Article

Not peer-reviewed version

The Path to Data Protection Governance in China Mainland

Bing Chen * and Yongji Liu

Posted Date: 24 April 2024

doi: 10.20944/preprints202404.0357.v3

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

 doi:10.20944/preprints202404.0357.v3

Article

The Path to Data Protection Governance in China Mainland

Bing Chen * and Yongji Liu

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

Abstract: In the age of the digital economy, the data security and personal privacy for multimedia systems issues are increasingly manifested in the form of data. The level of data protection governance capability determines whether the data security and personal privacy of multimedia systems can be protected. In recent years, China has introduced laws and regulations on the protection of personal information, personal privacy, data security, and cyber-security. Although data protection is still to be improved, China has been refining the provisions on data security management through practice and the adoption of supporting regulations.

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

1. Introduction

The regulation of Internet technology with artificial intelligence, social media, big data and other technologies, while promoting social development, has also brought unprecedented risks and challenges to human society. Today, China remains the world's most populous country [1], by December 2023, with more than 1.09billion Internet users. Meanwhile, internet penetration had increased to 77.5 percent [2]. From the beginning of the Internet in China was only used in the field of education and scientific research, but nowadays, the Internet has become a necessary tool for socializing, office and leisure [3]. More and more people enjoy the convenience brought by the development of digital technology. However, the data security and personal privacy for multimedia systems issues brought about by the continuous development of Internet technology have attracted more and more attention.

In recent years, the Chinese government continues to promote digital industrialization and industrial digitization. As the digital economy has become an important part of the economy and society, the data security risks have penetrated into all aspects of human life and work. With the development of digital technology, the issue of security and privacy for multimedia systems such as personal information, personal privacy, and trade secret are constantly presented in the form of data. Finally, data security issues come thick and fast, making it is no longer ignorable in the process of vigorously developing the digital economy in China.

After the emergence of computers and digital technology, human beings' behaviors such as accepting services, online and offline consumption, and browsing websites have been digitized, and their words and deeds are basically available in data [4]. The data security and personal privacy are gradually reflected in the form of data security, which is particularly evident in multimedia systems [5]. The multimedia is a representative product of the digital economy, and in term of multimedia system, China's protection of privacy and information is mainly embodied in specific systems in legislation such as data utilization and cross-border data flow. Therefore, the protection system of privacy and security in China is mainly constructed based on data security.

Due the data security and personal privacy for multimedia systems are mainly reflected in data security, it is the key to solving it lies in realizing data security. For the protection of data security, in addition to the need to avoid risks such as data leakage through advanced technology, it is also necessary to constrain the behavior of using data through the formulation of laws and regulations. In

 doi:10.20944/preprints202404.0357.v3

this paper, we will summarize the main ideas of data protection in China by sorting out the relevant laws and regulations in China, and hope that China's data protection strategy can provide guidelines on data protection for technicist. In the final analysis, the key to solving this series of problems lies in the governance of data security.

2. China's Data Security Continues to be Emphasized in Mainland

Since the 13th Five-Year Plan, China has continued to develop the 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 is account 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.

At the same time, various types of personal information are important sources of data and the main component. Enterprises can achieve the innovative development of goods, and provide personalized services for consumers through collecting massive data. However, the collection and utilization of data should not be borderless. Coupled with recurring risks like information leakage, data leakage, privacy infringement, and so onfrom time to time, data security has become an imperative concern in the development of the digital economy.

With the advancement of algorithms, the increase of 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 getting closer and closer. As a result, data containing users' personal information, citizens' privacy and even commercial secrets are constantly exposed to Internet platforms. In the 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 also brought unprecedented challenges to security and privacy protection. Based on the characteristics of the digital era, data security and personal privacy protection, along with data security issues are mutually exclusive, and the focus of the Chinese government's regulation of data security and personal privacy protection is data security governance. The key to data security governance lies in the protection of data security and personal privacy, which mainly encompasses the security of personal information, privacy security, and national security issues.

One of the important features of the digital era is that data have become an important factor of production. Nowadays, data is gradually becoming ubiquitous and pervasive, and becoming the "blood" of active beating in cyberspace. In fact, the identities, properties, and activities of all kinds of subjects are presented in the form of data, which determines that the data has multiple legal attributes. Data security is 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 characteristic of "data".

3. The Fundamental Legal Framework of Data Governance in China Mainland

China's digital economy has developed rapidly. New forms, modes, and industries emerging thick and fast, and some platform companies has developed into industry giants in just a few years. These companies have accumulated a large amount of data during their development, including a lot of personal information, user personal data, and other sensitive information. 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)*, the *Ministry of Industry and Information Technology of Issuing the Administrative Measures for Data Security in the Field of Industry and Information Technology (for Trial Implementation)*. Additionally,

 doi:10.20944/preprints202404.0357.v3

national standards such as the *Information Security Technology-Personal Information Security Specification* have been introduced to address the issue of data security, including personal information, privacy, national security. Through an examination of the Chinese government's approach on data security governance, it can be found that its governance of data security is mainly reflected in the construction of the institutional frameworks for data collection, data processing, data circulation, and accountability.

3.1. Focus on Improving Data-Processing Systems

Data processing is the most important data activity carried out by data processors in the digital era, which 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 avoid the emergence of security risks from emerging at the root. 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 handling of personal information and other data and information: The principle of minimum necessary, the principles of openness and transparency, and the principle of informed consent.

3.1.1. The Principle of Minimum Necessary

In the 1970s, the U.S. Fair Information Practice Principles (FIPPs) established rules on collection limitations, use limitations, disclosure limitations, etc., which provided the ideological source for the establishment and development of the principle of minimum necessary. China has made similar provisions in the *Civil Code* and the *Personal Information Protection Law* atipiullates, " 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 focus on the type and scope of data collected, such as personal information, shall be directly related to the provision of services, and 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 the services's purpose. In addition, the relevant service subject shall not 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 mainly 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 through an appropriate way so that users can understand them conveniently.

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 about 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 to it. Handlers cannot collect information after they have explicitly

 doi:10.20944/preprints202404.0357.v3

indicated their refusal to consent to it, 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 and ways 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 in violation of the applicable rules on collection announced.

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 fact, 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

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

In 2017, China's *Cybersecurity Law* came into force, which 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 in 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 or important data generated within China should be stored domestically require approval from national competent authorities for any data exit from the country [9]. For example, 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), the Measures for Data Security Management in the Industrial and Information Sector (for Trial Implementation) issued by the Ministry of Industry and Information Technology, and other relevant regulations and documents.

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

Completely blocking the cross-border circulation and trading of data is neither in line with the objective law nor practically possible. Therefore the adoption of a data localization policy meets the current practical needs. The data exit security has gained more and more attention and importance at all levels, and data security has become an important issue in national digital governance [10]. In terms of data flows, many countries have generally adopted a more conservative and strict governance model for cross-border data flows. A report by the U.S. Information Technology and Innovation Foundation (ITIF) shows that since 2017, the number of countries restricting cross-border

 doi:10.20944/preprints202404.0357.v3

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 cyber-attacks. According to the Report on Analysis of China's Internet Cybersecurity Monitoring Data, released in July 2021, China's exposure to cyberattacks from abroad the country is becoming an increasingly serious problem, posing unprecedented challenges to sovereignty and security of national data are facing unprecedented challenges.

Although cross-border flow of data brings challenges to data security protection, the Chinese government has tried to establish a reasonable system to facilitate cross-border data flow. 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 to explore the supervision of cross-border data flow, which is not only a detailed implementation of the provisions about data exit security assessment in the *Cybersecurity Law*, the *Data Security Law*, and 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 background 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 has been issued by the Beijing office of the Cyberspace Administration of China (Beijing CAC) has approved the first cross-border data transfer case under these new rules. 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].

The fact that data can realize cross-border flows lies fundamentally in the assurance of 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 constructed a scientific and systematic legal framework for data exit in 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 a 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 build 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 *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 shall bear civil liability for data security incidents caused by failure to take necessary security measures by regulations. Enterprises engaged in data-related business activities in accordance with the provisions of Article 27 in the *Data Security* Law shall 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 shall 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, or illegally uses or maliciously uses data, or illegally leaks data. Moreover, individuals may also be civilly liable if they negligently

 doi:10.20944/preprints202404.0357.v3

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 infringement of personal information, personal privacy and other data security.

3.3.2. Administrative Liability

In addition to civil liability, administrative authorities can also 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 about 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, the enhancing of the competitiveness of enterprises, the promotion for the development of the digital economy, and the individual level of safeguarding the rights of personal data [14].

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

Finally, at the level of personal information, in the Internet sector, platform companies are prone to data security problems due to the over-collection sensitive personal data, which mainly includes names, genders, identity card numbers and medication use. In China, if a data processor fails to fulfill its data security protection obligations, fails to take any technical measures such as anti-tampering, anti-leakage and anti-intrusion, and fails to take technical protection measures such as de-identification and encryption measures for sensitive data, which lead 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 ways 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 the crimes such as stealing, spying, bribing and illegally providing state secrets and intelligence for an organization, institution, or personnel outside the country, infringing on trade secret, infringing on citizens' personal information, and illegally deleting, altering, or adding the data or application programs installed in or processed and transmitted by the computer systems, while 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*, also 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.

 doi:10.20944/preprints202404.0357.v3

4. Data Security Governance Practices in China Mainland

Over the past decade, China's efforts in addressing data security issues have not only made certain achievements at the level of institutional construction but also. With the implementation of relevant laws and regulations, the Chinese government has also accumulated a wealth of practical experience in data security governance. As China's attention to data security and personal privacy protection continues to deepen, China has responded in the process of governing data security issues from three latitudes: 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 legislations. 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 protection 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*. Moreover, 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 is more focused on 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.

In addition, 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, a view that is particularly evident in law enforcement practices involving data security. In the context of the digital economy, one of most significant features of the platform operators is the possession of massive amounts of data, and the manner in which platform enterprises handle and utilize data impacts whether data security can be protected. In administrative enforcement practice, on July 21, 2022, China's National Internet Information Office imposed the fine of over 8 billion yuan ($1.19 billion) on ride-hailing giant Didi Global Inc 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 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].

Since 2021, China's law enforcement departments at all levels of net information and other law enforcement agencies have carried out law enforcement in the field of data security in accordance with the law. In response to the serious problem of illegal collection and use of personal information by dozens of mobile apps such as Didi, notified platform operators notified to take down the relevant apps in accordance with the law, and were required the relevant operators to strictly comply with the legal requirements for safeguarding the security of users' information.

 doi:10.20944/preprints202404.0357.v3

In addition, the establishment of China's National Data Bureau in 2023 marks 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. Main problems of law enforcement in the field of data security that will be addressed, which include that platforms operators engage in a serious illegal and unlawful collection, and use of personal information through coercion, enticement, fraud, and other illegal means. In addition, Additionally, attention will be directed towards operators fail to carry out security assessments as required and having potential security problems, among other things will be focused on.

4.3. Judicial Practice and Emphasis

In the judicial practice, China's governance of data security is mainly reflected in the punishment of crimes related to data security. These data-related crimes generally include a wide range of criminal acts relating to personal information, privacy rights and other legal good. Through searches, the scope of "data" as the object of crimes includes not only traditional property such as network virtual property and cryptocurrency, which are associated with property crimes, but also personal information such as candidate information and household registration information, which can identify specific natural individuals. There is an overlapping 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 [17]. Or the act of collecting victims' personal information (including users' name, ID number, bank card number, and phone number, by database cracking) through database cracking [18].

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 carried as "data", and there is an overlapping between the various concepts. The concept of "data" is often interpreted broadly. Especially in the digital age, the intertwining of data and personal information, privacy and even national security are becoming more and more obvious, making it is difficult to distinguish them in judicial practice. Moreover the protection of the rights and interests of all of them is categorized under the protection of data security, which is also the path of the current judicial practice in China Mainland.

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 are still many incidents in China that jeopardize data security because data processors do not handle data in accordance with laws and regulations.

5. China's Data Security and Privacy Protection Path

By sorting out China's practical experience in data security, it can be found that China attaches great importance to data security protection. Although China has made many attempts in 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, national security and many other issues 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 rule of law for the development of the data industry. However, in the process of practice, there are still many places that need to be optimized and improved in order to address the data security issues.

 doi:10.20944/preprints202404.0357.v3

In terms of 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 in terms of fine-grained governance. Furthermore, there are deficiencies in terms of dynamically responding to changes in internal and external data security risks [19]. Although the *Data Security Law* puts forward principled requirements for designing a security risk system in the flow of data, it does not put forward targeted measures for security risks in the process of data flow. In terms of interconnectivity of laws, despite *Civil Code*, the *Criminal Law*, the *Data Security Law*, and the *Personal Information Protection Law* are all reflected in respect of data security issues, but the interface among the civil, criminal and criminal law is not very smooth, ultimately resulting in challenges in effectively addressing certain violations.

5.2. Improving the Data Infrastructure

5.2.1. Improvement of Data Grounded Theory

At some level, the imperfect data-related fundamental institutions allow technology-based enterprises to collect, analyze, and use data arbitrarily, which contribute to data security risks and privacy infringement. The lack of clarity about 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, made the remarks at a forum at the second Global Digital Trade Expo. He said that the administration is pressing ahead with a series of works, 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 January 4, 2024, the National Data Bureau collaborate with relevant departments to explore the implementation of a "Data Element X" plan for 2024-2026. These initiatives are important to bring the digital economy into a deeper stage of development and to provide 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." Subsequently, the *Practice Guidelines for Cybersecurity Standards — Guidelines for Network Data Classification and Grading* subsequently promulgated classify data into three levels according to its importance: namely, ordinary data, important data and core data. However, since general data covers a wide range of data, the same level of security 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, combining with the industry data classification rules or the organization's production and operation needs to refine the grading of general data.

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. But modern Internet communication tools and exchange platforms form the problem that the content of communications can be easily forwarded, and the boundaries between private communication contacts and public information dissemination 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, making it easy for network operators and users to clarify the private or public attributes of the network socialization scenarios in which they are engaged. Subsequently, it would facilitate the establishment of strict confidentiality norms for private

 doi:10.20944/preprints202404.0357.v3

communications and orderly management of public information in accordance with the idea of categorization and management [20].

5.3. Improvement of Supporting Measures

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

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

Secondly, in establishing a data property rights system guaranteeing rights and interests and compliant use. The system of structural separation of data property rights is at the core. 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 respectively, and a property right 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 [21].

Finally, the 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 the 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

In terms of multifaceted governance, China has insisted on multifaceted governance. First of all, China has established a hierarchical structures 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 big data industry around the industries and fields under their jurisdiction, 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 and the hierarchical classification of data, and other areas to develop relevant documents and a policy system [22].

In practice, because of the deep integration of digital data technology and human production and life has had a significant and profound impact on economic development, social governance and people's lives, it is necessary to adopt multifaceted governance. Especially, with the cross-border integration and cross-interconnection of data, the structure of subjects covered by the digital economy has become increasingly complex, 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 involves the state and government. Therefore, data security is not only the affairs of one subject, but also the affairs of 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.

 doi:10.20944/preprints202404.0357.v3

6. Summary

As far as data security and privacy protection are concerned, it is necessary to avoid security problems technically, but the pursuit of technological perfection alone may also committing the fallacy of composition if it can 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 realize data security as a whole.

By analyzing the path of data security governance in China, it can be found that the accidents that damage data security in China are not only caused by technical problems, but also many accidents are caused by data processors who do not operate in accordance with the law. For data security protection, it is undeniable that technicians should first ensure data security from the technical level, but it should not be ignored that technicians should also have an understanding of the laws and regulations of each country, because the development and innovation of technology should follow the provisions of laws, and only by understanding the specific security of the legal provisions for the protection of data security, can help us develop technologies that enable data to be more comprehensively protected.

In summary, data security, whether from the national level, social level or individual level, has an extremely close relationship with national sovereign security, social stability, individual rights and interests, etc. On the one hand, data security is more closely linked to personal information, personal privacy, national security protection and other issues, and the data security issue, making it the centralized manifestation of these issues. On the other hand, data as a carrier of various types of information, coupled with the non-exclusivity and renewability of data, has posed higher challenges to data security. Effective management of data security issues requires not only the continuous improvement of the theoretical system, but also needs to build a set of laws and regulations throughout the data collection, utilization, circulation, and other aspects of the system.

References

1. N. Kanem, “State of the World Population Report 2023,” United Nations Population Fund, New York, NY, USA, 2023.
2. F.D. Li,”The comprehensive strength of China's Internet industry has increased significantly,” Economic Daily, Accessed: Apr, 23, 2024 [Online]. Available: http://paper.ce.cn/pc/content/202404/19/content_293164.html
3. Y. Bu,”Internet users exceed 1.079 billion, thousands of industries ‘touch the Internet’ digital economy for China to inject vigorous momentum”, China National Radio. Accessed: Apr, 21, 2024 [Online]. Available: https://finance.cnr.cn/ycbd/20230829/t20230829_526401178.shtml
4. B. Schneier, *Data and Goliath: The Hidden Battles to Collect Your Data and Control Your World*, NY, USA: W. W. Norton & Company, 2015.
5. S. H. Li, “Legislative Responses to the Protection of Privacy in the Digital Age”(数字时代隐私权保护的立法因应), *Law Science*, vol. 508, no. 3, pp. 17-31, 2024.
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. Accessed: Apr, 21. 2024 [Online]. Available: https://www.ndrc.gov.cn/fggz/fzzlgh/gjjzxgh/202203/t20220325_1320207.html?eqid=dd629fc70007c70700000006645ddddd
7. W. Fan, “Reconstructing the Path of Personal Information Protection in the Age of Big Data,” (大数据时代个人信息保护的路径重构), *Global Law Review*. vol. 38, no. 5, pp.92-115, Feb, 2016.
8. T. Wu, “Application of the principle of data minimization to the platform's practice of handling personal information,” (最小必要原则在平台处理个人信息实践中的适用), *Chinese Journal of Law*, Vol. 43, no. 6, pp.71-89, 2021.

 doi:10.20944/preprints202404.0357.v3

9. Y. Liang,"Divergences, causes, and consequences of U.S.-China global data governance," (中美全球数据治理的分歧、原因与后果), Journal of Nanjing University of Posts and Telecommunications (Social Science), vol. 26, no. 01, pp. 41-50, 2024. https://doi.org/10.14132/j.cnki.nysk.20240022.001.
10. K. Dong, J. C. Wu, and T. C. MA, "Research of Outbound Data Transfer Security Risk Element System in China," (我国数据出境安全风险要素体系研究), *Information Studies: Theory & Application*. Jan, 2024. Accessed: Apr, 1, 2024, [Online.] Available: https://link.cnki.net/urlid/11.1762.G3.20240115.1347.004
11. C. Nigel, D. Luke, "How barriers to cross-border data flows are spreading globally, what they cost, and how to address them," ITIF. Accessed: Apr 1, 2024. [Online.] Available: https://itif.org/publications/2021/07/19/how-barriers-cross-border-data-flows-are-spreading-globally-what-they-cost/
12. B Chen.; "Data outbound security governance ushers in new regulations," (数据出境安全治理迎来新规) *in Explaining the logic of multidimensional governance in the digital economy* . Beijing, China: China Legal Publishing House, 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. Accessed: Arp 1, 2024. [Online.] Available: https://www.bfh.com.cn/Html/News/Articles/5797.html
14. D. Q. Xu, "On the rule of law in regulating corporate two-way compliance of exit data Flows," (论跨境数据流动规制企业双向合规的法治保障), *Oriental Law*, no. 02, pp. 185-197, Feb. 2020. https://doi.org/10.19404/j.cnki.dffx.20200220.006.
15. H. L. Zhang, "Platform's date security obiligation in data production," (数据生产论下的平台数据安全保障义务), *Legal Forum*, vol. 36, no. 36, pp: 46-57, Mar. 2021. https://doi.org/10.19404/j.cnki.dffx.20200220.006.
16. G. Webster, "Translation: Chinese Authorities Announce $1.2B Fine in DiDi Case, Describe 'Despicable' Stanford University. Data Abuses" Accessed: Apr, 21. 2024 [Online]. Available: https://digichina.stanford.edu/work/translation-chinese-authorities-announce-2b-fine-in-didi-case-describe-despicable-data-abuses/
17. You - Case of destroying computer information system, PiZhou, JiangSu, China, no. 868, 2020.
18. J. Y. Han, "The judicial dilemma of data crime and the way forward for its governance," (数据犯罪的司法困境及治理进路), *in Proc. The Yangtze River Delta Jurisprudence Forum*, Shanghai, China, 2022, pp.185-197. https://doi.org/10.26914/c.cnkihy.2023.003170.
19. Y. Q. Hong, "The logical deconstruction and institutional construction of China's data security legislation," (我国数据安全法的体系逻辑与实施优化), *Law Science Magazine*, vol. 44, pp. 38-53, 2023. https://doi.org/10.16092/j.cnki.1001-618x.2023.02.001.
20. Y. Liu, "Improve data classification regulations and data security legislation," Cyberspace Administration of China. Accessed: Arp 1, 2024. [Online.] Available: https://www.cac.gov.cn/2020-09/28/c_1602854536494247.htm
21. S. Lin, "China to introduce 'Data Element X' plan to unlock data's multiplier effects in diverse scenarios: official," Global Times. Accessed Arp 1, 2024. [Online] Available: https://www.globaltimes.cn/page/202311/1302484.shtml
22. L. Zhang, J. Bian," An analysis of data governance strategies against the backdrop of digital economy", *Macroeconomic Managemen*t, 02(2022), pp. 35-41. https://doi.org/10.19709/j.cnki.11-3199/f.2022.02.013.