmarks have been outlined for the legal framework, except for a general requirement that CPTPP parties "take into account principles or guidelines of relevant international bodies."[21] Moreover, Article 14.7.3 of the CPTPP advocates for collaborative efforts among national consumer protection agencies to ensure the effective protection of consumer rights, while Article 14.8.5

[21] Article 14.8.2, CPTPP.

emphasizes the need to advance the harmonization of privacy protection standards between parties by treating lower standards as equivalent. This prioritization of economic rights over privacy rights illustrates the U.S.'s position on these matters. To some extent, the presence of these collective responsibilities mitigates the necessity of unilateral measures taken by source countries, as outlined in the exception clauses, and fosters enhanced assurance of personal data accessibility for exporters. However, it remains uncertain how parties would construe and execute the stipulation of "endeavor to adopt non-discriminatory practices in protecting users of electronic commerce" stated in Article 14.8.3, along with the level of assurance in ensuring comprehensive coverage of all consumers and contracts across all jurisdictions. Overall, although the CPTPP includes provisions for privacy protection, most of the statements are open to interpretation and do not adequately guarantee a sufficient level of privacy protection (US Congressional Research Service Report, 2019).

3. USMCA

Following the conclusion of the CPTPP, a more rigorous "American model," the USMCA, was established in 2018. It encompasses significant provisions governing data flow and protection in Chapter 19, Digital Trade, aiming to facilitate cross-border data flow and prevent data localization. Article 19.11.1 on Cross-Border Transfer of Information by Electronic Means stipulates that "No Party shall prohibit or restrict the cross-border transfer of information, including personal information, by electronic means if this activity is for the conduct of the business of a covered person," while Article 19.12 on Location of Computing Facilities states that "No Party shall require a covered person

to use or locate computing facilities in that Party's territory as a condition for conducting business in that territory." Article 19.11 remains aligned with the CPTPP in allowing for LPPOs as an exception to the limitation on the cross-border transfer of data; however, it omits the provisions of the CPTPP that authorize member states to apply their respective domestic privacy protection regulations to govern such cross-border data flow. Moreover, unlike the CPTPP, Article 19.12 of the USMCA specifically removes the exemptions for local data storage. Hence, data localization measures, even for personal data protection, cannot be justified by public policy objectives under the USMCA. In this regard, Article 19.12 may not align with the general exceptions clause in Article XIV of the GATS. In contrast to the CPTPP, the USMCA has established "armed-to-the-teeth" legal provisions to safeguard personal information and significantly elevate domestic protection standards (Lingli, 2020).

Furthermore, the USMCA deviates from the typical approach of the U.S., as it indicates adherence to specific data protection principles under Article 19.8 of Personal Information Protection. Articles 19.8.1 and 19.8.2 stipulate that "The Parties recognize the economic and social benefits of protecting the personal information of users of digital trade and the contribution that this makes to enhancing consumer confidence in digital trade. To this end, each Party shall adopt or maintain a legal framework that protects the personal information of the users of digital trade." Regarding the pertinent legal framework, the USMCA remains aligned with the CPTPP in explicitly referencing the OECD Guidelines and APF as recognized standards. Article 19.8.3 further emphasizes the significance of ensuring adherence to measures to safeguard personal data and ensuring that any limitations on the cross-border transfer of personal data are necessary

and proportionate to the risk. The rationale is that the U.S. may seek to leverage APEC to promote its distinctive approach to cross-border data flow and privacy protection (Zhou, 2020).

In contrast to the stringent data protection policies enforced by the EU, the U.S. holds relatively less sway in forming policies governing the cross-border transfer and protection of personal data. By strategically utilizing its political and economic influence within the Asia-Pacific region, the U.S. can establish a set of regulations that compete with those of the EU. This means that the U.S. can consistently broaden the implementation of its recommended data protection measures. Furthermore, the APF was developed under the leadership of the U.S., with the key objectives of stimulating e-commerce growth in the Asia-Pacific region and facilitating cross-border data transfers. The APF employs the U.S. model to safeguard personal data through industry self-discipline.

V. Toward a Global Privacy Protection Mechanism

The preceding chapters delved into the escalating conflict between the unrestricted flow of data—an integral aspect of the digital economy—and the protection of privacy, which is a fundamental right of individuals. Additionally, they highlighted the varied regulatory approaches embraced by countries and international organizations to reconcile these divergent interests, resulting in a fragmented regulatory landscape. Countries actively explore viable mechanisms that provide businesses with reliable market access and stability and those that align with their respective societal and economic values. It has been contended that inconsistent, conflicting, or incompatible data protection regimes significantly threaten the digital economy. However, the quest for an optimal model for effectively managing privacy protection on a global scale is ongoing.

Existing models can be divided into three categories: accountability mechanisms, unilateral mechanisms, and PTAs. This chapter thoroughly examines these three mechanisms and explores avenues for enhancing their effectiveness as well as the interoperability and compatibility of data protection regulations to establish a comprehensive global mechanism for privacy protection.

1. Accountability Mechanisms: OECD and APEC

The accountability mechanisms established by the OECD and APEC have played a significant role in shaping regulatory principles for privacy protection, emphasizing the implementation of minimum standards and accountability instead of a one-size-fits-all approach. Although these mechanisms are non-binding and limited to a specific number of member countries, they have successfully fostered a consensus on the fundamental

regulatory principles that balance the free flow of personal data with privacy protection. The fundamental principles and standards of these privacy and data protection mechanisms have been increasingly integrated into trade agreements such as the CPTPP, USMCA, and the recent SADEA,[22], fortifying their regulatory efficacy and propagation in multiple nations. In particular, the APEC CBPR system is expected to gain wider acceptance globally than China's protectionist model or the EU's GDPR (Bygrave, 2014).

Despite its potential, the CBPR system has experienced low participation from member economies, as discussed in Chapter III. The inactive participation of CBPR economies can be attributed to several factors. The perceived costs and efforts associated with compliance may deter businesses, especially MSMEs, from engaging in the system. Additionally, many organizations may be unaware of the advantages of CBPR principles, despite the significant compliance costs. Another essential factor may be the absence of major players (e.g., Big Tech companies) engaging in global businesses in certain CBPR economies. This indirectly indicates that the current CBPR system concentrates mainly on Big Tech companies and is not approachable by relatively smaller organizations.

Therefore, to enhance the effectiveness of the CBPR system, it is necessary to focus on expanding membership in the CBPR system and promoting members' active participation. Efforts to increase membership are underway by the U.S. through the disassociation of the CBPR from APEC. However, disparities in viewpoints regarding cross-border data flows among APEC member nations hinder the expansion of the CBPR system. Countries such as China and Russia may resist this proposal, making it challenging for APEC to advance as its decision-making process is based on unanimous

[22] The Singapore-Australia Digital Economy Agreement (SADEA) came into effect on December 8, 2020.

approval. Nonetheless, expanding the membership of APEC CBPR to include countries such as those in Central and South America, those in the African Union, and India could offer promising opportunities to enhance the effectiveness of the CBPR system. Furthermore, to facilitate active participation, it is advisable to shift the focus from Big Tech companies to MSMEs by recognizing the resource constraints that smaller organizations face and providing them with tailored guidelines.

Furthermore, governments must consistently endeavor to enhance the effectiveness of the CBPR system by improving interoperability with other certification systems and engaging in collaborative efforts. The scheduling of informal APEC meetings to examine CBPR-BCR compatibility has been temporarily postponed in light of other priorities, notably the implementation and implications of the GDPR. Efforts have been made to enhance interoperability by recognizing accountability mechanisms, such as the CBPR, as certified mechanisms by the GDPR. However, discussions regarding this matter have become uncertain due to the recent nullification of the US-EU Privacy Shield Framework[23] by the CJEU. Consequently, there is currently no consensus on the specific course of action. Nevertheless, discussions regarding interoperability must continue. In general, APEC needs to align the varying approaches taken by member economies by leveraging its non-binding nature. This would help them work toward harmonizing their efforts and achieve a more cohesive and effective framework for cross-border privacy protection.

[23] The EU-US Privacy Shield was a legally binding structure that governed transatlantic trade involving personal data for business purposes between the United States and the European Union. One of its objectives was to facilitate the acquisition of personal data from EU entities by U.S. companies while adhering to EU privacy regulations to protect the interests of EU citizens. The Privacy Shield was enacted in 2016 but was invalidated in 2020 in the *Schrems II* case.

2. Unilateral Mechanism: GDPR

The most prominent example of unilateral mechanisms is the EU's GDPR, which has the most significant impact on a global scale. However, it should be noted that exporting personal data in compliance with the GDPR can present significant challenges. As demonstrated in Chapter III, such transfers are only permitted in limited circumstances, and the criteria for granting trade partners "adequacy status" by the EU is subject to criticisms for its lack of transparency and consistency, thereby increasing the risks of legal disputes. It can also be challenging to transpose the European privacy and data protection approach into other legal systems, given its extraterritorial effect and the potential for tension with partners. Kuner (2017) describes the implementation of GDPR on a global scale as an "illusion that EU data protection law can provide seamless, effective protection of EU personal data transferred around the world."

Furthermore, the fundamental cultural and constitutional basis of the European approach to privacy compounds this challenge. Disparate approaches adopted by different sovereign states and the idiosyncratic gaps in their respective domestic legislations impede the universal dissemination of a unilateral mechanism at the global level. Rigorous unilateralism results in increased compliance costs for foreign firms and countries, which in turn may adversely affect the economy and innovation capabilities of the EU, particularly in the era of big data and AI (Burri, 2021b).

Despite these criticisms, the GDPR currently stands as the most comprehensive and advanced legislation with a global impact on privacy regulations owing to the EU's significant market power and extensive global influence. The regulatory principles and guidelines established in the GDPR have been widely adopted across several nations,

particularly in francophone countries such as Morocco, Tunisia, Benin, Mali, Canada, and Switzerland. Several nations, including Brazil, India, Japan, and the Republic of Korea, have also implemented comparable measures (Habib, 2020). Some experts, such as Jesdanum (2018), argue that the GDPR could potentially establish novel data privacy standards worldwide, as several enterprises and organizations are endeavoring to conform to the GDPR to evade compliance-related setbacks such as hefty fines or exclusion from the EU market, as well as to safeguard themselves against the imposition of analog regulations from other countries.

Irrespective of the motivations behind their adoption, EU extraterritoriality significantly influences global standards for data protection. A decrease in the level of protection may occur in the future, although its likelihood is minimal; however, dismissing the existence of the GDPR is impossible. Instead, it is crucial to explore methods to promote harmonious coexistence and cooperation. In this regard, the normative question remains as to how third countries can improve the effectiveness of GDPR adequacy decisions granted from a broader perspective. One promising approach is to establish a hub among third countries that recognize and acknowledge each other's equivalent levels of privacy protection. The EU unilaterally determines the adequacy decision for an independent country. However, considering the substantial compliance costs associated with the GDPR, it would be advantageous for third countries to leverage their adequacy status not only for conducting business with European countries but also for closer cooperation among themselves. Mutual recognition and cooperation benefit individual countries by reducing redundant compliance costs and complexity for

businesses, facilitating international businesses, and promoting a harmonized and streamlined global privacy protection landscape.

3. PTAs

Numerous trade agreements encompassing various stakeholders also have the potential to establish a more comprehensive and inclusive multilateral concurrence, which could culminate in greater efficacy and accountability through the adoption and implementation of fundamental WTO principles such as non-discrimination, least trade restrictiveness, and transparency. Additionally, as previously mentioned, differentiating between personal and non-personal data can be challenging. While only privacy concerns are addressed through accountability mechanisms and the GDPR, trade agreements can address various data-related issues such as cross-border data flows, data localization, and privacy protection. This mechanism offers more comprehensive and practical guidelines for foreign firms and countries to conduct digital trade in different jurisdictions.

Furthermore, with the limited diversity of models for current PTAs concerning digital issues, there are few concerns about the fragmentation of PTAs. Therefore, the increasing number of PTAs does not constitute a stumbling block to trade rules for global privacy protection. Moreover, the privacy protection regulations in existing FTAs do not reflect the current digital economy, and FTAs prioritize the economy over privacy protection. Their primary focus is often on economic factors such as market access, tariffs, and investments. Therefore, vitalizing PTAs that best reflect newly emerging digital issues is even more important. Although existing PTAs may have drawbacks regarding dispute mechanisms, implementation challenges, and ambiguous terminology in exceptions

clauses, these issues can be addressed and reflected on in the future without posing major obstacles.

Given the complexity of privacy issues, achieving a one-size-fits-all solution within a short time period may not be feasible. Instead, a fragmented and contested regulatory landscape is expected to persist and evolve (Farrell & Newman, 2021). Considering the importance of data regulation interoperability for an effective digital economy, this study suggests that two-sided efforts are necessary: a vertical approach and a horizontal approach. For the vertical approach, it is necessary to develop a compatibility mechanism built on the two pillars, the APEC CBPR and the EU GDPR, which can elevate the level of privacy protection regulation. For example, one solution could be a hybrid mechanism that reconciles the stringent data protection standards of the EU with the relatively lenient standards of the U.S. It is acknowledged that complete compatibility between the divergent approaches to cross-border data flows and privacy protection of the two countries may not be attainable, as the U.S. views privacy measures as means to facilitate international trade, considering them as "trade values," while the EU perceives privacy as a fundamental human right (Yakoleva, 2019).[24] Ongoing negotiations on the Trans-

[24] There remains a significant divergence between the two superpowers, despite a growing emphasis on privacy protection in the United States, as evidenced by the introduction of a federal online privacy bill in 2022, the American Data Privacy and Protection Act. As of May 26, 2023, the following states in the United States have enacted comprehensive privacy laws: California, Colorado, Connecticut, Indiana, Iowa, Montana, Tennessee, Utah, and Virginia. See more Anokhy Desai, "US State Privacy Legislation Tracker", International Association of Privacy Professionals, last updated 26th May, 2023, available online: https://iapp.org/resources/article/us-state-privacy-legislation-tracker/.

Atlantic Data Privacy Framework [25] between the two sides may fulfill the requirements of a flexible privacy protection mechanism.

Regarding the horizontal approach, this study suggests fostering consensus on cross-border data flows and privacy protection through the proliferation of PTAs with broader member economies to enhance inclusiveness. Inclusiveness plays a crucial role in the rapid expansion of digital trade. It is imperative to establish common standards that can be embraced by the majority of countries and consolidate the digital hub with active participation from broader nations. Generally, a challenge presents in reconciling global regulatory standards when seeking broader membership. Only a few countries can meet the high regulatory standards set by certain systems. To attract more countries to participate, it is necessary to lower the level of protection regulations. PTAs with relatively low privacy protection requirements, such as the CPTPP and RCEP[26], are good examples. Increasing inclusiveness is likely to foster the facilitation of digital networks and enable the realization of the national interests of individual countries.

Overall, the focus should be on striking a balance between preserving strict regulatory standards and ensuring the active participation of many countries. Such a compatibility mechanism, along with PTAs, can serve as an experimental domain for governance, thereby paving the way for a more effective and harmonious international regulatory framework for digital trade and the potential establishment of a global privacy protection mechanism.

[25] The Trans-Atlantic Data Privacy Framework was introduced following the invalidation of the EU-US Privacy Shield in July 2020.

[26] The RCEP is an FTA signed in November 2020 among the Asia-Pacific nations of Australia, Brunei, Cambodia, China, Indonesia, Japan, the Republic of Korea, Laos, Malaysia, Myanmar, New Zealand, the Philippines, Singapore, Thailand, and Vietnam.

Conclusion

Privacy protection has become of utmost importance in trade negotiations, with emerging regulations aimed at striking a balance between facilitating data flow in the digital economy and upholding individuals' rights and values. However, the absence of multilateral regulations within the WTO framework for cross-border data flows and privacy protection has led to variations in data regulations among countries, influenced by different priorities, cultural backgrounds, and legal frameworks. While current fragmented legal frameworks have encouraged regional collaboration to some extent, the interoperability issue of these frameworks has been receiving increasing attention.

Given the complexity of privacy issues, achieving a one-size-fits-all solution within a short time period may not be feasible. Instead, a fragmented and contested regulatory landscape is expected to persist and evolve (Farrell & Newman, 2021). To promote interoperability among national and international regulatory frameworks and eliminate discriminatory trade barriers, two-sided efforts are necessary. The first is a vertical approach, which involves developing a compatibility mechanism built on the APEC CBPR and EU GDPR; this could elevate the level of privacy protection regulation. The second is a horizontal approach, fostering consensus on cross-border data flows and privacy protection through PTAs to increase inclusiveness. Such a compatibility mechanism, along with PTAs, can serve as an experimental domain for governance, thereby paving the way for a more effective and harmonious international regulatory framework for digital trade and the potential establishment of a global privacy protection mechanism.

Bibliography

Andrew D Mitchell and Jarrod Hepburn, 'Don't Fence Me In: Reforming Trade and Investment Law to Better Facilitate Cross-Border Data Transfer' (2018) 19 Yale Journal of Law and Technology 182, 188–195.

APEC (2019), *APEC CROSS-BORDER PRIVACY RULES SYSTEM: Policies, Rules and Guidelines*, http://cbprs.org/wp-content/uploads/2019/11/4.-CBPR-Policies-Rules-and-Guidelines-Revised-For Posting-3-16-updated-1709-2019.pdf.

Burri, M. (2021a). A WTO Agreement on Electronic Commerce: An Enquiry into Its Legal Substance and Viability.

Burri, M. (2021b). Interfacing privacy and trade. *Case W. Res. J. Int'l L.*, *53*, 35.

Burri, M. (2021c). Privacy and Data Protection. *Forthcoming in D. Bethlehem, D. McRae, R. Neufeld and I. Van Damme (eds) The Oxford Handbook on International Trade Law, 2nd edn.* (Oxford University Press, 2022), 745-767.

Bygrave, L. A. (2014). Data privacy law: an international perspective.

Casalini, F. and J. López González (2019), "Trade and Cross-Border Data Flows", OECD Trade Policy Papers, No. 220, OECD Publishing, Paris, https://dx.doi.org/10.1787/b2023a47-en.

Casalini, F., González, J. L., & Nemoto, T. (2021). Mapping commonalities in regulatory approaches to cross-border data transfers.

Central Product Classification Version 1.0, Series M: Miscellaneous Statistical Papers, No. 77 Ver. 1.0, New York: United Nations. ST/ESA/STAT/SER.M/77.

Chan-Mo Chung, 'Data Localization: The Causes, Evolving International Regimes and Korean Practices' (2018) 52 Journal of World Trade 187, 203.

Charter of Fundamental Rights of the European Union (OJ C 202, 7.6.2016, pp. 389–405).

Chimène I. Keitner and Harry L. Clark, "Cybersecurity and trade Agreements: the State of the Art" (2019) 10 Harvard Business Review 1 at 4, 10-12.

Dan Ciuriak, "The WTO in the Digital Age" (4 May 2020) CIGI, available online: https://www.cigionline.org/articles/wto-digital-age.

Digital Watch, "The WTO Joint Statement Initiative (JSI) on e-commerce", available online: https://dig.watch/processes/wto-ecommerce

European Commission, "Adequacy decisions: How the EU determines if a non-country has an adequate level of data protection", available at: https://commission.europa.eu/law/law-topic/data-protection/international-dimension-data-protection/adequacy-decisions_en

European Parliament and Council Directive 95/46/EC on the protection of individuals with regard to the processing of personal data and on the free movement of such data, OJ 1995 L 281, 23 November 1995 P. 0031 – 0050.

Farrell, H., & Newman, A. L. (2021). The Janus Face of the liberal international information order: When global institutions are self-undermining. *International Organization*, *75*(2), 333-358.

Fefer, Rachel F. (2020), Internet Regimes and WTO E-Commerce Negotiations (R46198), Washington D.C.: Congressional Research Service, 10-13.

Freude, A., & Freude, T. (2016). Echoes of history: Understanding German data protection. Bertelsmann Foundation, 1.

H. Sender, 'US-China Contest Centres on Race for 5G Domination', The Financial Times (25 January 2019).

Habib Kazzi (2020). Digital Trade and Data Protection: The Need for a Global Approach Balancing Policy Objectives. *European Journal of Economics, Law and Social Sciences, 4*(2), 41-56.

James Q. Whitman. "The Two Western Cultures of Privacy: Dignity versus Liberty" (2004) 113 Yale Law Journal 1151 at 1161-2.

Javier López-González and Janos Ferencz, 'Digital Trade and Market Openness' (OECD 2018) Working Party of the Trade Committee TAD/TC/WP (2018)3/FINAL 39.

Jesdanum, A., (2018), Microsoft pledges to extend EU data rights worldwide, available: https://www.foxbusiness.com/features/microsoft-pledges-to-extend-eu-data-rights-worldwide.

KIEP (2023), 국경 간 프라이버시 규칙 (CBPR: Cross Border Privacy Rules) 분석과 향후 전망, 디지털 통상 브리프, 2023 년 2 월호.

Kim Nam-Jong (2021), “Global Trend and Challenges for Data Localization in Digital Trade”, Finance Brief, 30(2), pp14-16.

Kim Seung-Min (2017), “New Trade Rules to Limit Internet Restrictions: With Special Attention to Cross-Border Data Flow and Data-Localization of TPP Agreement”, The Korean Journal of International Law, 62(2), pp11-54.

Kuner, C. (2013). Transborder data flows and data privacy law.

Kuner, C. (2017). Reality and illusion in EU data transfer regulation post Schrems. *German Law Journal*, *18*(4), 881-918.

Lee Jong-Seok (2019), “The Reasons Why the Establishment of Global Digital Trade Rule has been Delayed and the Implications on Korean Digital Trade Policy”, Korea Logistics Review, 29(1), pp63-80.

Lingli, Z. (2020). Construction of Cross-Border E-Commerce Rules along the Belt and Road: With Reference to the CPTPP & USMCA. *J. WTO & China, 10*, 93.

López González J, et al. (2022), “A Preliminary Mapping of Data Localization Measures”, OECD Trade Policy Papers, No. 262, OECD Publishing, Paris.

Martina F Ferracane and Hosuk Lee-Makiyama, ‘China’s Technology Protectionism and Its Non-Negotiable Rationales’ (ECIPE 2017) <http://ecipe.org/publications/chinas-technologyprotectionism/>.

Matthias Bauer and others, ‘The Costs of Data Localisation: Friendly Fire on Economic Recovery’ (ECIPE 2014) ECIPE Occasional Paper 3/2014, 10 <https://ecipe.org/publications/dataloc/>

Mattoo, A., & Meltzer, J. P. (2018). International data flows and privacy: The conflict and its resolution. *Journal of International Economic Law*, *21*(4), 769-789.

National Board of Trade (2015), “No Transfer, No Production – a Report on Cross-Border Data Transfers, Global Value Chains, and the Production of Goods”, Kommerskollegium, Stockholm.

OECD (2013), The OECD Privacy Framework 2013, OECD Publishing, Paris, http://www.oecd.org/sti/ieconomy/oecd_privacy_framework.pdf.

OECD (2020), "Mapping Approaches to data and data flows", Report for the G20 Digital Economy Task Force, https://www.oecd.org/sti/mapping-approaches-to-data-and-data-flows.pdf.

OECD (Organization for Economic Cooperation and Development). 2013. The Evolving Privacy Landscape: 30 Years After the OECD Privacy Guidelines, in The OECD Privacy Framework. https://www.oecd.org/sti/ieconomy/oecd_privacy_framework.pdf

Schwartz, P. M., & Solove, D. J. (2014). Reconciling personal information in the United States and European Union. Calif. L. Rev., 102, 877.

Selby, J. (2017). Data localization laws: trade barriers or legitimate responses to cybersecurity risks, or both?, International Journal of Law and Information Technology, 25(3), 213-232.

Standing Committee of the National People's Congress, Counterterrorism Law of the People's Republic of China, Order No. 36 of the President of the People's Republic of China, 27 December 2015;

Susan Ariel Aaronson and Patrick Leblond, 'Another Digital Divide: The Rise of Data Realms and Its Implications for the WTO' (2018) 21 Journal of International Economic Law 245, 248.

Technological development reduced international trade costs by 15 percent between 1995 and 2014. See World Trade Organization. The future of world trade: How digital technologies are transforming global commerce, World Trade Report 2018.

U.S. International Trade Commission (2017), Global Digital Trade 1: Market Opportunities and Key Foreign Trade Restrictions, Investigation Number: 332-561.

UNCTAD (2019), "The Value and Role of Data in Electronic Commerce and the Digital Economy and Its Implications for Inclusive Trade and Development"

UNCTAD, Cross-border data flows and development: For whom the data flow, Digital Economy Report 2021.

US Congressional Research Service Report, Digital Trade and U.S. Trade Policy, (R44565), May 21, 2019, pp.35-36.

US Department of Commerce. 2022. Global Cross-Border Privacy Rules Declaration. Available at: https://www.commerce.gov/global-cross-border-privacy-rules-declaration.

Weber S (2017). Data, Dgevelopment and Growth. Business and Politics, 19(3): 397–423.

World Trade Organization – WTO, *Global Trade Outlook and Statistics*, 2023. Available at: https://www.wto.org/english/res_e/publications_e/trade_outlook23_e.htm

Yakovleva, S. (2019). Privacy protection (ism): the latest wave of trade constraints on regulatory autonomy. *U. Miami L. Rev.*, *74*, 416.

Yakovleva, S., & Irion, K. (2020). Pitching trade against privacy: reconciling EU governance of personal data flows with external trade. *International Data Privacy Law*, *10*(3), 201-221.

Zhou Meng, "New Trends in the Development of Personal Data Protection Law under the Background of WTO's E-commerce Negotiations," Journal of WTO and China, Vol.10, No.2, 2020.

이효영. (2021). 아· 태지역 디지털 무역 관련 지역무역협정을 통한 규범화 발전 동향과 평가. 무역학회지, 46(4), 39-60.

국문초록

개인정보보호의 글로벌 메커니즘 모색

- 국경 간 데이터 이동과 개인정보보호의 균형을 중심으로 -

서울대학교 국제대학원

국제학과 국제통상전공 박근영

데이터는 오늘날 상호 연결된 디지털 경제에서 경제 및 사회적 거래의 기반이 되는 귀중한 자원이다. 하지만 데이터, 특히 개인정보의 공유가 증가함에 따라 국경 간 이동하는 데이터의 적절한 사용 및 착취에 대한 우려를 낳으며 개인정보보호를 촉구하는 여론이 해를 거듭할수록 강렬해지고 있다. 이에 대응하여 여러 국가에서 데이터 규제를 강화하여 국경 간 데이터 이동을 제한하거나 특정 위치 내에서 데이터 저장 및 처리를 의무화하는 조치를 시행하고 있다. 그러나 다양한 규제의 확산은 국가 간 규제 환경의 세분화를 초래하여, 개인정보보호 및 데이터 보호와 같은 공공 정책 목표를 효과적으로 시행하는 데 상당한 어려움을 야기하고 있다. 이러한 상황은 상당수 기업이 원활하게 여러 관할권에서 운영하는데 큰 장애물로 작용하여 기업의 글로벌 확장 가능성이 제한되고 디지털화의 이점을 충분히 이용하지 못한다는 우려가 제기된다.

따라서 본 연구는 국경 간 데이터 이동과 개인정보보호를 둘러싼 정책 환경을 이해하고 여러 국가 간 세분화된 규제 체제에 대응할 수 있는 실용적인 접근 방식과 메커니즘을 제시하는데 의의가 있다. 이를 위해 본 연구는 기존 규제 메커니즘을 검토하고 프라이버시와 개인정보보호를 위한

포괄적인 글로벌 메커니즘을 구축하기 위해 지역 및 국제 데이터 보호 규정의 효율성과 상호 운용성 및 호환성을 향상시킬 수 있는 방법을 모색하고자 한다.