UNIVERSITY OF TURKU
Turku School of Economics

CHINA'S DATA PROTECTION LEGISLATION AND ITS IMPACT ON MULTINATIONAL CORPORATIONS

International Business
Bachelor's thesis
Turku school of Economics

Author:
Sara Korpineva

Supervisor:
D.Sc. Johanna Raitis

22.4.2025
Turku

The originality of this thesis has been checked in accordance with the University of Turku quality assurance system using the Turnitin Originality Check service. Artificial intelligence (ChatGPT) was used in this thesis to assist in ideation on subject matter and grammar (see Appendix 1 for detailed report on the use of AI in this thesis).

Bachelor's thesis

Subject: International Business
Author: Sara Korpineva
Title: China’s data protection legislation and its impact on multinational corporations
Supervisor: D.Sc. Johanna Raitis
Number of pages: 30 pages + appendices 1 pages
Date: 22.4.2025

The collection and utilization of data has significantly increased, creating risks to the security of countries and individuals. Due to these new threats, many countries, including China, have implemented data protection laws to safeguard national security. China's data protection legislation poses challenges for multinational corporations operating in the Chinese market. This bachelor’s thesis focuses on the impact of China’s data protection legislation on multinational corporations and provides an analysis of existing academic literature on China’s data protection legislation and its impacts.

The aim of this literature review is to understand the impacts that China’s data protection legislation has on multinational corporations’ business operations, focusing on the regulatory challenges posed by the Cyber Security Law (CSL), the Data Security Law (DSL), and the Personal Information Protection Law (PIPL). The research findings indicate that multinational corporations encounter significant challenges to comply with China’s three key data protection laws. These challenges primarily arise from the complexities of cross-border data transfer and data localization requirements. These requirements restrict market access and diminish the competitiveness of multinational corporations, leading to higher operational costs and increased legal risks.

Key words: China, data protection legislation, multinational corporation

Kandidaatintutkielma

Oppiaine: Kansainvälinen liiketoiminta
Tekijä: Sara Korpineva
Otsikko: Kiinan tietosuojalainsäädäntö ja sen vaikutukset monikansallisiin yrityksiin
Ohjaaja: KTT Johanna Raitis
Sivumäärä: 30 sivua + liitteet 1 sivua
Päivämäärä: 22.4.2025

Datan kerääminen ja hyödyntäminen on kasvanut merkittävästi, luoden riskejä maiden ja yksilöiden turvallisuudelle. Näiden uusien uhkien vuoksi monet maat, kuten Kiina, ovat kehittäneet tietosuojalakeja turvaamaan maata ja sen kansalaisia. Kiinan tietosuojalainsäädäntö luo suuria haasteista monikansallisille yrityksille, jotka toimivat Kiinan markkinoilla. Tämä kandidaatintutkielma keskittyy Kiinan tietosuojalainsäädännön vaikutuksiin monikansallisille yrityksille ja tarjoaa analyysin olemassa olevasta akateemisesta kirjallisuudesta, joka käsittelee Kiinan tietosuojalainsäädäntöä ja sen vaikutuksia.

Tämän kirjallisuuskatsauksen tavoitteena on ymmärtää, millaisia vaikutuksia Kiinan tietosuojalainsäädännöllä on monikansallisten yritysten liiketoiminnoille, keskittyen erityisesti kyberturvallisuuslain (CSL), tietoturvalain (DSL) ja henkilötietojen suojauslain (PIPL) asettamiin sääntelyhaasteisiin. Tutkimustulokset osoittavat, että monikansalliset yritykset kohtaavat merkittäviä haasteita Kiinan kolmen keskeisimmän tietosuojalain noudattamisessa. Nämä haasteet johtuvat pääasiassa rajat ylittävän tiedonsiirron ja datan paikallistamisvaatimusten monimutkaisuudesta. Vaatimukset rajoittavat markkinoille pääsyä ja heikentävät monikansallisten yritysten kilpailukykyä, joka johtaa korkeampiin toiminnan kustannuksiin ja lisääntyneisiin oikeudellisiin riskeihin.

Avainsanat: Kiina, tietosuojalainsäädäntö, monikansallinen yritys

TABLE OF CONTENTS

LIST OF FIGURES

LIST OF TABLES

1 Introduction

In the modern digital world, efficient transfer of data is crucial for multinational corporations (MNCs) (Wang, 2022, p. 385). The use of data does not stop at the national borders. MNCs operating in various countries around the world use data for their business operations, and this reliance on data necessitates cross-border data transfer. (Xie et al., 2023, p. 3.) MNCs can use data to understand customers, develop products or services, and set the direction for business operations, making data a key factor in gaining competitive advantage over competitors (Redman, 2008, p. 11). Data can be re-traded, a copy of the data can be shared without a decrease in value, and the physical storage location of data is hard to determine (Xie et al., 2023, p. 4). Due to the greater importance of data sovereignty, countries are implementing stringent data protection laws, creating more complex compliance challenges for MNCs (Xie, 2024, p. 114).

The first national data privacy law was developed in Sweden in 1973. As of 2023, 107 countries have enacted data privacy laws, making data protection a global trend. (Yu, 2023, p. 105.) China is one of these countries that have developed their data protection legislation. The rise of China in the world economy has attracted businesses from all over the world to explore its market (Tian, 2016, p. 1). Between 2016 and 2023, the size of China's digital economy has doubled, accounting for 39.8% of national GDP (Xie et al., 2023, p. 4). Although the legal foundations for data processing in China and EU are similar, China's data protection laws impose more stringent regulations on cross-border data transfers (Xie et al., 2023, p. 2). China's data protection legislation will inevitably impact MNCs' business operations. The Chinese market accounts for approximately one-seventh of the world's population, meaning that many MNCs will either suffer from additional costs and strict government supervision or lose the opportunity of accessing one of the biggest markets in the world (Quinn, 2017, pp. 432–433). Due to China's position as a major market and the strict data protection legislation China imposes on MNCs, it is important to examine this topic.

The increase in cross-border data transfers by MNCs may lead to the leakage of sensitive information, which can affect national security. This has forced China to introduce new data protection laws. (Xie, 2024, p. 111.) In the past few years between 2017 and 2021, China has implemented three key laws regarding data protection. These are the Cyber Security Law (CSL), the Data Security Law (DSL) and the Personal Information Protection Law (PIPL) that establish the foundation for data protection in China to ensure national security. (Xie et al., 2023, p. 6.) The Chinese approach to data protection is considered one of the most restrictive because of the data localizations requirements and the supervision over cross-border data transfer (Chen, 2024, p. 7).

China’s new data protection legislation presents challenges for businesses operating in China. Compliance with data regulations impacts MNCs' data transfers, operational costs, competitiveness, and legal risks. For example, the United States technology company Yahoo had been operating in China since 1999. Yahoo offers various internet services such as a multilingual news site and email. When China implemented the (PIPL), Yahoo shut down its services in China due to the increasingly complex business and legal environment. (Xie et al., 2023, p. 22.) Yahoo's exit from the Chinese market demonstrates the significant impact of China's new data protection legislation on MNCs operating within the country.

Considering these challenges, the main research question of this study is: What are the impacts of China’s data protection legislation on multinational corporations?

To answer the main research question, the study examines two sub-questions:

1. What are the key characteristics of China's data protection legislation?
2. How does China’s data protection legislation impact MNCs’ business operations?

This study seeks to bring together existing studies of China’s data protection legislation and to examine its key impacts on MNCs’ business operations. The theoretical section begins with chapter 2.1, which examines the three key laws of China's data protection legislation. The specific three laws that the study examines have been chosen, because related research agrees that the core of China’s data protections legislation is based on these three laws. This first chapter provides the foundation for examining the main research question and helps to understand the structure of China's data protection legislation. Chapter 2.2 focuses on the impacts of China’s data protection legislation on MNCs’ business operations. This chapter examines the cross-border data transfer regulations and data localization requirements imposed by China’s data protection legislation and the impacts of the legislation on MNCs’ market access, competitiveness, operational costs, and legal risks, as related research suggests that these are the business operations most affected by China’s data protection legislation. Finally, chapter 3 presents the conclusions of the study and offers perspective for future research.

2 Theory

2.1 Overview of China's data protection legislation

In a country like China, where data holds immense economic value yet poses significant privacy risks, a robust data protection legislation is essential (Conde, Li, & Vyas, 2023, p. 61). China's data protection laws were implemented primarily to protect national security, with business facilitation being a less significant concern (Xie et al., 2023, p. 2). China's data protection legislation now rests on the three legislative pillars of the Cyber Security Law (CSL), the Data Security Law (DSL) and the Personal Information Protection Law (PIPL) (Lee, 2022, p. 23). The following table 1 illustrates the purpose, application, and regulated objects of the three key laws of China's data protection legislation.

	Data Security Law (DSL)	**Personal Information Protection Law (PIPL)**	**Cybersecurity Law (CSL)**
Year	2021	2021	2016
Purpose	Regulates the security of data and information within networks (Article 1).	Aims to protect personal information and protect the free flow of personal information (Article 1).	Focuses on establishing China's sovereignty in cyberspace (Article 1).
Applicable to…	The construction, operation, maintenance, and use of networks, as well as to cybersecurity supervision and management within the People's Republic of China (Article 2).	All personal information protection handlers, including both governmental and private entities (Article 72).	Network operators, such as network service providers (Article 76)
Regulated Objects	Regulates "network data" or "electronic data". Data recorded in non-electronic formats is also regulated.	Personal information, including data identifying individuals.	Regulates "network data" or "electronic data".

Table 1 The three key laws of China's data protection legislation (Akin, 2024, p. 108)

At the core of the legislation the CSL, the DSL and the PIPL apply to all activities of data processing and set unified processing rules (Cai & Chen, 2022, p. 78). The CSL was the first of the three laws being implemented on June 1st, 2017. A few years later, the DSL was implemented on September 1st, 2021, and the PIPL on November 1st, 2021. (Xie et al., 2023, p. 6.) China's data protection legislation is now the most comprehensive system for the government to monitor, control, and influence the digital domain, including foreign entities within its jurisdiction (Lee, 2022, p. 22).

2.1.1 Cyber Security Law (CSL)

As the internet continues to become more important worldwide, concerns about its potential negative impacts have grown. Countries around the world are facing problems that arise with the growing reliance of essential life and governance functions on the world wide web. It has become evident that enemies of a nation can cause more significant disruption through cyberspace than through the physical world. (Quinn, 2017, p. 408.) Given the concern over cyberattacks, cybersecurity has become increasingly important for both governments and businesses globally (Qi, Shao, & Zheng, 2018, p.1342).

Individuals using the internet benefit from search engines, ecommerce, social networks and cloud computing, however they are also vulnerable to numerous cyber threats, including hacking, surveillance, and personal data breaches (Qi, Shao, & Zheng, 2018, p. 1343). Cyberspace threats appear in various forms, but they can be categorized by the target of the threat. When targeting an individual, the harm is usually intended on theft of finances. When a business is targeted, the harm is usually intended on intellectual property, consumer information and private communications. When targeting a government, the harm is usually intended on theft of information, dissemination of false information, or a disruption of services. (Quinn, 2017, pp. 408–410.)

China is a country facing some of the most significant threats from the internet. In 2015, before the implementation of the CSL, there were 126,424 cybersecurity attacks within Chinese jurisdiction. These cybersecurity attacks can cause significant social impact. In 2013, for instance, a corporation in China called YTO Express was attacked and the personal data of over a million customers was leaked and sold. A number of significant cybersecurity attacks over the past years helped to bring the issue to public attention. Not only did the surge in cybersecurity incidents heighten public concern about cybersecurity but it also reinforced the government’s commitment to enhance the regulation of cyberspace. A comprehensive law addressing cyber threats was essential to ensure cybersecurity in China. (Qi, Shao, & Zheng, 2018, p. 1343.)

In 2017, China implemented the Cyber Security Law (Creemers, 2022, p. 4). The CSL is one of the most comprehensive laws for securing cyberspace in China (Akin, 2024, p. 108). The law establishes national cybersecurity protection policies and designates enforcement authorities (Qi, Shao, & Zheng, 2018, p. 1344). It directs the development, maintenance and use of cyber infrastructure, providing a framework for supervising and managing network security in China (Shen & Roberts, 2023, p. 199). The CSL serves as a guideline for internet access by government agencies, organizations, and individuals (Qi, Shao, & Zheng, 2018, p. 1344).

The CSL is structured around seven chapters and seventy-nine articles. The first six chapters of the CSL contain guidelines on cyber security and network protection, while the seventh chapter defines related terms. The first chapter of the CSL states the general provisions, the objectives and the scope of the law. (Qi, Shao, & Zheng, 2018, p. 1344.) The objectives of the CSL, as stated in the first article of the law, are to "maintain the cybersecurity and safeguard the cyberspace sovereignty, national security and public interests; to protect the lawful rights and interests of citizens, legal persons and other organizations, and to promote the sound development of economic and social information technology ". These objectives indicate that the CSL was primarily implemented to ensure national security and applies solely within the context of cyberspace. (Yu, 2023, p.117.)

The third chapter of the CSL outlines the general requirements for network operators, who are responsible for managing internet services (Quinn, 2017, p. 416). The Chinese government implements a multi-layered protection system (MLPS) that requires network operators to fulfil security protection duties to safeguard networks from interference, damage, or unauthorized access. The system obligates network operators to establish internal security management protocols and implement technical measures to prevent computer viruses, cyberattacks, and network intrusions, as well as monitor and document network activity and cybersecurity incidents. Additionally, network operators must adopt measures, including data classification, backup of important data, and encryption. (Stanford University, 2017.)

Chapter four of the CSL outlines more detailed requirements for network operators, focusing on protecting personal information collected by operators (Quinn, 2017, p. 418). Article 41 of the CSL specifies that "network operators collecting and using personal information shall abide by the principles of legality, propriety, and necessity" (Stanford University, 2017). Consent must be obtained from individuals before their data is collected, and network operators should implement measures to secure the personal information they collect. Individuals can demand network operators to delete their personal information, if they discover that the operators have violated these provisions. The state will perform supervision and management on the network operators to ensure they abide by these principles. (Timoteo, Verri & Nanni, 2023, p. 183.)

The final section of the CSL focuses on the legal responsibility of network operators to comply with this law (Quinn, 2017, p. 419). Network operators who do not comply with the CSL will receive corrections and warnings. When corrections are not complied with, a fine will be imposed to the network operator and the directly responsible management personnel. When foreign entities perform intrusions, interference, damage, or other activities that threaten China's critical

information infrastructure, the State Council is also authorized to freeze the assets of institutions, organizations, or individuals, or to implement other necessary punitive actions. (Stanford University, 2017.)

2.1.2 Data Security Law (DSL)

Businesses utilize data globally to create models, make predictions, and test hypotheses. A vast amount of data is constantly generated through network technologies by people, businesses, societies, states, devices, and servers. (Nalbantoğlu, 2022, pp. 57–58.) Data differs significantly from other physical assets. It is considered to have two features that set it apart from other economic inputs: nonrivalry and excludability. Data's nonrivalry refers to its ability to be reused indefinitely and excludability refers to the difficulty of detecting its reuse. (Liu, 2021.)

Due to the difficulty of detecting the reuse of data, once individuals share their personal data, they often lose control over its future use. This characteristic of data is a political issue, as it raises concerns of surveillance conducted by foreign governments. Two of the most significant concerns regarding foreign government surveillance are that MNCs cannot guarantee they will not share individuals' personal data with their home governments, and that the home governments of these corporations operating in China cannot guarantee they will not misuse personal data for surveillance or other political purposes. (Liu, 2021, p. 56.) Because of these concerns, data security has become more significant in ensuring national security.

In the Data Security Law (DSL), data security is defined as “ensuring data is in a state of effective protection and lawful use through adopting necessary measures, and to possessing the capacity to ensure a persistent state of security” (Stanford University, 2021a). The DSL was implemented in 2021 to further develop China’s data protection legislation by introducing guidelines for data processing activities, including data security mechanisms, as well as the obligations and liabilities of state departments, organizations, and individuals handling data (Timoteo, Verri & Nanni, 2023, p. 184). The DSL provides the foundation for data processing and storage, with the goal of enhancing data security measures in China (Conde, Li, & Vyas, 2023, p. 69). The law classifies data into important data and core national data, applying different obligations to each (Akin, 2024, p. 108).

The DSL requires the state to implement a hierarchical data classification system for data security. This system categorizes data according on its relevance to economic and social development, as well as the potential risks for individuals, organizations, and national security. (Chen & Sun, 2021,

p. 210.) Important data and core data will be given prioritised protection (Shen & Roberts, 2023, p. 122). The DSL identifies important data as data for which unauthorized access, exploitation, or loss could threaten the rights of individuals, public interests or national security. Core data is defined as state, economic, or trade secrets. Categorizing data into important and core data is important as it determines the level of protection needed to mitigate the risk of incidents. (Tan, 2024, p. 8.)

The DSL is structured around seven chapters and 55 articles (Chen & Sun, 2021, p. 209). The first six chapters of the DSL contain guidelines on data security, while the seventh chapter defines related terms. The first chapter of the DSL states the general provisions, the objectives and the scope of the law. (Stanford University, 2021a.) The objective of the DSL is to ensure data security, facilitate data-driven development, and protect the legitimate rights and interests of individuals and organizations (Akin, 2024, p.107). The law applies to data handling activities within mainland China, but also has certain application beyond national borders, as activities conducted outside China are legally liable under the law, if they harm national security, public interests or the rights of individuals and corporations (Lee, 2022, p. 26).

The fourth chapter of the DSL covers the data security obligations and rules for data handling as well as outlines requirements for cross-border data transfers of Critical Information Infrastructure Operators (CIIOs). Data handling must comply with the law, and include a data security management system, training, and technical security measures. (Stanford University, 2021a). Data handlers dealing with important data must name personnel responsible for data security and regularly perform and submit risk assessment for these data handling activities. They must respond quickly to data breaches and cooperate with national security authorities. (Shen & Roberts, 2023, pp. 202–203.) The development of new data technologies must be beneficial for economic and social growth, and any individual or organization collecting data are prohibited from acquiring data through theft or any other unlawful means (Stanford University, 2021a).

Chapter six of the DSL focuses on the legal responsibility of data handlers to comply with this law. Similarly to the CSL, if data handlers, organizations, or individuals do not comply with the DSL, they are given corrections and warnings. According to the DSL, when corrections are not complied with, a fine will be imposed to the data handler and the directly responsible management personnel. The data handlers who do not comply with the law and cause serious consequences, may be ordered to suspend relevant business operations or have business permits revoked. (Chen & Sun, 2021, p. 214.)

2.1.3 Personal Information Protection Law (PIPL)

In the last several years, individuals' data privacy issues have become an increasingly important topic worldwide (Calzada, 2022, p. 1129). The protection of personal data is, from a legal perspective, one of the most important issues due to its complex implications for individual rights, government accountability, and internationally binding obligations. Without adequate data protection, individuals' privacy and rights may be at risk. (Bolatbekkyzy, 2024, p. 130.) China, with one of the largest populations in the world is continuously expanding its social welfare systems, which increasingly rely on the use of personal data and data processing. However, the collection of personal data, including facial images and personal identification, poses a greater risk for privacy issues in China. (Conde, Li, & Vyas, 2023, p. 62.)

The Internet of Things (IoT), mobile payments, and online shopping sites are evolving rapidly. Many customers value the ability to shop 24/7 and trust the sellers enough to give their personal information to use these systems. (Calzada, 2022, p. 1131.) The Personal Information Protection Law (PIPL) defines personal information as "all kinds of information, recorded by electronic or other means, related to identified or identifiable natural persons". The processing of personal information includes activities such as gathering, retaining, utilizing, transferring, sharing, and erasing individuals' information. (Stanford University, 2021b.)

Economic activity and trade are dependent on personal data, as it enables the organization of global value chains and the delivery of services. Businesses collect, process and transfer data to promote the development of new products, processes, organizational methods, and markets, while also generating greater economic and social value. The increase in data processing and transferring activities results in greater risk for the security and privacy of personal information. (Yan, 2023, pp. 1250–1251.) In 2021 China implemented the Personal Information Protection Law (PIPL) to mitigate these risks (Yan, 2023, p. 1260). Together with the Cyber Security Law and the Data Security Law, the PIPL has complemented the three pillars of China's data protection legislation (Gao, 2022, p. 86). The PIPL is the most comprehensive of the three laws and it is expected to have significant impact on MNCs doing business in China (Xie et al., 2023, p. 6). It provides detailed guidelines for safeguarding personal information, requires transparency in data processing activities and enforces penalties for non-compliance (Conde, Li, & Vyas, 2023, p. 68). The PIPL aims to protect the individuals from illegitimate data collection and use, promote the development of the digital economy, and safeguard public interest (Akin, 2024, p. 107).

The PIPL is structured around 8 chapters and 74 articles (Yu, 2023, p. 131). The first seven chapters of the PIPL contain guidelines on personal information protection, while the eighth chapter defines related terms. The first chapter of the PIPL states the general provisions, the objectives and the scope of the law. The primary objective of the PIPL is to safeguard individuals' rights by regulating their relationship with personal information handlers. While the primary objective of the law is to protect individuals, it also ensures that the handling of personal information does not endanger national security. The law applies to both private and public entities handling the personal information of individuals within the borders of China. (Timoteo, Verri & Nanni, 2023, p. 188.)

The second chapter of the PIPL establishes the basic rules for handling personal information. The law states that personal information handlers must obtain the individuals' consent before handling their personal information. Consent must be given with full knowledge of the situation, and it must be both voluntary and explicit. Individuals have the right to withdraw their consent, and the personal information handler is obligated to inform them of this right. Consent is the key requirement for handling personal information, but the PIPL outlines specific cases, where data processing can be justified without it, for example, in response to public health emergencies, to protect individuals' lives and health, or to ensure the security of their property. (Timoteo, Verri & Nanni, 2023pp. 188–189.)

Chapter three of the PIPL outlines the rules for cross-border transfer of personal information (Stanford University, 2021b). The PIPL provides four ways that enable entities to transfer personal data across international borders. These are by passing the security evaluation conducted by the Cyberspace Administration of China (CAC), acquiring certification for personal data protection, signing a contract with the foreign recipient based on a standard agreement set by the CAC, or fulfil other conditions in laws or regulation established by the CAC. (Bolatbekkyzy, 2024, p. 138.) MNCs that process large volumes of data are obligated to store the data locally in China (Xie et al., 2023, p. 18).

Chapters four and five of the PIPL form the core of the law, outlining individuals' rights in personal information handling and the obligations of personal information handlers (Timoteo, Verri & Nanni, 2023, p. 189). The PIPL states that individuals have a right to information about their personal information, and a right to limit or refuse the use of their personal information (Stanford University, 2021b). Individuals have a right to demand the deletion of their personal information and a right to request the handler to explain personal information handling rules (Yu, 2023, p. 121). The PIPL sets multiple obligations for personal data handlers (Calzada, 2022, p. 1136). Handlers

must implement internal management procedures, restrict access to personal data, and provide data protection training to ensure compliance with the PIPL (Yu, 2023, p. 122). Entities handling personal information beyond China's jurisdiction must disclose personnel responsible for personal information and a local representative within the borders of China. Handlers must report the names and contacts of the personnel in charge of personal information. Personal information handlers must conduct regular audits of their personal information processing and compliance with laws. (Stanford University, 2021b.)

The final section of the PIPL focuses on the legal responsibility of personal information handlers. It outlines procedures for cases where handlers fail to comply with the law. The PIPL imposes various sanctions for non-compliance, including correction for non-compliance, confiscation of unlawful income, and suspension or termination of services provided by unlawful personal information handlers. If these corrections are not complied with, a fine will be imposed on these personal information handlers. (Bolatbekkyzy, 2024, p. 139.)

2.2 The impact of China's data protection legislation on MNCs' business operations

In the following chapters, I will address how China's data protection legislation impacts MNCs' business operations. Globalization has driven many corporations to conduct business in multiple countries, requiring data to be transferred across national borders (Xie, 2024, p. 111). China's data protection legislation imposes strict regulations on cross-border data transfers and data localization requirements, posing various compliance challenges for MNCs (Xie et al., 2023). These restrictions on the cross-border transfers of data create more bureaucratic hurdles for MNCs and impact them on a broad range of business operations. They impact MNCs' market access and competitiveness by creating barriers to business expansion and innovation. MNC's operational costs will increase due to additional investments in technology, infrastructure, and personnel. (Xie et al., 2023, pp. 18–20.) The CSL, the DSL, and the PIPL all impose sanctions in cases of non-compliance, creating more legal risks for MNCs. (See Table 2)

	Legal requirement	Impact area	Impact for MNCs
1.	Cross-border data transfer & data localization	Market access, competitiveness, operational costs	Barriers to business expansion, need for local infrastructure
2.	Compliance enforcement (CSL, DSL & PIPL)	Sanctions, legal risks	Higher exposure for legal risks, need for legal compliance

Table 2 Key business impact areas

Table 2 above outlines the legal requirements and the key business impact areas of China's data protection legislation on MNCs. These requirements and business impact areas will be examined in more detail in the following chapters.

2.2.1 Cross-border data transfer regulations and data localization requirements

Cross-border data transfer refers to the transmission of information from one country to another. Data localization, on the other hand, refers to any measure that restricts or limits such transfers. MNCs' business operations rely on the efficient transfer of data. (Wang, 2022, p. 387.) Cross-border data transfers are essential components of the globalized data economy, enabling MNCs to transfer customer data across borders between different offices (Xie et al., 2023, p. 16). China's data protection legislation creates challenges for MNCs' data transfers by imposing regulations on cross-border data transfers and data localization (Lee, 2022, p. 31). Among the three laws, the PIPL has the most stringent regulations on cross-border data transfers of personal information (Xie et al., 2023, p. 6). However, the DSL also imposes regulations on cross-border data transfers of important information (Chen & Sun, 2021, p. 214). The requirements for cross-border data transfers make data transfer significantly more complex for MNCs by creating more bureaucratic hurdles (Gao, 2022). Data localization requirements also create compliance challenges for MNCs (Zhang, 2024, p. 12). China's data protection legislation states that before MNCs can transfer personal data, one of four requirements must be met (Bolatbekkyzy, 2024, p. 138). (See Figure 1)

Figure 1 Requirements for cross-border data transfer (Xie et al., 2023, p. 7)

First, MNCs can gain approval for data export by completing a security assessment administered by the Cyberspace Administration of China (CAC) (Bolatbekkyzy, 2024, p. 138). Passing this security assessment is mandatory for MNCs that process important data, handle the personal information of over one million individuals, or have transferred the data of 100,000 individuals to foreign countries (Chen, 2024, p. 2). Before the implementation of this assessment, MNCs must conduct a self-assessment, including the purpose, scope and manner of data export, the associated risks of exported data as well as mechanisms for protecting personal information in cases of data damage and leakage. Second, MNCs can obtain a personal information protection certification to export data. The certification process includes a technical inspection, an on-site review, and post-certification supervision. (Xie et al., 2023, p. 8). The third option for MNCs, which are not required to undergo the mandatory security assessment by the CAC, is to sign a contract with the foreign data handler, based on standards defined by the CAC. MNCs that meet other legal requirements can also export data, although this method requires further legislative and regulatory clarification. (Bolatbekkyzy, 2024, p. 138.)

The data protection laws also outline obligations for MNCs during data processing activities. Data protection is crucial during data export. MNCs are required to disclose personnel responsible for personal information and a local representative within the borders of China. The individuals in charge of personal information protection must establish the primary objectives, core requirements, key responsibilities, and protection measures for ensuring the protection of personal data. MNCs are additionally required to set up a personal information protection agency that is responsible for preventing unauthorized access to personal information as well as leaks, tampering, and data loss. (Xie et al., 2023, p. 10.) China's data protection legislation also imposes data localization regulations on MNCs that handle personal information exceeding a certain threshold (Creemers, 2022, p. 6). MNCs that are required to undergo a security assessment by the CAC must store data

within China's borders. A copy of the data must be stored locally, even if these MNCs pass the security assessment. Consequently, many MNCs need to establish new data centers in China to comply with the country's data protection legislation. (Xie et al., 2023, p. 18.)

China's data protection legislation has specific requirements for Critical Information Infrastructure Operators (CIIOs) handling important data (Chen & Sun, 2021, p. 214). Critical information infrastructure operators are entities responsible for operating information systems that are essential to a country's national security or economic stability (Herrera & Maennel, 2019, p. 50). The legislation mandates that these operators must store their data within the borders of China and when they need to transfer data out of China, they must pass the security assessment by the Cyberspace Administrative Departments. The non-CIIO operators must follow measures enacted by the CAC to transfer data out of China. (Chen & Sun, 2021, p. 214.) The following figure 2 demonstrates the rules for cross-border data transfers of personal information and important information.

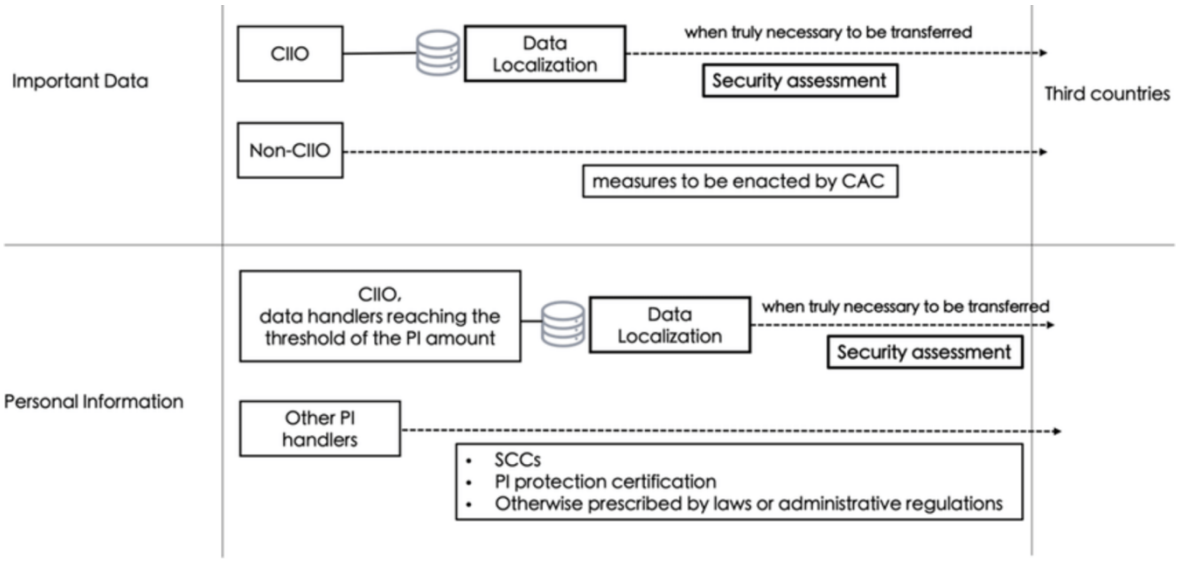

Figure 2 Rules for cross-border data transfer (Chen & Sun, 2021, p. 216)

Examples of MNCs that have adapted to these data localization requirements are Apple and LinkedIn. Apple has been storing its Chinese customers data within China since 2017, following the implementation of the CSL. Apple does not use the same encryption technology for data stored in China as it does elsewhere, allowing the government to access this data when necessary. Another way to comply with China's data protection legislation without storing data in China is to offer products that operate independently from the non-Chinese market thereby eliminating the need for cross-border data transfers. In 2021, LinkedIn announced it would shut its platform in China due to the significantly more challenging compliance requirements. Rather than fully exiting the Chinese market, LinkedIn introduced a separate platform, InCareer, in December 2021. This new platform is

entirely separate from the global LinkedIn platform, enabling the company to navigate around the new cross-border data transfer and data localization regulations. (Xie et al., 2023, p. 25.)

MNCs should address the challenges posed by China's data protection legislation on cross-border data transfers and data localization in three main areas: legal compliance, technical safeguards, and international cooperation. To ensure legal compliance, MNCs should establish a comprehensive compliance system and form a dedicated team responsible for aligning the company's data management policies with legal requirements. The team should include experts from various fields, such as legal, technical, and business, to effectively develop a compliance strategy based on China's data protection legislation. MNCs should also establish clear guidelines on the responsibilities of personnel handling cross-border data transfers and implement a system for self-assessing data compliance. (Xie, 2024, pp. 121–122.)

To ensure technical safeguards, MNCs should enhance their data protection technologies. They should implement measures such as data encryption, anonymization, and de-identification to protect user privacy, reduce the risk of data leakage, and ensure compliance with China's data protection laws. MNCs can also enhance data protection automation by integrating artificial intelligence and machine learning into their business operations, enabling continuous monitoring and prompt mitigation of data leaks. In terms of international cooperation, MNCs should engage in regular communication with Chinese data protection regulators to stay informed about the latest legal developments and regulatory obligations, adjusting their data management systems accordingly. (Xie, 2024 pp. 121–122.)

2.2.2 Market access and competition

China's data protection legislation will impact both the market access of MNCs and their competitive position within the market. MNCs will lose market share, and China's data protection laws will affect the competitiveness and innovativeness of these corporations. (Xie et al., 2023.) Already during the drafting of the CSL, foreign corporations were concerned that the law would limit MNCs' market access and lead to unfair competitive advantages for Chinese corporations (Qi, Shao, & Zheng, 2018, p. 1351). While China's data protection legislation presents challenges for MNCs, the country's enormous consumer market and business opportunities make market access highly beneficial for many corporations (Xie et al., 2023, p. 25).

The strict regulations on cross-border data transfers and data localization imposed by China's data protection legislation function as trade barriers on service imports, increasing the market share of

local corporations. These requirements also allow China to restrict MNCs' market access if the required cross-border data transfer and data localization requirements are not met. (Qi, Shao, & Zheng, 2018, p. 1352.) China's data protection legislation will increase the market share of Chinese firms putting MNCs at a disadvantage (Xie et al., 2023, p. 2). A good example of the challenges MNCs face to access the Chinese market is Google's attempt to establish a Chinese domain. Google, based in California originally had difficulties accessing the Chinese market. After establishing a Chinese domain, Google began to censor itself to comply with the Chinese data protection legislation, despite this being against Google's policy. After exiting from the Chinese market for a period, Google returned, again facing the challenges of the country's data protection legislation. Ultimately, the result was that Chinese individuals were deprived of access to a large amount of information. (Quinn, 2017, pp. 433–434.)

In comparison to Chinese corporations, which do not engage in cross-border data transfers, MNCs are required to undertake significantly more efforts to comply with China's data protection legislation. Compliance with cross-border data transfer and data localization regulations, forces MNCs to duplicate data centers, staff, and key operative processes within China. These data protection laws are likely to impact the competitiveness of MNCs operating in various sectors, including tourism and financial services. For instance, hotels rely on customer information to provide services across multiple locations, requiring free flow of data. On the other hand, in the financial sector, overseas wealth management organizations need to process sensitive customer information, including details related to clients' financial status, family background, and health conditions. (Xie et al., 2023, p. 23.)

The competitiveness of corporations depends on their capability for innovation. Innovation is a cornerstone of competitiveness and a key driver of the development of MNCs, sustainable economic growth, and social well-being. (Doğan, 2016.) China's strict data protection legislation will likely affect MNCs' innovation in data-based products and services due to restrictions on data sharing. The legislation restricts the merging of different databases and prevents MNCs from collecting data without a clearly defined purpose. These regulations significantly restrict innovation in data-based products and services. (Xie et al., 2023, p. 23.)

The restrictions imposed by China's data protection laws can be leveraged by the government to strengthen the local economy by providing domestic corporations with competitive advantages (Qi, Shao, & Zheng, 2018, p. 1351). These restrictions on data sharing significantly diminish the value of MNCs in China, because their employees based in China will not be able to access the group's

knowledge, experience, and expertise from other markets. The rest of the group will also be unable to leverage the knowledge, experience, and expertise of its China entity. (Shen & Roberts, 2023, p. 209.) Data can be reused indefinitely, leading to increased welfare gains as it is shared within and across corporations to generate business insights. Due to data transfer restrictions, China is limiting MNCs' access to this key productive capital. On the other hand, China is promoting data flows between corporations within the country, enhancing the productivity of local Chinese firms as they can leverage more data. (Xie et al., 2023, pp. 23–24.)

2.2.3 Operational costs

In comparison to the EU's GDPR, the implementation of China's data protection legislation is likely to result in higher operational costs for MNCs (Xie et al., 2023, p. 21). MNCs have to make investments to implement compliance initiatives, seek legal consultations, and restructure data management systems to separate their Chinese operations from their global network (Tan, 2024, p. 9). Estimates suggest that complying with the GDPR has cost the average European company close to three million USD. It is expected that China's data protection legislation will similarly raise the operational costs of MNCs. (Xie et al., 2023, p. 21.) China's data protection laws impose multiple requirements on MNCs operating in China. These include cross-border data transfer and data localization rules and the implementation of new systems and procedures. To comply with these laws, MNCs' operational costs will increase. (Tan, 2024, p. 8–9.)

Under China's data protection legislation, MNCs with global systems are unable to freely transfer data to their overseas recipient (Lee, 2022). MNCs must allocate additional resources to bureaucratic processes, such as security assessments and certification procedures, to continue cross-border data transfers. MNCs that meet the criteria for security assessments are required to store their Chinese customers' data within the country. (Xie et al., 2023, p.21.) These localization regulations require certain MNCs to establish local data centers, increasing their operational costs (Zhang, 2024, p. 12). Findings from the United States International Trade Commission (USITC) and the Global Economic Survey indicate that 22% of digital technology companies, 24% of digital social enterprises, and 25% of wholesalers believe that removing these digital barriers created by cross-border data transfer regulations would increase their revenue by more than 15 percent (Abdelrehim Hammad, Khan & Soomro, 2021, p. 42).

China's data protection legislation requires MNCs to implement new systems and procedures to ensure compliance (Tan, 2024, p. 8). MNCs are required to implement internal security management systems and adopt technical measures to prevent computer viruses, cyber-attacks, and

network intrusions. Additionally, they must adopt measures, including data classification, backup of important data, and encryption. (Stanford University, 2017.) The obligations imposed by China's data protection legislation will significantly increase MNCs' operational costs, as they must invest more in carefully assessing and adapting their internal data governance structures while conducting risk and compliance assessments (Tan, 2024, p. 9).

The demand for experts with knowledge of both the technical and legal aspects of data compliance is growing rapidly. As data protection is advancing and demand rising significantly, there is a shortage of these professionals. (Jiang, 2024a, p. 318.) Hiring new personnel to comply with China's data protection legislation will increase MNCs' operational costs. For example, Facebook had to hire 1,000 additional staff globally to ensure compliance with the GDPR (Xie et al., 2023, p. 21).

2.2.4 Legal risks and sanctions

MNCs operating in China are exposed to multiple legal risks under the country's data protection legislation. They must also consider that China's government is prepared to impose punitive measures in response to illegal actions (Lee, 2022, p. 33–34.) Every corporation faces legal risks, which refer to the potential exposure to penalties, financial sanctions, and material losses resulting from non-compliance with laws and regulations. MNCs should take compliance seriously to avoid significant negative consequences. Identifying and mitigating legal risks can lead to lower regulatory penalties, reduced management time, and decreased operational activities. (Buresh, 2022.)

A significant legal risk for MNCs is the sharing of data with foreign law enforcement agencies. China's data protection legislation mandates that MNCs must not share data stored within China's territory with foreign law enforcement agencies without consent from Chinese authorities. MNCs may encounter legal conflicts if their home country requires them to provide information from their subsidiaries in China, which they may be unable to do under the legislation. For example, MNCs in the financial industry may be required to disclose data to law enforcement authorities in their home jurisdiction. One of the key challenges for MNCs is the lack of clear guidance on how to obtain approval for sharing data with foreign law enforcement agencies. (Shen & Roberts, 2023, pp. 203–204.)

China's data protection laws impose sanctions on MNCs for non-compliance (Yu, 2023, p. 123). Under the CSL, non-compliance with personal data protection regulations can result in fines

ranging from 10,000 to 100,000 yuan for the network operator, while directly responsible management personnel can face fines between 5,000 and 50,000 yuan. When MNCs engage in intrusions, disruptions, damage, or other actions that threaten China's critical information infrastructure, the State Council may freeze the assets of institutions, organizations, or individuals, and impose other necessary punitive measures. (Stanford University, 2017.)

As the DSL mandates that MNCs cannot share data stored within China's territory with foreign law enforcement agencies without approval from Chinese authorities, violating these regulations will result in sanctions. MNCs violating these regulations can be fined up to 5 million yuan while directly responsible management personnel may face fines up to 500,000 yuan. The data handlers who do not comply with the law and cause serious consequences, may be ordered to suspend relevant business operations or have business permits revoked. (Chen & Sun, 2021, pp. 2017–2018.)

The PIPL imposes various sanctions for non-compliance, including correction, confiscation of unlawful income, and suspension or termination of services provided by unlawful personal information handlers. MNCs which do not correct their actions can be fined up to one million yuan while directly responsible management personnel may face fines up to 100,000 yuan. (Bolatbekkyzy, 2024, p. 139.) The PIPL imposes significant sanctions for violations of cross-border data transfer and data localization regulations. MNCs that violate these regulations may be fined up to five percent of their annual turnover or up to 50 million yuan. (Tan, 2024, p. 10.)

An example of the Chinese government's punitive actions is the Didi case. China conducted a cybersecurity review of Didi Global's business operations, resulting in a fine of 8.026 billion yuan for violations of various data security regulations. (Jiang, 2024b, p. 81.) Didi's penalty was imposed under the PIPL, which allows fines of up to 1 million yuan for general violations and up to 50 million yuan or five percent of the previous year's turnover for severe violations. Didi's fine was calculated based on five percent of its 2021 revenue, which amounted 173.83 billion yuan. (Conde, Li, & Vyas, 2023, p. 69.) These actions by the Chinese government demonstrate the significant legal risks that MNCs face when doing business in China (Jiang, 2024b, p. 82).

3 Conclusions

This bachelor's thesis offers a review of China's data protection legislation and its impact on MNCs' business operations. The aim of this study is to understand the impact of China's data protection legislation on multinational corporations. To understand these impacts, I examined the key characteristics of China's three key data protection laws and their impact on MNCs' business operations, focusing on cross-border data transfer regulations and data localization requirements, market access and competitiveness, operational costs, sanctions, and legal risks. In the following discussion, I will review both sub-questions to summarize the key findings leading to the main objective of this study: understanding the impact of China's data protection legislation on multinational corporations.

Data has become an increasingly valuable asset for MNCs, posing greater privacy risks to countries. China, among many other countries, has implemented new data protection laws, including the CSL, the DSL, and the PIPL, all of which impose strict restrictions on MNCs operating in China. These three key laws primarily aim to protect the personal information of Chinese individuals and safeguard national security. Key obligations imposed by China's data protection legislation on MNCs are the requirement for data localization and strict regulations on cross-border data transfers. The laws require companies to go through complex bureaucratic hurdles to conduct cross-border data transfers. They also mandate that MNCs store the data of Chinese individuals within the borders of China, requiring many MNCs to establish new data centers to ensure compliance.

China's data protection legislation also mandates MNCs to implement new security management systems, adopt new data security measures and name personnel responsible for data security and personal information protection. The personal information of Chinese individuals is well protected, and MNCs seeking to use this data must obtain individuals' consent for its collection. All three key laws of China's data protection legislation impose sanctions for non-compliance. These sanctions can create serious legal risks for MNCs, as they can be financially substantial in size. The sanctions can vary from fines to the revocation of MNCs' business permits.

The most significant impacts of China's data protection legislation on MNCs are created by cross-border data transfer restrictions and data localization requirements. The transfer of data across national borders is one of the most important business operations for MNCs, as they need to share data collected in China with their headquarters and global partners to maximize its benefits. MNCs can leverage data to enhance their products and services and to set strategic goals for their business.

These restrictions on cross-border data transfers and data localization requirements impact MNCs across a broad range of operational areas.

First, cross-border data transfer restrictions create digital barriers, making it more difficult for MNCs to enter the Chinese market. MNCs must meet strict requirements before transferring data across borders, and without this ability, operating in foreign markets becomes significantly more challenging. MNCs' competitiveness is also negatively affected by these restrictions. In order to comply with cross-border data transfer and localization regulations, MNCs must establish duplicate data centers, workforce, and key operational processes within China. Local Chinese corporations, which are not subject to these additional requirements, gain a competitive advantage over MNCs, which must undertake significant additional efforts to comply with China's data protection legislation.

MNCs' operational costs can rise under these cross-border data transfer and data localization regulations, due to MNCs having to invest more money on bureaucratic processes, such as security assessments and certification procedures. Localization regulations require MNCs to establish local data centers increasing their operational costs. In addition, MNCs have significant legal risks related to cross-border data transfer and face sanctions if they violate these regulations. MNCs are not allowed to share data stored within China with foreign law enforcement agencies, without consent from Chinese authorities. This can create legal risks if the home country requires MNCs to hand over data from their Chinese subsidiaries.

As established through this analysis, the extent of the impacts of China's data protection legislation on MNCs is significant and may even prevent MNCs from doing business in China. China's three key data protection laws collectively create a complex compliance landscape for MNCs, with the PIPL having the greatest impact. Its stringent regulations on cross-border data transfer and data localization present the most significant compliance challenges for MNCs. These three key laws of China's data protection legislation are still relatively new, and their impacts are not yet entirely clear. This study is based on existing academic research about China's data protection legislation. Many existing studies use, for example, the EU's GDPR to assess the impacts of the legislation on MNCs, comparing the regulatory frameworks of China and the EU, and their effects on global business operations.

Future research could further explore the impacts on technology companies, which are significantly affected by data protection laws. My study of the impacts of China's data protection legislation does not focus on a specific industry, and existing research on the impacts on technology companies is

limited. Technology companies are dependent on data collection and processing. Therefore, it would be beneficial to further explore how multinational technology companies adapt their products and services to ensure compliance in China, as well as the challenges posed by China's data protection laws to cooperation between Chinese and Western companies.

References

Abdelrehim Hammad, A. A., Khan, A., & Soomro, N. E. (2021). Digital Economy Barriers to Trade Regulation Status, Challenges, and China's Response. International Journal of Social Sciences Perspectives, 8(2), 41-49.

Akin, E. E. (2024). Chapter VI. The Chinese Approach to Information Technology Law. SMART CITIES, ARTIFICIAL INTELLIGENCE AND DIGITAL TRANSFORMATION LAW, 105.

Bolatbekkyzy, G. (2024). Comparative Insights from the EU's GDPR and China's PIPL for Advancing Personal Data Protection Legislation. Groningen Journal of International Law, 11(1).

Buresh, D. L. (2022). Risk and Its Effect on Complying with International Privacy Laws. Indon. J. Int'l & Comp. L., 9, 449.

Cai, P., & Chen, L. (2022). Demystifying data law in China: a unified regime of tomorrow. International Data Privacy Law, 12(2), 75-92.

Calzada, I. (2022). Citizens' data privacy in China: The state of the art of the Personal Information Protection Law (PIPL). Smart Cities, 5(3), 1129-1150.

Chen, J., & Sun, J. (2021). Understanding the Chinese data security law. International Cybersecurity Law Review, 2(2), 209-221.

Chen, M. (2024). Developing China's Approaches to Regulate Cross-border Data Transfer: Relaxation and Integration. Computer Law & Security Review, 54, 105997.

Conde, I., Li, Y., & Vyas, R. P. (2023). Global Companies and China's Data Privacy Laws: Analysing DIDI'S Case and Regulatory Compliance Implications. Chinese Journal of Transnational Law, 2753412X241288770.

Creemers, R. (2022). China's emerging data protection framework. Journal of Cybersecurity, 8(1), tyac011.

Doğan, E. (2016). The effect of innovation on competitiveness. Istanbul University Econometrics and Statistics e-Journal, (24), 60-81.

Gao, G. (2022). Cross-Border Provision of Information under New Chinese Data Protection Legislation. Disp. Resol. Int'l, 16, 85.

Herrera, L. C., & Maennel, O. (2019). A comprehensive instrument for identifying critical information infrastructure services. International Journal of Critical Infrastructure Protection, 25, 50-61.

Jiang, F. (2024b). China's legal efforts to facilitate cross-border data transfers: a comprehensive reality check. Asia Pacific Law Review, 32(1), 81-101.

Jiang, Y. (2024a, October). Data Protection from A Global Perspective: Challenges and Strategies for Multinational Corporation Data Security Compliance. In 2024 2nd International Conference on Management Innovation and Economy Development (MIED 2024) (pp. 314-325). Atlantis Press.

Liu, L. (2021). The rise of data politics: digital China and the world. Studies in Comparative International Development, 56(1), 45-67.

Lee, J. (2022). Cyberspace Governance in China: Evolution, Features and Future Trends.

Qi, A., Shao, G., & Zheng, W. (2018). Assessing China's cybersecurity law. Computer law & security review, 34(6), 1342-1354.

Quinn, J. (2017). A Peek Over the Great Firewall: A Breakdown of China's New Cybersecurity Law. SMU Sci. & Tech. L. Rev., 20, 407.

Redman, T. C. (2008). Data driven: profiting from your most important business asset. Harvard Business Press.

Shen, E., & Roberts, A. (2023). China's cross-border data sharing requirements: Compliance challenges for global institutions. Journal of Financial Compliance, 6(3), 198-212.

Stanford University. (2017, June 1). Translation: Cybersecurity law of the People's Republic of China (Effective June 1, 2017). DigiChina. https://digichina.stanford.edu/work/translation-cybersecurity-law-of-the-peoples-republic-of-china-effective-june-1-2017/ Retrieved 12.4.2025

Stanford University. (2021a, June 29). Translation: Data security law of the People's Republic of China (Effective Sept. 1, 2021). DigiChina. https://digichina.stanford.edu/work/translation-data-security-law-of-the-peoples-republic-of-china/ Retrieved 12.4.2025

Stanford University. (2021b, November 1). Translation: Personal information protection law of the People's Republic of China (Effective Nov. 1, 2021). DigiChina. https://digichina.stanford.edu/work/translation-personal-information-protection-law-of-the-peoples-republic-of-china-effective-nov-1-2021/ Retrieved 12.4.2025

Tan, C. (2024, August). THE GREAT CYBERWALL: NAVIGATING CHINA'S CROSS-BORDER DATA LAWS. In Boston College Intellectual Property and Technology Forum (Vol. 2024, pp. 1-18).

Tian, X. (2016). Managing international business in China. Cambridge University Press.

Timoteo, M., Verri, B., & Nanni, R. (2023). Quo Vadis, Sovereignty? (Vol. 154).

Wang, J. Y. (2022). The best data plan is to have a game plan: Obstacles and solutions to reaching international data privacy agreements. Michigan Technology Law Review, 28(2), 385-420.

Xie, T., Liu, J., Sengstschmid, U., & Ge, Y. (2023). Navigating cross-border data transfer policies: The case of China (Research Paper #01-2023). Asia Competitiveness Institute.

Xie, Y. (2024). Legal dilemmas and paths to relief in cross-border transfers of personal data by multinational corporations. Science of Law Journal, 3(4), 111-123.

Yan, Y. (2023). The Risk-Based Approach to Personal Data Protection and the Response of the International Trade Law. Beijing L. Rev., 14, 1250.

Yu, L. (2023). The Regulation of Transborder Data Flows from the EU to China Within the Framework of China-EU E-Commerce under the GDPR.

Zhang, C. (2024). China's privacy protection strategy and its geopolitical implications. Asian Review of Political Economy, 3(1), 6.

Appendices

Appendix 1 Artificial Intelligence

In this thesis, Artificial Intelligence (ChatGPT) was used as a tool in ideation for the topic as well as to improve errors in grammar throughout the text. Artificial intelligence was initially used as a tool for ideation to discuss possible topics for a literature review, but ultimately, I decided my topic independently of this discussion.

Prompts:

- "Is this sentence grammatically correct?"
- "Would you add a comma to this sentence?"
- "Is this word spelled correctly?"
- "What are some potential topics for a literature review in the field of international business?"

Appendix 2 Abbreviations

CAC: Cyberspace Administration of China
CIIO: Critical Information Infrastructure Operators
CSL: Cyber Security Law
DSL: Data Security Law
EU: European Union
GDP: Gross Domestic Product
GDPR: General Data Protection Regulation
IoT: Internet of Things
MLPS: Multi-Layered Protection System
MNC: Multinational Corporation
PI: Personal information
PIPL: Personal Information Protection Law
USD: United States Dollar
USITC: United States International Trade Commission