electronics

MDPI

Article

Promotion and Advancement of Data Security Governance in China

Bing Chen * and Yongji Liu

Center of Competition Law, Nankai University School of Law, Tianjin 300350, China; nku_gk@mail.nankai.edu.cn
* Correspondence: bing.chen@nankai.edu.cn

Abstract: In this age of digital economy, issues relating to the data security and personal privacy of multimedia systems are increasingly manifesting in the form of unprotected data. The level of governance capability for data protection determines whether the data security and personal privacy of multimedia systems can be protected and developed in the future. In recent years, China has introduced laws and regulations on the protection of personal information, personal privacy, data security, and cybersecurity. Although data protection still needs to be improved, China has been refining the framework and provisions on data security governance through certain practices and the adoption of supporting regulations. The country aims to rapidly promote the current governance capability of data security and gradually form a good institutional environment to support international collaboration in the realm of global data security.

Keywords: data protection; personal privacy; cybersecurity; data security; promotion

Citation: Chen, B.; Liu, Y. Promotion and Advancement of Data Security Governance in China. *Electronics* **2024**, *13*, 1905. https://doi.org/10.3390/electronics13101905

Academic Editors: Cheonshik Kim and Raylin Tso

Received: 2 April 2024
Revised: 4 May 2024
Accepted: 10 May 2024
Published: 13 May 2024

1. Introduction

Information communication technology and digital computing science, such as clouding computing, big data, and artificial intelligence, while promoting social development, has also led to unprecedented risks and challenges to human society, necessitating regulation. China is the world's most populous country [1] as of December 2023, with more than 1.09 billion Internet users, and Internet penetration has increased to 77.5 percent [2]. Initially, the Internet in China was only used in the fields of education and scientific research, but the Internet has since become a necessary tool for socializing, office work, and leisure [3]. An increasing number of people are enjoying the convenience brought about by the development of digital technology. However, the issues of data security and personal privacy for multimedia systems raised by the continuous development of Internet technology have attracted increasing attention.

In recent years, the Chinese government has continued to promote digital industrialization and industrial digitization. As the digital economy has become an important part of the economy and society, data security risks have penetrated all aspects of human life and work. With the development of digital technology, the issues of security and privacy for multimedia systems concern aspects such as personal information, personal privacy, and trade secrets, which are constantly presented in the form of data. Data security issues come thick and fast, meaning they can no longer be ignored in the process of vigorously developing the digital economy in China.

Due to the emergence of computers and digital technology, information on peoples' behaviors such as accepting services, online and offline consumption, and browsing websites has been digitized, and words and actions are available in the form of data [4]. Data security and personal privacy are gradually being reflected in the form of data protection, which is particularly evident in multimedia systems [5]. The multimedia system is a representative product of the digital economy, and in terms of these systems, China's protection of privacy and information is mainly embodied in specific systems in its legislation, such as legislation

on data utilization and cross-border data flow. Therefore, the system for protecting privacy and security in China is mainly constructed based on data security.

Because personal privacy in multimedia systems is mainly reflected in data security, the key to solving this issue lies in realizing data protection. To protect data, it is necessary to constrain the behavior of using data through the formulation of laws and regulations as well as avoid risks such as data leakage through advanced technology. In this paper, we will summarize the main ideas of data protection in China by reviewing the relevant laws and regulations in China. We hope that this analysis of China's data protection strategies can provide guidelines on data protection for industry professionals. In our final analysis, we conclude that the key to solving this series of problems lies in the governance of data security.

2. China's Data Security Continues to Be Emphasized

Since the introduction of the 13th Five-Year Plan, China has continued to develop its digital economy, improved its digital infrastructure, accelerated the cultivation of new business forms and new models, and achieved positive results in promoting the industrialization of digital industries and the digitization of industries [6]. By 2023, the added value of the core industries of the digital economy accounted for 8.5 percent of China's gross domestic product, and the digital economy provided a powerful impetus for sustained and healthy economic and social development.

Various types of personal information are important sources and the main components of data. Enterprises can innovatively develop goods and provide personalized services for consumers through collecting big data. However, the collection and utilization of data should not be borderless. Data security has become an imperative concern over time in the development of the digital economy along with recurring risks like information leakage, data leakage, and privacy infringement.

With the advancement of algorithms and the increase in their arithmetic power; the continuous emergence of digital products such as instant messaging software, online shopping platforms, and online travel software; and the emergence of new products and new forms of business, the relationship between citizens and Internet platforms is becoming increasingly close. As a result, data containing users' personal information and information relating to citizens' privacy and even commercial secrets are constantly exposed to Internet platforms. In this era of the digital economy, the issue of data security and personal privacy has become particularly prominent.

The digital era has not only revolutionized traditional security and privacy protection but has also brought unprecedented challenges to security and privacy protection. Based on the characteristics of the digital era, personal privacy protection and data security issues are mutually exclusive, and the focus of the Chinese government's regulations in this field is data security governance. The key to data security governance lies in the protection of data and personal privacy, which mainly encompasses the security of personal information and privacy as well as national security issues.

One of the important features of the digital era is that data have become an important factor of production. Data are gradually becoming the ubiquitous "blood" running through cyberspace. The identities, properties, and activities of various subjects are presented in the form of data, which means that the data have multiple legal attributes. Data security refers to the concentration of personal information, privacy, and even national security, while personal information and privacy protection are specific manifestations of data security. For this reason, the governance of data security and personal privacy needs to be based on the characteristics of "data".

3. The Fundamental Legal Framework of Data Governance in China

China's digital economy has developed rapidly. New forms, modes, and industries are emerging fast, and some companies have developed into industry giants in just a few years. These companies have accumulated a large amount of data during their development,

including personal information and personal user data. Therefore, the protection of data security requires active government action.

In recent years, China has enacted and amended a series of laws, such as the Civil Code, the Data Security Law, the Cyber Security Law, and the Personal Information Protection Law, as well as regulations like the Data Exit Security Assessment, the Regulations for the Administration of Network Data Security (Draft), and the Ministry of Industry and Information Technology's Administrative Measures for Data Security in the Field of Industry and Information Technology (for Trial Implementation). Additionally, national standards such as the Information Security Technology-Personal Information Security Specification have been introduced to address the issues of data security, including personal information, privacy, and national security. Through an examination of the Chinese government's approach to data security governance, it can be found that the governance of data security is mainly reflected in the construction of institutional frameworks for data collection, data processing, data circulation, and accountability.

3.1. Focus on Improving Data-Processing Systems

Data processing is an important data activity in the digital era. It is carried out by data processors and includes the collection, storage, use, processing, transmission, provision, and disclosure of data. Data processing activities are the beginning of the circulation and utilization of data. Reasonable regulation of data processing activities can prevent the emergence of security risks. According to the Civil Code, the Personal Information Protection Law, the Data Security Law, and other laws and regulations, there are three main principles on the handling of personal information and other data and information: minimum necessary, openness and transparency, and informed consent.

3.1.1. The Principle of Minimum Necessary

In the 1970s, the U.S. Fair Information Practice Principles (FIPPs) established rules on the limitation of collection, use, and disclosure, etc., which provided the ideological source for the establishment and development of the principle of minimum necessary. China has developed similar provisions in the Civil Code, and the Personal Information Protection Law stipulates that "Personal information processing shall be based on explicit and reasonable purposes and directly related to those purposes and shall exert the minimum impacts on the rights and interests of individuals". The principle of minimum necessary is mainly focused on the type and scope of data collected, such as personal information. Collected data should be directly related to the provision of services and only collected where the purpose of the service cannot be realized without the collection of the corresponding data of the individual. Moreover, the amount of personal data collected shall be the minimum necessary for the realization of a service's purpose. In addition, the relevant service provider should be forbidden to provide services based on the excessive collection of information that is not agreed to by the provider of the personal information [7,8].

3.1.2. The Principles of Openness and Transparency

According to Article 7 of the Personal Information Protection Law, "The principles of openness and transparency shall be observed in the processing of personal information, the rules for processing personal information shall be disclosed, and the purposes, means, and scope of processing shall be explicitly indicated". In terms of the principles of openness and transparency, the case of APPs includes several aspects: first, the disclosure should be complete and include both a privacy policy and rules for the collection and use of personal information within the APP. The scope of the purpose and method of the collection and use of personal information should be made explicit. Second, these disclosed rules should be made available to the individual in an appropriate and clear way.

3.1.3. The Principle of Informed Consent

The principle of informed consent is that the information collector should obtain individuals' consent. According to article 14 of the Personal Information Protection Law, "Where personal information is handled based on individual consent, said consent shall be given by individuals under the precondition of full knowledge, and in a voluntary and explicit statement". The provisions for the principle of informed consent in China's laws and regulations can be summarized at four levels. Firstly, information handlers can only collect information after individuals have expressly consented. Handlers cannot collect information after they have explicitly indicated their refusal to consent, nor can they frequently ask for individuals' consent or interfere with individuals' normal use of the information. Secondly, individuals should be provided with the means to withdraw their consent to the collection of information. Thirdly, information should be collected in a proper manner, and users should not be misled into giving consent. Fourthly, information collection should not exceed the scope of consent. This means that collecting information beyond the scope of individuals' authorization is in violation of the applicable rules on collection.

3.2. Focus on Improving the Environment of Data Circulation

Emphasizing data security does not mean prohibiting data circulation. In terms of national policy, the Chinese government encourages data trading and circulation, as reflected in the Electronic Commerce Law and the Data Security Law. In the data industry, data circulation is also a necessary choice to unlock the value of data elements. Establishing a reasonable data circulation system is not only conducive to the prosperity of the data industry but also helps to enhance data security. At present, China's data circulation system mainly focuses on domestic and cross-border circulation.

3.2.1. Improving the Regulation of Data Localization

Economic globalization remains a major trend in the context of the digital economy. Cross-border data flows have become an important form and pathway for data and information as well as economic and trade exchanges among countries and regions. While the explosive growth of cross-border data circulation promotes the prosperity of international digital trade, it also poses challenges to the security of personal information, the development of the data industry, and even national data security. Especially after the "Prism Gate" incident of the United States in 2013, data localization has become a trend sweeping the world.

In 2017, China's Cybersecurity Law came into force. This law stipulates that personal information and important data collected and generated by operators of critical information infrastructures in their operations within China should be stored domestically. The Data Security Law, enforced in China since 1 September 2021, explicitly states that, unless approved by the competent authorities in China, organizations and individuals within the country shall not provide foreign judicial or law enforcement agencies data stored in China.

Various regulations and guidelines emphasize that personal information and important data generated within China should be stored domestically and that any data exit from the country requires approval from the national competent authorities [9]. Examples of relevant regulations and documents include the Guiding Opinions on Encouraging and Regulating the Development of Internet Rental Bicycles issued by the Ministry of Transportation and Communications (MOTC), the Administrative Measures for Scientific Data issued by the Ministry of Science and Technology (MOST), the Guidelines on Internet Personal Information Security Protection and the Guiding Opinions on Implementing the Cybersecurity Multi-Level Protection System and Critical Information Infrastructure Security Protection System issued by the Ministry of Public Security (MPS), and the Measures for Data Security Management in the Industrial and Information Sector (for Trial Implementation) issued by the Ministry of Industry and Information Technology.

3.2.2. Improvement of Regulation of Cross-Border Circulation of Data

Completely blocking the cross-border circulation and trading of data is neither in line with the legislation objective nor practically possible. Therefore, the adoption of a data localization policy meets the current practical needs. Data exit security has gained increasing attention and importance at all levels, and data security has become an important issue in national digital governance [10]. In terms of cross-border data flows, many countries have generally adopted a more conservative and strict governance model. A report by the U.S. Information Technology and Innovation Foundation (ITIF) shows that since 2017, the number of countries restricting cross-border data flows has risen from 35 to 62, and the number of data localization measures implemented has risen from 67 to 144 [11]. China is one of the main victims of data leakage and cyberattacks. According to the Report on the Analysis of China's Internet Cybersecurity Monitoring Data, released in July 2021, China's exposure to cyberattacks from abroad is becoming an increasingly serious problem posing unprecedented challenges to the sovereignty and security of national data.

Although the cross-border flow of data poses challenges to data security, the Chinese government has tried to establish a reasonable system to facilitate this process. In 2022, the State Internet Information Office published the Data Exit Security Assessment, which provides specific regulations on the management measures for exit security assessment of personal information and important data. This is an important practice for China in exploring the supervision of cross-border data flow. These regulations represent not only a detailed implementation of the provisions for data exit security assessment in the Cybersecurity Law, the Data Security Law, the Protection of Personal Information Law, and other laws and regulations, but also a key measure for the protection of China's basic strategic resources and national security in the context of internationalized data circulation and sharing [12].

After the implementation of the Data Exit Security Assessment, the first cross-border data transfer case approved under these new rules was issued by the Beijing office of the Cyberspace Administration of China (Beijing CAC). This approval pertains to a data export by the Beijing Friendship Hospital of the Capital Medical University. In this case, the data will be received by Amsterdam University Medical Center for purposes of a joint multi-center clinical research project in colorectal medicine [13].

Cross-border data flows are fundamentally made possible by the underlying system. Prior to the release of the Data Exit Security Assessment, the Cybersecurity Law, the Data Security Law, and the Personal Information Protection Law had established data exit assessment mechanisms at a preliminary level and were utilized to construct a scientific and systematic legal framework for data exit in the cyberspace field. In addition, the Chinese Government adheres to the combination of prior assessment and continuous supervision and to the combination of risk self-assessment and security assessment, providing relatively complete institutional support for the cross-border flow of data.

3.3. Focusing on the System of Assuming Responsibility for Data Security

Regarding behaviors that threaten data security, China mainly pursues responsibility for the relevant responsible parties in the three areas of civil liability, administrative liability, and criminal liability. Data security responsibilities are reflected in the Civil Code, Criminal Law, Data Security Law, Personal Information Protection Law, and other laws and regulations. The liability systems in different fields of laws and regulations jointly comprise a data security responsibility mechanism, which provides a legal basis for the pursuit of data security responsibilities.

3.3.1. Civil Liability

In terms of civil liability, the assumption of responsibility for data security is mainly embodied in the Data Security Law. The scope of civil liability under the Data Security Law mainly covers two aspects. Firstly, enterprises engaging in data-related business activities should bear civil liability for data security incidents caused by the failure to take

necessary security measures according to regulations. Enterprises engaged in data-related business activities in accordance with the provisions of Article 27 in the Data Security Law should establish and improve a comprehensive security system and take the necessary technical or other measures to protect data security. When an enterprise fails to take the necessary security measures as required and a data security incident occurs, the enterprise should bear civil liability. Secondly, individuals who damage data security should also bear civil liability. According to the provisions of the Data Security Law, an individual shall be civilly liable if he or she intentionally destroys data security; steals, alters, or destroys data; illegally uses or maliciously uses data; or illegally leaks data. Individuals may also be civilly liable if they negligently cause a data security incident to occur. In addition to these, there are provisions in the Civil Code, the Personal Information Protection Act, and other laws and regulations on the infringement of personal information, personal privacy, and other forms of data security.

3.3.2. Administrative Liability

In addition to civil liability, administrative authorities can take administrative enforcement measures to impose administrative penalties for violations of data security. After the promulgation and implementation of the Cybersecurity Law, a large number of administrative enforcement cases related to data security have been published by administrative authorities such as the Cyberspace Administration of China. Among administrative responsibilities, the issue of data security can be categorized into the national level of safeguarding data sovereignty, enhancing competitiveness of enterprises, the development of the digital economy, and the individual level of safeguarding the rights of personal data [14].

Firstly, at the level of national data sovereignty and data security, data handlers have failed to comply with regulations on the security of data transactions and have provided important data to parties outside the country without authorization. Some of the data collected by enterprises may belong to important state intelligence, and the leakage of such data will seriously jeopardize national security. Therefore, the data classification regulations need to be improved, and the protection of data needs to be strengthened.

Secondly, at the level of enterprise data security, the data security guarantee obligations affect data processors, particularly platform enterprises, and include the three dimensions of establishment of a data security management system, fulfillment of the obligation to protect personal information rights, and cooperation with supervisory authorities [15]. When enterprises fail to fulfill their obligations to build a data security management system or to fulfill their obligations to protect personal information rights, the administrative authorities can impose corresponding penalties.

Finally, at the level of personal information, in the Internet sector, companies are prone to data security problems due to the over-collection of sensitive personal data, which mainly include names, genders, identity card numbers, and medication use. In China, if a data processor fails to fulfill its data security obligations; fails to take technical measures such as anti-tampering, anti-leakage, and anti-intrusion practices; and fails to take technical protection measures such as de-identification and encryption of sensitive data, leading to data leakage or the risk of data leakage, the law enforcement authorities may penalize such acts in accordance with the Data Security Law.

3.3.3. Criminal Liability

At the level of criminal liability, China has mainly adopted the approach of combining criminal law and non-criminal law regulation. The Criminal Law and judicial interpretations can be broadly categorized into two methods of regulating crimes involving data security: firstly, based on the essential attributes of the data, they are protected as information; secondly, based on the technical characteristics of the data, they are protected as an intrinsic part of the computer system. The former mainly includes crimes such as stealing, spying, bribing, and illegally providing state secrets and intelligence to an organization, institution, or personnel outside the country; infringing on trade secrets; infringing on

citizens' personal information; and illegally deleting, altering, or adding data or applications installed in or processed and transmitted by computer systems. The latter mainly includes the crimes of destroying computer information systems and failing to perform the obligation of information network security management.

At the level of non-criminal laws and regulations, in addition to the regulation of behaviors endangering data security in criminal laws and regulations represented by the Criminal Law, subsidiary criminal law norms in non-criminal laws, such as the Data Security Law, contain relevant provisions on related behaviors. According to Article 45 of the Data Security Law, data handlers who violate the data management system and jeopardize the country's sovereignty, security, and development interests will also face criminal liability.

4. Data Security Governance Practices in Mainland China

Over the past decade, China's efforts in addressing data security issues have led to certain achievements at the level of institutional construction. With the implementation of relevant laws and regulations, the Chinese government has also accumulated a wealth of practical experience in data security governance. China has increasingly focused on data security and personal privacy protection, governing data security issues from three perspectives: legislation, law enforcement, and justice.

4.1. Legislative Practice and Achievements

In legislative practice, China has continuously insisted on improving relevant laws and regulations to provide more comprehensive protection for data security, which is now mainly reflected in the Civil Code, Criminal Law, Data Security Law, Personal Information Protection Law, Cybersecurity Law, and other legislation. As mentioned above, China has regulated the infringement of data security at different levels in the laws and regulations on civil, administrative, and criminal liability, and the promulgation and implementation of the Data Security Law has filled the gap in China's data security legislation and pointed out the development direction for the establishment of a sound data security governance system. There are some differences between the Data Security Law and the Personal Information Protection Law. The Data Security Law aims to safeguard data security in terms of national security and social public interests. The Personal Information Protection Law, on the other hand, focuses on the security of personal information and private rights and interests and is designed to safeguard the privacy, personality, property, and other interests of individual citizens. The two laws complement each other and improve China's protection of various types of data.

At the legislative level, China has also focused on strengthening the connection between specific systems and the overall governance framework. This effort includes reinforcing connections with the Cybersecurity Law and other laws in terms of basic definitions, data security management, data categorization and classification, and the exit of important data in order to improve the construction of China's legal system for data governance.

4.2. The Administrative Law Enforcement and Improvement

The issue of data security is fundamental to the development of the digital economy, and this view is particularly evident in law enforcement practices involving data security. In the context of the digital economy, one of most significant features of platform operators is their possession of massive amounts of data, and the manner in which platform enterprises handle and utilize data impacts whether data security can be protected. With regard to administrative enforcement practice, on 21 July 2022, China's National Internet Information Office imposed a fine of over CNY 8 billion (USD 1.19 billion) on the ride-hailing giant Didi Global Inc (DiDi) in accordance with the Cybersecurity Law, the Data Security Law, the Personal Information Protection Law, and the Administrative Penalties Law. It marked the highest fine imposed in China on an operator for a violation of data security.

These illegal activities mainly include the illegal collection of 11.9639 million pieces of screenshot information from users' mobile phone photo albums, excessive collection of

8.323 billion pieces of user clipboard and application list information, excessive collection of 167 million pieces of precise location information, inaccurate and unclear explanation of 19 personal information handling purposes, and other illegal activities [16]. In this case, China's ride-hailing giant DiDi was fined a hefty amount for data security, which is emblematic of data security governance in China. As a result, some scholars believe that China is setting up barriers and trying to block the flow of data in China. However, in practice, while China has made many decisions on data security penalties in recent years, high fines are uncommon. The Chinese government is more accustomed to using more lenient methods such as warnings, with the hope that these minor penalties will promote the development of corporate compliance and ultimately realize the protection of information, privacy, and other data [17].

Since 2021, China's various law enforcement departments have overseen the field of data security. In September 2023, on the second anniversary of the effective implementation of the data security law, some scholars compiled a list of 28 cases that had been publicly released. The reasons for penalization were divided into four main categories. Firstly, the largest number of cases were penalized for failing to fulfill data security obligations, with a total of 24 cases. Failure to fulfill data security obligations resulted in the risk of data leakage, and there were also cases in which it was not clear whether data had been leaked or not. Secondly, in the relevant cases, two involved infringement of national security, and a number of laws and regulations were combined to make a judgment. Thirdly, there was one case in which no effective measures were taken for data leakage. Fourthly, one case of failure to cooperate with the relevant authorities in retrieving relevant data was recorded. This shows that in terms of data security, the largest proportion of data processors were penalized for their own actions. Therefore, it is necessary and urgent for data processors to understand the relevant laws and regulations on data security [18].

In addition, the establishment of China's National Data Bureau in 2023 has marked a new stage in China's efforts to utilize, protect, develop, and regulate data elements. It also means that the administrative authorities will continue to enhance Cybersecurity Law enforcement in the field of data security. The main problems of law enforcement in the field of data security that will be addressed include platform operators engaging in the serious unlawful collection and use of personal information through coercion, enticement, fraud, and other illegal means. Additionally, attention will be directed towards operators failing to carry out security assessments as required and having potential security problems, among other issues.

4.3. Judicial Practice and Emphasis

In judicial practice, China's governance of data security is mainly reflected in the punishment for such crimes. These data-related crimes include a wide range of criminal acts relating to personal information and privacy rights. In the literature, the scope of "data" as the object of crimes includes not only traditional property such as virtual network property and cryptocurrency, which are associated with property crimes, but also personal information such as candidate information and household registration information, which can be used to identify specific individuals. There is an overlap between data-related crimes and traditional crimes in terms of the scope of infringement, such as the act of generating virtual currencies for profit by cracking the instruction codes of virtual currency service providers [19] or the act of collecting victims' personal information (including users' names, ID numbers, bank card numbers, and phone numbers) through database cracking [20].

Although laws such as the Data Security Law and the Personal Information Protection Law have their own focus on protecting different types of data in their legislation, the concept of "data" is often interpreted broadly in the context of data crimes. This is because personal information and privacy are often stored as "data", and there is an overlap between the various concepts. Especially in the digital age, the intertwining of data and personal information, privacy, and even national security are becoming increasingly obvious, making it is difficult to distinguish them in judicial practice. Moreover, the protection of the rights

and interests of individuals is categorized as the protection of data security, which is also the path of the current judicial practice in Mainland China.

Through a brief review of China's legislation, administrative law enforcement, and judicial practice, we can find that China is constantly improving its laws and regulations at the legislative level in an attempt to ensure data security institutionally. However, even with legal provisions in place, there have still been many incidents in China that jeopardized data security because data processors did not handle data in accordance with laws and regulations.

5. The Promotion of China's Data Security and Privacy Protection

By reviewing China's practical experience in data security, it can be found that China attaches great importance to data protection. Although China has made many efforts in the realm of data security, there are still areas that need to be improved, such as further optimization of the legal level and improvement of the basic theory system of data.

5.1. Improvement of Laws and Regulations

In recent years, China has actively explored the field of data security and has regulated data security issues, including personal information, privacy protection, and national security, through legislation. The enactment and implementation of a series of laws and regulations, such as the Civil Code, the Personal Information Protection Law, and the Cybersecurity Law, have effectively solved some of the data security problems that need to be addressed and have provided a good framework for the rule of law in the development of the data industry. However, in practice, there are still many areas that need to be optimized and improved in order to address data security issues.

Regarding legislative refinement, the Data Security Law, for example, still needs to be strengthened in terms of clarifying the main security risks faced by each type of data exit as well as fine-grained governance. Furthermore, there are deficiencies in dynamically responding to changes in internal and external data security risks [21]. Although the Data Security Law puts forward principles for designing a security risk system for data flows, it does not provide targeted measures for security risks in these processes. In terms of the interconnectivity of laws, while the Civil Code, the Criminal Law, the Data Security Law, and the Personal Information Protection Law all pay regard to data security issues, the interface among civil and criminal law is unclear, ultimately resulting in challenges in effectively addressing certain violations.

5.2. Improving the Data Infrastructure

5.2.1. Improvement of Data Grounded Theory

To some extent, the imperfect, data-related, fundamental institutions allow technology-based data handlers to collect, analyze, and use data arbitrarily, which contributes to data security risks and privacy infringement. The lack of clarity on the legal attributes of data has made it impossible for regulators to effectively regulate issues related to data security. Therefore, it is necessary to explore the foundational theory system of data. Liu Liehong, the head of NDB, remarked at a forum at the second Global Digital Trade Expo that the administration is pressing ahead with a series of measures, such as improving the basic systems for data; promoting the circulation, transaction and utilization of data; bolstering data infrastructure construction; advancing research of key technologies in the data field; and strengthening data security governance. Subsequently, on 4 January 2024, the National Data Bureau collaborated with relevant departments to explore the implementation of a "Data Element X" plan for 2024–2026. These initiatives are important to bringing the digital economy into a deeper stage of development and to providing theoretical foundational support for data security.

5.2.2. Improvement of Data Classification Regulations

According to the requirements of Article 21 of the Data Security Law, "The State is to establish a categorized and graded protection system for data. This system is designed to implement protection based on the importance of data in economic and social development, as well as the degree of danger to national security, public interests, or the lawful rights and interests of individuals or organizations, if data was altered, destroyed, leaked, or illegally obtained or used". The Practice Guidelines for Cybersecurity Standards—Guidelines for Network Data Classification and Grading subsequently classified data into three levels according to importance, namely, ordinary data, important data, and core data. However, since general data cover a wide range, the same level of protection may not be able to meet the security needs of different types of data. Data handlers prioritize classification based on the basic framework provided. They can also refine the grading of general data by combining the industry data classification rules and the organization's production and operation needs.

However, there are also many challenges in the implementation of the regulations of data classification. For example, Article 40 of China's Constitution establishes a strict system for the protection of private communications which is mainly regulated by telecommunication carriers and state organs. Despite this, modern Internet communication tools and exchange platforms form the problem that the content of communications can be easily forwarded, and the boundaries between the dissemination of private communication and public information are unclear. This ambiguity is not conducive to the establishment of a security and protection order that is appropriate for different types of data. Therefore, it is necessary to distinguish between private communications and public information in Internet communication scenarios to make it easy for network operators and users to clarify the private or public attributes of the network socialization scenarios in which they are engaged. This would facilitate the establishment of strict confidentiality norms for private communications and orderly management of public information in accordance with the idea of categorization and management [22].

5.3. Improvement of Supporting Measures

To solve the current data security problems, we not only need to continue to improve the laws and regulations, consolidate the basic theory of data, and optimize and innovate the regulatory measures, but also strengthen the data-related infrastructure facilities to meet the urgent requirements for secure data flow.

Firstly, data resources and data products in the current market are complex and diverse and should be categorized based on data attributes, importance, risk level, and other factors.

Secondly, the digital property right system guaranteeing rights and interests and compliant use can be established. A system with the structural separation of data property rights is at the core of this concept. According to Opinions of the CPC Central Committee and the State Council on Establishing a Data Base System to Maximize a Better Role of Data Elements, a classified and hierarchal ownership affirmation and authorization system for public data, corporate data, and personal data shall be established. According to the characteristics of data sources and data generation, the legal rights enjoyed by each participant in the process of data production, circulation, and use shall be defined, and a property rights operation mechanism with ownership of data resources shall be implemented. An example of this progress can be seen in Shenzhen, Guangdong Province, where Data Exchange Management Regulations (for Trial Implementation) were released at the municipal level. Shenzhen has taken the lead in exploring the concrete practice of structural separation of data property rights and standardizing the data exchange mechanism [23].

Finally, focus should be placed on a compliance data exchange system. The compliance data exchange system is the key for optimizing the data circulation environment and strengthening data security, especially the system for cross-border data flow, which is even more important in the context of the current data security game among countries.

Compliance and security are the red lines of data exchange, and a security compliance system can reduce the risk of leakage of personal information and national secrets.

5.4. Building a Multifaceted Governance System and Implementation Framework

China has insisted on multifaceted governance and established a hierarchical structure of policies and regulations at the central, sectoral, and local levels. An organizational structure has been formed in which the central authorities take the lead and industry sectors specialize in management. At the national sector level, ministries and commissions such as the Ministry of Agriculture and Rural Affairs, the Ministry of Water Resources, and the Ministry of Science and Technology have formulated and issued guidance for the development of the big data industry and the industries and fields under their jurisdictions, while the Ministry of Industry and Information Technology (MIIT) and the Development and Reform Commission (DRC) have focused on the development of the big data industry, the hierarchical classification of data, and other areas to develop relevant documents and a policy system [24].

In practice, because of the deep integration of digital data technology and human production and the significant and profound impact this has had on economic development, social governance, and people's lives, it is necessary to adopt multifaceted governance. The structure of subjects covered by the digital economy has become increasingly complex, especially with the cross-border integration and cross-interconnection of data, and government agencies, social organizations, market entities, and citizens are all closely related to big data security. Data security not only involves individuals, enterprises, and other organizations but also the state and government. Therefore, data security concerns not just one but multiple subjects. In other words, data security not only needs to be guaranteed by the state and government in the process of governance but also needs to be jointly maintained by enterprises, citizens, and other subjects.

6. Summary

As far as data security and privacy protection are concerned, it is necessary to prevent technical security problems, but the pursuit of technological perfection alone must avoid the fallacy of composition if it is to completely guarantee data security. This is because unilateral emphasis on technological perfection may lack innovation and effectiveness, and data security cannot be realized at the macro level. In this circumstance, it is necessary to strengthen the top-level design and continuously guide the development of technology by improving laws and regulations so as to achieve data security as a whole.

By analyzing the path of data security governance in China, it can be found that the accidents that pose damage to data security in China are not only caused by technical problems but also data processors who do not operate in accordance with the laws. Regarding data security, technicians should not only ensure data security at the technical level but also have a deep understanding of the laws and regulations of each country that the development and innovation of technology should follow.

Through a review of Chinese laws and analysis of relevant cases, it can be found that China is attempting to establish strict data security measures for various multimedia systems, but at the same time, it is still very supportive of the development of data-related industries. For example, even in the cross-border flow of data, which is a risky data security issue, the Chinese government is actively exploring the best solution. It is clear that China does not reject the innovation and development of multimedia systems and will continue to support them in the future. In this circumstance, it is necessary for system developers to understand and comply with laws and regulations in order to design a secure system program.

In summary, data security, whether at the national level, social level, or individual level, has an extremely close relationship with national sovereign security, social stability, individual rights, and interests, among other issues. On the one hand, data security is more closely linked to personal information, personal privacy, national security, and other

relevant issues, making it the centralized manifestation of these issues. On the other hand, data as a carrier of various types of information, given their non-exclusivity and renewability, have posed greater challenges to data security. Effective management of data security issues requires not only the continuous improvement of the theoretical system but also a set of laws and regulations covering data collection, utilization, circulation, and other aspects of the system.

Author Contributions: Conceptualization, methodology, writing—original draft preparation, project administration, funding acquisition, B.C.; data curation, Y.L.; writing—review and editing, B.C. and Y.L. All authors have read and agreed to the published version of the manuscript.

Funding: This research was funded by the major project in Judicial Research of the Supreme People's Court of P.R.C. (grant number ZGFYZDKT202317-03) and the key project of Humanities and Social Science study from the Ministry of Education of P.R.C. (grant number 19JJD820009).

Data Availability Statement: All data underlying the results are available as part of the article and no additional source data are required.

Conflicts of Interest: The authors declare no conflicts of interest.

References

1. Kanem, N. *State of the World Population Report 2023*; United Nations Population Fund: New York, NY, USA, 2023.
2. Li, F.D. The Comprehensive Strength of China's Internet Industry has Increased Significantly. Economic Daily. Available online: http://paper.ce.cn/pc/content/202404/19/content_293164.html (accessed on 23 April 2024).
3. Bu, Y. Internet Users Exceed 1.079 Billion, Thousands of Industries 'Touch the Internet' Digital Economy for China to Inject Vigorous Momentum. China National Radio. Available online: https://finance.cnr.cn/ycbd/20230829/t20230829_526401178.shtml (accessed on 21 April 2024).
4. Schneier, B. *Data and Goliath: The Hidden Battles to Collect Your Data and Control Your World*; W. W. Norton & Company: New York, NY, USA, 2015.
5. Li, S.H. Legislative Responses to the Protection of Privacy in the Digital Age. *Law Sci.* **2024**, *508*, 17–31.
6. Department of Development Planning. *A Plan to Facilitate Development of the Digital Economy in the 14th Five-Year Plan Period (2021–2025)*; National Development and Reform Commission: Beijing, China. Available online: https://www.ndrc.gov.cn/fggz/fzzlgh/gjjzxgh/202203/t20220325_1320207.html?eqid=dd629fc70007c70700000006645ddddd (accessed on 21 April 2024).
7. Fan, W. Reconstructing the Path of Personal Information Protection in the Age of Big Data. *Glob. Law Rev.* **2016**, *38*, 92–115.
8. Wu, T. Application of the principle of data minimization to the platform's practice of handling personal information. *Chin. J. Law* **2021**, *43*, 71–89.
9. Liang, Y. Divergences, causes, and consequences of U.S.-China global data governance. *J. Nanjing Univ. Posts Telecommun. (Soc. Sci.)* **2024**, *26*, 41–50.
10. Dong, K.; Wu, J.C.; Ma, T.C. Research of Outbound Data Transfer Security Risk Element System in China. *Inf. Stud. Theory Appl.* **2024**. Available online: https://link.cnki.net/urlid/11.1762.G3.20240115.1347.004 (accessed on 1 April 2024).
11. Nigel, C.; Luke, D. How Barriers to Cross-Border Data Flows are Spreading Globally, What They Cost, and How to Address Them. ITIF. Available online: https://itif.org/publications/2021/07/19/how-barriers-cross-border-data-flows-are-spreading-globally-what-they-cost/ (accessed on 1 April 2024).
12. Chen, B. Data outbound security governance ushers in new regulations. In *Explaining the Logic of Multidimensional Governance in the Digital Economy*; China Legal Publishing House: Beijing, China, 2022; pp. 45–51.
13. Propaganda Office. The First Approved Data Exit Safety Assessment Case in China Landed in Beijing Friendship Hospital. Beijing Friendship Hospital. Available online: https://www.bfh.com.cn/Html/News/Articles/5797.html (accessed on 1 April 2024).
14. Xu, D.Q. On the rule of law in regulating corporate two-way compliance of exit data Flows. *Orient. Law* **2020**, 185–197.
15. Zhang, H.L. Platform's date security obligation in data production. *Leg. Forum* **2021**, *36*, 46–57.
16. Webster, G. Translation: Chinese Authorities Announce $1.2B Fine in DiDi Case, Describe 'Despicable' Stanford University. Data Abuses. Available online: https://digichina.stanford.edu/work/translation-chinese-authorities-announce-2b-fine-in-didi-case-describe-despicable-data-abuses/ (accessed on 21 April 2024).
17. National Engineering Research Center for Information Security. Second anniversary of the Data Security Law. Tianjin Intellectual Property Protection Center. Available online: https://www.tjippc.cn/view/article/558fdf60d79f4b9d9498d54a0300fdca.html?categoryId=hyxw (accessed on 3 May 2024).
18. Zheng, X. Read the Second Anniversary of the Data Security Law. 21st Century Business Herald. Available online: https://m.21jingji.com/article/20230901/herald/fe4bd5cfaa534bff75c0402f2255416e.html (accessed on 3 May 2024).
19. *Case of Destroying Computer Information System*; Criminal Initial Litigation: Pizhou, China, 2020.
20. Han, J.Y. *The Judicial Dilemma of Data Crime and the Way Forward for Its Governance*; The Yangtze River Delta Jurisprudence Forum: Shanghai, China, 2022; pp. 185–197.

21. Hong, Y.Q. The logical deconstruction and institutional construction of China's data security legislation. *Law Sci. Mag.* **2023**, *44*, 38–53.
22. Liu, Y. Improve Data Classification Regulations and Data Security Legislation. Cyberspace Administration of China. Available online: https://www.cac.gov.cn/2020-09/28/c_1602854536494247.htm (accessed on 1 April 2024).
23. Lin, S. China to Introduce 'Data Element X' Plan to Unlock Data's Multiplier Effects in Diverse Scenarios: Official. Global Times. Available online: https://www.globaltimes.cn/page/202311/1302484.shtml (accessed on 1 April 2024).
24. Zhang, L.; Bian, J. An analysis of data governance strategies against the backdrop of digital economy. *Macroecon. Manag.* **2022**, *2*, 35–41.