THREE ISSUES OF DATA COMPLIANCE GOVERNANCE IN CHINA BASED ON CASE ANALYSIS

Teng Zhang[*]

Abstract: With the rapid development of China’s digital economy and increasingly stringent global data protection regulations, corporate data security and compliance have become key factors that determine the competitiveness and sustainable development of enterprises. However, China's data compliance governance still faces three main challenges: inadequate self-regulation of corporate data compliance, imperfect internal management system, and the risk of violations throughout the entire data lifecycle. To address these issues, China needs to comprehensively improve data security and compliance of Chinese enterprises by improving the system to strengthen corporate behavior guidance, intensifying internal compliance mechanisms, and identifying the compliance process for data processing. Based on the world’s most typical legal systems related to data security and corporate compliance, and drawing on local Chinese judicial cases, this paper provides an in-depth analysis of the current challenges faced by Chinese enterprises in data security compliance. Finally, the paper explores and proposes a comprehensive governance path. Through the implementation of the comprehensive measures proposed in this study, Chinese enterprises now have practical guidance in the increasingly complex data security environment, thereby promoting their stable and sustainable development.

Keywords: Data Compliance, Chinese Enterprises, Corporate Governance, Information Security, Compliance

[*] School of Cyber Security and Information Law, Chongiqng University of Posts and Telecommunications, China.

Table of Contents

INTRODUCTION

In recent years, China has issued numerous laws and regulations focusing on data security and compliance governance, placing increasing emphasis on the issue of compliance governance for data security in enterprises. Corporate compliance refers to proactive prevention of the risks of civil sanctions, administrative penalties, and reputation damage by complying with laws and regulations.[1] Data compliance encompasses the key aspects of traditional corporate compliance and introduces new requirements for the handling of corporate data: firstly, it requires adherence to rules and regulations to ensure that business activities are not punished; secondly, it mandates the establishment of a sound data compliance management system to prevent risks such as data infringement and data leakage.

However, according to the "White Paper on Enterprise Data Compliance (2021)" issued by the China Software Testing Center[2], most enterprises closely related to data and digital economy face issues such as failure to fulfill their related compliance obligations in data handling, lack of a well-established compliance system, and escalating difficulties in security governance. These problems expose the vast amount of data stored by enterprises to significant risks of data leakage, and the social impact caused by these risks is also showing an expanding trend.

With the increasing requirements for data security and compliance, enterprises are facing unprecedented challenges and opportunities. They must establish an effective compliance governance system based on compliance with laws and regulations to ensure sustainable business development. Data compliance not only focuses on the traditional physical security of data but also on the content security of the information contained in the data. Therefore, strengthening the legality and compliance of enterprise data security has become a significant topic in current business operations, academic research, market regulation, and other scenarios.

Based on a comparison of data compliance laws between China, Europe, and the United States, as well as an analysis of current judicial cases in China, there are still three major issues in China: inadequate self-regulation of corporate data compliance, imperfect internal management system, and the risk of violations throughout the entire data lifecycle.

Data compliance cannot be achieved overnight. To address the existing related issues, we should approach from three perspectives: first, improving the system to strengthen corporate behavior guidance, and guiding enterprises to establish a suitable compliance system based on their own characteristics and needs from a legal perspective; second, enhancing the internal compliance mechanism of enterprises and building a management framework for data compliance from within the enterprise; third, identifying the compliance process for data processing to ensure that legal risks can be eliminated throughout the data lifecycle.

[1] Zhang, Y. H. (2019). Criminal compliance: International trends and Chinese practices. *Procuratorial Daily*. November 2, p. 3.

[2] China Software Testing Center. (2022). Official website. Retrieved from https://www.cstc.org.cn/search.jsp?wbtreeid=1001.

Considering the increasing attention paid by legal academics and legal practitioners to data compliance issues in China, data compliance research remains scarce and one-sided. This paper delves into three aspects: the current state, challenges, and coping strategies for data compliance in China. It aims to promote research on Chinese data compliance in the global legal community and address current issues of data security compliance governance in Chinese enterprises.

I. RELATED WORK

Currently, academic research on enterprise data compliance focuses primarily on the introduction and implementation of a criminal compliance system for data security, legal regulations on data circulation and cross-border data management, and the construction and optimization of a data protection compliance system.

Li Bencan (2018)[3], Yu Chong (2020)[4], and Zhang Yong (2022)[5] believe that it is necessary to implement a criminal compliance system to address the increasing complexity and frequency of data crimes. Through co-governance between enterprises and the state, they aim to strengthen data security protection, achieve active general prevention, and promote the convergence of criminal and administrative measures to achieve collaborative governance.

Wang Liming (2023)[6], Paul de Hert et al. (2016)[7], and Xu Duoqi (2020)[8] argue that in the era of the data economy, enterprise data circulation and cross-border data management face challenges, emphasizing the need to promote compliance, facilitate circulation, and ensure security through improved laws, regulatory mechanisms, and technical means.

Chen Ruihua (2020)[9], Mao Yixiao (2022)[10], and He Hang (2022)[11] believe that in the process of digital transformation, enterprises should establish and optimize a data protection compliance system, achieving a shift from passive compliance response to proactive compliance governance. This ensures data security and compliance, thus strengthening the data governance structure and compliance management processes to address the challenges and risks of data protection compliance.

Based on the aforementioned research context, current scholars' research on enterprise data compliance still ignores the effectiveness of industry self-regulation

[3] Li, B. (2018). *Compliance and Criminal Law: A Global Perspective*. China University of Political Science and Law Press.

[4] Yu, C. (2020). The iterative alienation of data security crimes and the path of criminal law regulation: From the perspective of the introduction of criminal compliance programs. *Journal of Northwest University (Philosophy and Social Sciences Edition)*, 5, 93-102.

[5] Zhang, Y. (2022). The crime filtering model of criminal compliance in data security. *Academic Forum*, 3, 13-24.

[6] Wang, L. (2023). Data Protection by Civil Law. *Digital Law*, (1), 43-56.

[7] Paul & Vagelis. (2016). The new General Data Protection Regulation: Still a sound system for the protection of individuals? *Computer Law & Security Review*, 32(2), 179-194.

[8] Xu, D. (2020). On the legal guarantee of two-way compliance for cross-border data flow regulation enterprises. *Eastern Law Review*, (2), 185-197.

[9] Chen, R. (2020). Basic issues of corporate compliance. *China Legal Review*, (1), 178-196.

[10] Mao, Y. (2022). Research on data protection compliance system. *Journal of the National Procurators' College*, (2), 84-100.

[11] He, H. (2022). Key issues and relief measures of corporate data security compliance governance. *Guizhou Social Sciences*, (10), 126-133.

systems, the perfection of internal management systems, and the widespread existence of data violation risks in enterprises. Therefore, this paper focuses on three prominent issues: insufficient self-regulation systems for enterprise data compliance, imperfections in the internal management system, and the risk of violations throughout the entire data lifecycle. To address these issues and ensure the effective protection and legitimate utilization of electronic data, as well as to maintain enterprise security and data-driven operations, the author believes that the problems of data security compliance governance in Chinese enterprises today should be solved by improving systems to strengthen enterprise behavior orientation, intensifying internal compliance mechanisms, and clarifying the compliance process for data processing.

II. OVERVIEW OF DATA SECURITY LEGISLATION IN CHINA, EUROPE AND AMERICA

As humanity enters the digital age, the severity and possible spillover effects of data security risks have had negative impacts in multiple fields such as politics, technology, economy, and society. Therefore, the scientific response to data security is bound to become a key focus of research in the digital age. People's attention has shifted from the possibilities and extensibility of "Being Digital"[12] to the characteristics and forms of the "Network Society"[13], and further to topics such as data security and artificial intelligence in the "Cyber Society"[14]. As the network society and the real society become increasingly integrated, security issues in cyberspace are becoming more prominent. Computer crimes have also evolved into cybercrime, manifesting in three basic types: cybercrime where the network serves as the "criminal object", "criminal tool", and "criminal space"[15]. However, regardless of the type of cybercrime, its manifestations always revolve around electronic data and information technology composed of "0" and "1" in "bits".

With the digital transformation of economic and social life, people have realized that data is a fundamental strategic element of the digital economy. Data has become the foundation for individuals to participate in economic and social activities, for businesses to carry out operational activities, and for social public organizations and state agencies to fulfill their duties. The protection of data security has become an important guarantee for the healthy development of the digital economy.

Currently, legislation in Europe, the United States, and other countries is mainly divided into two categories: data jurisdiction and data protection.

Firstly, there is the legislation targeting data jurisdiction in the United States. Leveraging the authority granted by the Foreign Corrupt Practices Act (FCPA), the US government utilizes its formidable national strength and global influence. Through joint law enforcement actions between the Department of Justice and the Securities and Exchange Commission, it actively mobilizes various departments such as the Federal Bureau of Investigation, Homeland Security, and the Criminal Investigation Division of the Internal Revenue Service. It employs diverse legal means including wiretaps,

[12] Negroponte, N. (1997). *Being Digital*. Hainan Publishing House. (Original work published 1995)

[13] Castells, M. (2010). *The Rise of the Network Society*. Blackwell Publishing. pp. 500-509.

[14] Zheng, Z., & He, M. (2004). Analysis and discrimination of the concept of "network society." *Sociological Research*, 1, 9.

[15] Yu, Z. (2014). Intergenerational evolution of cybercrime and the response of criminal legislation and theory. *Qinghai Social Sciences*, 2, 1-11.

undercover operations, search warrants, and subpoenas, and has established a whistleblower hotline and reward mechanism. These efforts are fully coordinated to combat overseas corruption and maintain a fair and just international business environment. When overseas businesses conducting operations in the US or having business relationships with US companies are suspected of violations, they often seek lenient criminal and administrative penalties through agreements and the establishment of a compliance governance system. However, many companies still pay heavy fines[16]. With the advent of the information age, the US has formulated a cybersecurity strategy to clarify national interests and responsibilities[17]. The US government has expanded its "long-arm jurisdiction" experience under the FCPA to protect personal information, privacy, and data through domestic legislation at different levels. As long as there is a jurisdictional connection with the US, companies from anywhere must accept the jurisdiction of US law. Although this model has been opposed by many countries since its inception, accusing the US of violating the basic principles of international law with its "long-arm jurisdiction," most have to accept this reality due to the US's absolute advantages in technology, finance, politics, military, and soft power.

The second aspect is data protection legislation in EU countries, which originated from the Western society's strong emphasis on privacy protection. As the information age surged in the 1990s, the risk of privacy breaches increased daily. To address this situation, the Privacy Impact Assessment (PIA) system emerged as a response and gradually became a conventional measure to protect individual privacy. The EU provides high-standard guarantees for data security by establishing a sound and rigorous rule system. In 1995, the "Directive on the Processing of Personal Data and Data Protection" conducted a preliminary exploration of the operational mechanism of data protection agencies in EU countries in the form of binding governance rules for the first time. With the continuous improvement of Internet technology and the advent of the big data era, the legal environment in the EU has undergone profound changes. In May 2018, the General Data Protection Regulation (GDPR) came into effect, regarded as the strictest personal information protection and data regulation[18]. Based on the Privacy Impact Assessment (PIA), the EU has specially established a Data Protection Impact Assessment (DPIA). As the core content of the EU data protection framework, DPIA has not only become a key approach to personal data security governance in various countries but also provides a path guide for corporate compliance management, economic digital transformation, and the construction of a data security governance legal system in various countries.

Since China joined the international Internet system in 1994, the internet has gone through nearly 30 years of ups and downs in China. The focus has shifted from an initial emphasis on computer and cybercrime, to network security protection at the national security level, and finally to addressing the challenges of personal information protection and data security risks in the information society. The cyberspace governance legislative process has shown a three-phase incremental development trend, including legislation on infrastructure and legal relationships, legislation on network

[16] Yang, K., & Tao, D. (2017). The US Foreign Corrupt Practices Act. *China Economic Weekly*, 49, 2.
[17] Yu, L. (2012). The impact of American internet strategy on China's political and cultural security. *International Forum*, (2), 7.
[18] Jiao, N. (2022). Research on the operational mechanism of data protection agencies in EU countries. *Information Magazine*, 41(5), 154-161.

information services and industry management, and legislation on information security, data security, and online transactions. Specifically:

The first aspect is legislation on infrastructure and legal regulatory systems. In this phase, administrative legislation was adopted to address the issues of the foundation for internet development and network security from the perspective of network infrastructure. Regulations and rules related to the network infrastructure and basic behaviors were successively formulated.

Table 1. *Data Security Guarantee and Network Transaction Legislation.*

Year	Effectiveness Level	Laws and Regulations
2013	Administrative Regulations	Regulations on the Protection of Computer Software
2011	Administrative Regulations	Regulations on the Security Protection of Computer Information Systems
1997	Departmental Rules	Interim Provisions on the Administration of International Networking of Computer Information Networks

The second aspect is legislation on the Internet information services and industry management systems. In 2013, Edward Snowden, a former employee of the Central Intelligence Agency (CIA) and the National Security Agency (NSA) in the United States, exposed the "Prism" program[19]. This program revealed the serious harm caused by the United States' use of the Internet to conduct network surveillance and cyberattacks on other countries, which endangered the network security and information security of various countries. Based on this, Chinese legislative bodies began targeted and systematic legislative activities to address the issue of cyberspace governance and issued the following laws and regulations.

Table 2. *Data Security Guarantee and Network Transaction Legislation.*

Year	Effectiveness Level	Laws and Regulations
2011	Administrative Regulations	Measures for the Administration of Internet Information Services
2013	Administrative Regulations	Regulations on the Protection of Information Network Transmission Rights
2013	Departmental Rules	Regulations on the Protection of Personal Information of

[19] Zou, Q. "Prism Gate" causes huge legal controversy in the US. Retrieved from https://www.chinacourt.org/article/detail/2013/06/id/1014622.shtml.

		Telecommunications and Internet Users
2017	Departmental Rules	Measures for the Administration of Internet Domain Names
2017	Departmental Rules	Regulations on the Administration of Internet News Information Services
2019	Departmental Rules	Regulations on the Administration of Blockchain Information Services"
2019	Departmental Rules	Regulations on the Administration of Financial Information Services
2011	Administrative Regulations	Measures for the Administration of Internet Information Services
2013	Administrative Regulations	Regulations on the Protection of Information Network Transmission Rights

The third aspect is data security guarantee and improvement of the network transaction law. This stage focuses mainly on strengthening and improving cyberspace governance through the enactment of basic laws by the legislature. Based on maintaining national security and data sovereignty and competing for dominance in cyberspace and data flow governance with developed European and American countries, the following laws and regulations have been formulated and implemented:

Table 3. *Data Security Guarantee and Network Transaction Legislation.*

Year	Effectiveness Level	Laws and Regulations
2015	Law	National Security Law
2017	Law	Cybersecurity Law
2019	Law	E-commerce Law
2020	Law	Cryptography Law
2021	Law	Data Security Law
2021	Law	Personal Information Protection Law
2021	Administrative Regulations	Regulations on the Safety Protection of Critical Information Infrastructure
2022	Departmental Rules	Measures for the Safety Assessment of Data Export

2022	Departmental Rules	Measures for Cybersecurity Review

With the promulgation of the Data Security Law in June 2021, the data governance system achieved a breakthrough from scratch, becoming a fundamental law in the field of security in China. According to the provisions of China's Data Security Law, data security refers to the state of effective protection and lawful utilization of data through the adoption of necessary measures, as well as the ability to maintain a continuous state of security. The Data Security Law also clearly states that the protection of data security aims to "protect national sovereignty, security, and development interests" and to "promote data development and utilization, and protect the legitimate rights and interests of citizens and organizations."

III. DATA COMPLIANCE TRENDS AMONG CHINESE ENTERPRISES

As mentioned earlier, corporate compliance refers to conforming to legal requirements.[20] The legal norms in this region can be broadly categorized into four main types: Firstly, the national legal system, which encompasses laws, administrative regulations, administrative rules, local regulations, and judicial interpretations. All normative documents with legal authority are binding guidelines that must be followed. Secondly, business practices, which include both written norms such as codes of conduct issued by various industry associations, as well as unwritten business practices and ethics. Thirdly, internally developed company rules and regulations. Violations of rules established by the company itself may also result in penalties for the business. Lastly, international organizational treaties, such as compliance management and sanctions systems established by international organizations such as the World Bank. For violations of treaty obligations by companies, the World Bank can impose sanctions with conditions for lifting, setting a probationary period of several years for the company and requiring it to rebuild its compliance program.

Based on the research conducted by Chinese scholars, corporate compliance, as a form of corporate governance, encompasses three aspects: administrative compliance, criminal compliance, and compliance with international sanctions. Specifically:

Firstly, in terms of criminal compliance. The criminal compliance mechanism views corporate compliance as a key basis for prosecution, conviction, and sentencing, and also serves as an important basis and content for corporate settlement agreements. This mechanism has been established as a statutory basis for corporate criminal liability and is presented as an alternative, informal criminal procedure in criminal procedure law.[21] Therefore, criminal compliance refers to a legal system in which prosecutors set a probationary period for corporate compliance when a company is suspected of specific crimes, urging the company to make a commitment to compliance and actively implement rectification measures. After inspection and evaluation by a third-party organization, lenient treatment is implemented for the relevant companies based on the actual situation.[22]

[20] Zhang, Y. H. (2019). Criminal compliance: International trends and Chinese practices. *Procuratorial Daily*. November 2, p. 3.

[21] Chen, R. H. (2020). Basic issues of corporate compliance. *China Legal Review*, (1), 178-196.

[22] Wang, L., & Wang, J. (2022). Active Duty to Enhance the Quality and Efficiency of Corporate Compliance Governance. *Prosecutorial Daily*, April 11, p. 3.

Secondly, in terms of administrative compliance, it refers to a legal system in which administrative regulatory agencies use specific institutional designs and regulatory measures to ensure that companies comply with administrative laws and regulations, prompting them to meet compliance standards. If a company suspected of violating administrative laws has established a compliance system, it can be used as a legal basis to obtain more lenient or flexible administrative treatment.

Thirdly, anti-international sanctions compliance refers to an international legal system where international organizations that establish compliance management agencies require companies that violate the trading rules set by the organizations to establish effective compliance programs in exchange for the lifting of sanctions and penalties.[23]

Whether from the perspective of the enterprise's own development, the long-term stability and security of society, or the strategic layout of the country, corporate compliance is the inevitable path for the vigorous development of enterprises and even the national economy. With the development of the digital economy, the importance of data security has not only become the key to economic stability and development but also a focus of national security concerns. As the main participants in the digital economy, enterprises' compliance governance in the field of data security is the foundation and guarantee for resolving data security risks. Generally speaking, it encompasses two levels of meaning: one is to ensure the security of the data itself, and the other is to meet the security requirements of the environment where the data resides[24]. Specifically, compliance governance in the field of data security requires that enterprises' behaviors during operation should comply with relevant national laws, regulations, and rules related to data security, and must not violate the internal rules and regulations formulated by the enterprise.

A. The Issue of Data Circulation Security is Severe

In the era of digital economy, economic globalization is entering a new era led by data flows. Data is increasingly becoming the core driving force for the vigorous development of economic activities, and compliance processing of data flows has become increasingly important. Economic globalization has enabled businesses to operate beyond geographical and national boundaries, while the rapid development of the Internet has further narrowed the distance between people around the world. However, in the process of carrying out cross-border operations or financing, enterprises will inevitably face the issue of cross-border data flows.

Cross-border data flows have become increasingly common. According to the *White Paper on Compliance and Technical Application of Cross-border Data Flows* issued by the Cross-border Data Flows Group of the Open Islands Open Source Community[25], China has emerged as a leading country in digital trade and is actively accumulating and utilizing massive amounts of data. Based on predictions from International Data Corporation (IDC), the average annual growth rate of data volume

[23] Chen, R. (2022). *Basic Theory of Corporate Compliance*. Legal Publishing House.

[24] Chen, B., & Hu, Z. (2021). The legal path to coordinate data security and development in the digital economy. *Changbaixuekan*.

[25] Digital Elite Network. (2023). Retrieved from https://www.digitalelite.cn/h-nd-5751.html.

in China is expected to reach approximately 30 percent from 2021 to 2025, making China a leader in global data volume.

In the future, the digitization of the global economy driven by data elements will bring broader and more profound impacts. The acceleration of cross-border data flows is changing the global economic landscape. In the long run, this will affect the competitive relationship between developed and developing countries in the labor market, reshape the global labor market, and further influence the global industrial chain layout and value chain division of labor. Therefore, regions and enterprises with advantages in data elements and intelligent technology are expected to occupy the mid-to-high-end position in the global value chain.[26]

The cross-border flow of data elements will have profound and widespread impacts on core areas such as international benefit distribution, national and cyber security, and data sovereignty. In view of this, we must maintain a high level of awareness and vigilance regarding the security issues involved in data circulation. In 2021, the incident of Didi Chuxing's listing in the United States[27] triggered widespread concern about the security risks of "cross-border data circulation" across the internet. As a direct result, the National Internet Information Office of China imposed administrative penalties on Didi Chuxing, including stopping the registration of new users, removing the app from all platforms, issuing a notice, conducting a cybersecurity review, and imposing a fine of RMB 8.026 billion on Didi Global Inc.[28] The main violations committed by Didi Chuxing include illegally collecting and abusing personal information data, engaging in data processing activities that pose a serious threat to national security, and illegal operational behavior, which bring serious security risks to the security of national critical information infrastructure and data security. On December 18, 2020, the Chinese stock Luckin Coffee, which was listed in the United States, admitted to financial fraud[29]. This triggered the formal effectiveness of the U.S. Congress's legislation on the supervision of listed companies, the "Holding Foreign Companies Accountable Act", which empowers the U.S. Securities and Exchange Commission (SEC) to initiate stronger information disclosure requirements for Chinese stocks listed in the United States in order to protect investors' interests. It requires Chinese stocks to hand over audit working papers, otherwise, it will suspend trading or delist Chinese stocks that do not submit audit working papers for three consecutive years. Although this incident, which has continued to this day, was temporarily suspended from the delisting crisis of Chinese stocks after negotiations between China and the United States reached a cooperation agreement on August 26, 2022. However, the cross-border audit review issue related to audit working papers is undoubtedly closely related to data circulation security. The urgent risk of data circulation security brought about by the above typical cases once strengthened the Chinese government's

[26] Hong, Y., Zhang, M., & Liu, Y. (2022). Promoting the safe and orderly flow of cross-border data to lead the globalization of the digital economy. *Bulletin of the Chinese Academy of Sciences*, 37(10), 1418-1425.

[27] Cyberspace Administration of China. (2022). Official website. Retrieved from http://www.cac.gov.cn/2022-07/21/c_1660021534306352.htm.

[28] Wang, Z.,&Zhang, F. (2022). The Cyberspace Administration of China Imposes a Fine of 8.026 Billion Yuan on Didi, Cheng Wei and Liu Qing Each Fined 1 Million Yuan. People's Network. Retrieved from http://finance.people.com.cn/n1/2022/0721/c1004-32481985.html.

[29] China Securities Regulatory Commission. (2020). Notification on the Investigation and Disposition of Financial Fraud in Ruixing Coffee. Retrieved from http://www.csrc.gov.cn/csrc/c100028/c1000725/content.shtml.

legislative work on this issue. In July 2022, the Cyberspace Administration of China issued the "Measures for the Safety Assessment of Data Exit", and subsequently formulated and issued the "Guide for the Declaration of Safety Assessment of Data Exit (First Edition)", further building a comprehensive solution that focuses on institutional norms and integrates technological innovation in the field of cross-border data flow.

B. The Legal Risks of Data Leakage and Information Regulation Have Increased

With the widespread application and rapid development of digital technology, its utilization of personal information has become increasingly frequent and diversified. However, this also poses escalating risks to individual rights and interests. To mitigate these risks, it is particularly crucial for enterprises to achieve compliance in information data management. Relevant enterprises primarily serve individual users. According to Chinese laws and regulations on cyberspace governance, the collection of personal information under a real-name system is indispensable. During the generation, collection, and utilization of personal information data, the primary data security issues faced by enterprises include: firstly, the illegal and non-compliant collection and use of personal information, such as collecting sensitive personal information without the individual's knowledge or using personal information beyond the scope agreed upon by the data subject; secondly, the failure to adopt effective technical and management measures to protect data, leading to the theft, leakage, or damage of important data collected or generated during operations, thereby posing a threat to national security, public interest, and individual rights and interests.[30]

On the other hand, according to legal provisions, enterprises engaged in information services can be divided into three categories: network access services, information content services, and information service platform services. In the process of providing the aforementioned internet information services, enterprises are faced with obligations to supervise user behavior, information content, and enterprise qualifications. Meanwhile, if enterprises themselves are engaged in value-added telecommunications services, internet news information services, internet religious information services, internet live streaming services, and other fields, they still need to obtain corresponding licenses and registrations. Failure to obtain the corresponding licenses or registrations, or violations of relevant legal provisions resulting in serious consequences, may result in heavy administrative penalties or the revocation of licenses and registrations.

C. The Governance Dilemma of Data Ownership Confirmation and Data Flow

As an important component of assets, data possesses the attribute of eventually turning into capital through flow and transactions, similar to other assets.[31] The capitalization of data highlights the transformation of data's role, elevating it from being merely an information carrier to becoming an asset with the potential to create personal

[30] Feng, D., Zhang, M., & Li, H. (2014). Big data security and privacy protection. *Chinese Journal of Computers*, 37(1), 13.

[31] Lian, Y. (2021). *Data Rights Law 3.0: Legislative Prospects of Data Rights*. Social Sciences Academic Press.

or corporate wealth. This change has given the data market unprecedented and vast development opportunities.

In the course of business operations, enterprises produce and collect vast amounts of data. However, enterprises only possess de facto control over these data, which is the right to use the data, but this does not equate to ownership of the data. Therefore, in the face of the emerging data market with tremendous development potential, how to monetize the data at hand, turn it into capital, and create more wealth has become a key concern for enterprises.

The current ambiguous definition of data ownership in China has led to many difficulties in data sharing and openness, making it necessary to establish compliance for data handling. To achieve free flow, efficient allocation, and fair competition in the data element market, determining data ownership has become an urgent priority.[32] Coase Theorem suggests that "if transaction costs are zero, no matter how rights are defined, optimal allocation can be achieved through market transactions, independent of legal provisions."[33] Therefore, relying on market regulation, ambiguous data property rights and inappropriate ownership relations may negatively impact market operations. In the current legal environment where data ownership is not clearly defined, enterprises can only address market and legal risks in data circulation by establishing an effective compliance governance system that meets regulatory requirements.

IV. CHALLENGES OF DATA COMPLIANCE IN CHINA

A. Inadequate Self-Regulation of Corporate Data Compliance

In today's data-driven social landscape, self-regulation of industry data compliance affects the benchmark of corporate governance. However, there are significant deficiencies in China's self-regulatory system in the field of data compliance, which can be deeply analyzed from two levels: industry norms and technical capabilities.

Taking data scraping behavior as an example, from the perspective of industry norms, the lack of forward-looking legislation and ineffective implementation of norms have become the two main issues. Starting from the ten verdict cases related to data anti-unfair competition released by the Beijing Intellectual Property Court[34], it is observed that the court frequently applies the principled provisions of the Anti-Unfair Competition Law when dealing with data unfair competition cases. This indicates that there are gaps in the specific provisions of existing laws on data scraping behavior, and related data scraping behaviors often lack clear legal regulations.

The use and processing of data are constantly evolving, yet existing industry norms often struggle to keep pace with these changes, exhibiting a legislative lag. Industry norms lack specific regulations on data scraping, and in some industries, there

[32] Zhang, Y., & Zhang, B. (2022). Data ownership confirmation and institutional response in the context of building a data element market. *Journal of Shanghai University of Political Science and Law: Rule of Law Forum*, 37(4), 20.

[33] Coase, R. H. (1960). The problem of social cost. *Journal of Law and Economics*, 3(1), 1-44.

[34] "Top Ten Typical Cases of Data-Related Anti-Unfair Competition in Beijing Intellectual Property Court." Retrieved from Beijing Intellectual Property Court website: https://bjzcfy.bjcourt.gov.cn/article/detail/2023/07/id/7382298.shtml.

are no norms whatsoever related to data collection. This has led to widespread data violations among enterprises. In terms of norm implementation, even when relevant industry norms exist, enterprises often only symbolically comply with them in practice, falling far short of the standards expected by the norms. Both of these major issues identified through case analysis illustrate the significant lack of enforcement in industry self-regulation, with enterprises generally lacking the intrinsic motivation to strictly adhere to the norms.

From the perspective of technical specifications, the current technical specifications may have been inadequately considered during their formulation, making it difficult to achieve comprehensive and effective supervision in practical applications. The "Information Technology Big Data Data Classification Guide"[35] is overly theoretical, and its data classification methods and standards are disconnected from actual operations. Even if enterprises read this specification, it is difficult for them to have a clear definition of data classification, making it challenging for the specification to play its due regulatory role in practical applications. When formulating technical specifications, if similar specifications are not adequately scientifically argued and practically tested, the scientific and practical value of the specifications will be greatly reduced. In this case, even if enterprises try their best to comply with these specifications, it may be difficult to achieve the desired data compliance effects.

B. Imperfect Internal Management System

As enterprises increasingly rely on data, it is particularly important to establish a comprehensive internal management system. Currently, many enterprises still have many deficiencies in this area, mainly reflected in the loopholes in their internal data management processes and the urgent need to improve compliance mechanisms.

The so-called loopholes in the enterprise's internal data management process mainly refer to institutional defects or inadequate management in storage, access control, and other links. Taking the case of Han Bing's destruction of a computer information system[36] as an example, as a database administrator, he should have shouldered the responsibility of protecting corporate data security. However, due to the imperfect internal management system, Han Bing used his privileges to conveniently log in to the financial system, deleted financial data and related applications, resulting in the company's financial system being completely inaccessible. This fully exposes the company's deficiencies in data classification management, permission settings, and data operation procedures, failing to effectively prevent internal personnel from abusing their privileges, which led to a serious data security incident.

Today, enterprises are facing severe challenges and a constantly changing legal environment in terms of data management and compliance, thus their compliance mechanisms urgently need to be improved. Enterprises need to establish clear compliance standards and operational procedures in various aspects such as data collection, storage, use, and destruction. Didi Global Inc. was once heavily fined for

[35] State Administration for Market Regulation, Standardization Administration. (2020). *Information technology - Big data - Guidelines for data categorization*. GB/T 38667-2020.

[36] Beijing First Intermediate People's Court. (2020). Criminal Verdict, (2020) Jing 01 Xing Zhong 490.

not establishing clear data compliance standards and operational procedures. [37] Currently, many enterprises are still struggling in this regard, lacking systematic and forward-looking compliance planning. The lack of this section often leaves enterprises at a loss when facing data compliance risks, making it difficult to effectively respond, and ultimately leading to penalties.

C. The Risk of Violations Throughout the Entire Data Lifecycle

The risk of violation, which runs throughout the entire life cycle of data, is an important issue that cannot be ignored by enterprises. In the 1980s, the concept of life cycle was transferred to the field of information management[38], referring to the process of information data from generation, utilization to elimination. To be closer to the current enterprise's actual application of data, the enterprise data life cycle can be divided into four stages: data collection stage, data storage and use stage, data sharing and trading stage, and data destruction stage.

In the data collection stage, enterprises collect a large amount of data, and the risks of violation mainly focus on three core aspects: first, the compliance of data collection methods, especially the use of crawler technology; second, the randomness of data collection, where disorderly or improper operations occur occasionally; third, the excessiveness of data collection, which means excessive collection may infringe privacy or violate relevant regulations.

The administrative penalty imposed by the China Market Supervision and Administration Bureau on Chengdu Zhike Technology Co., Ltd.[39] provides a thorough illustration of the administrative penalty risks arising from non-compliant data collection methods. The excessive and indiscriminate collection of data is further exemplified in the case of Shanghai Yuanyun Investment Management Co., Ltd. suspected of excessively collecting consumer personal information[40]. Both cases reflect the current compliance issues faced by enterprises in the data collection process, including unauthorized collection of personal and platform data, failure to clearly state the purpose, method, and scope of data collection, as well as indiscriminate and excessive collection methods. These issues significantly increase the risk of administrative penalties for enterprises, such as hiccups to business operations and damage to public welfare.

In the data storage process, the risk of violation mainly stems from neglecting the establishment of data security management systems and operating procedures, as well as failing to implement deidentification and encryption measures when storing

[37] Wang, Z.,&Zhang, F. (2022). The Cyberspace Administration of China Imposes a Fine of 8.026 Billion Yuan on Didi, Cheng Wei and Liu Qing Each Fined 1 Million Yuan. People's Network. Retrieved from http://finance.people.com.cn/n1/2022/0721/c1004-32481985.html.

[38] Levitan, K. B. (1982). Information resources as “goods” in the life cycle of information production. *Journal of the American Society for Information Science*, 33(1), 44-54.

[39] Chengdu Zhike Technology Co., Ltd. Improper Conduct Case [No. 51010023000187]. (2024). Chengdu Administration for Market Regulation.

[40] Shanghai Yuanyun Investment Management Co., Ltd. (2023). Suspected of excessively collecting consumers' personal information case. Shanghai Jing'an District Market Supervision and Administration Bureau. Case No. Hu Shi Jian Jing Chu [2023] 062021002963.

data. The Guangdong Driving Training Data Security Case[41] exemplifies this point. Most enterprises have significant shortcomings in data storage management, not only lacking a data backup mechanism but also failing to set a clear data storage period. In terms of handling stored personal information, enterprises also appear to be insufficiently rigorous. They use personal information directly after collection without necessary processing, exacerbated by the problems of privacy leakage and abuse.

The risk of violation during the data sharing and trading phase focuses on requiring the data receiver to fulfill the obligation of data security protection. In the country's first case of commercial secret infringement involving a data transaction buyer[42], San Company, as the data receiver, failed to fulfill the corresponding data security obligations and even disclosed and used the information to third parties. This shows that during data sharing and trading, if enterprises do not take any measures to ensure the obligations of the data receiver, it can easily lead to data misuse, deviating from the original purpose authorized by the data owner. In the current increasingly strict administrative law enforcement environment for personal information protection, these reckless behaviors of enterprises, if discovered, will inevitably face serious legal consequences.

During the data destruction phase, it is necessary to regularly destroy data to prevent the accumulation of data, which can trigger the illegal risks mentioned above in the storage, sharing, and trading phases. The Cyberspace Administration of China conducted a cybersecurity review on CNKI. Based on CNKI's deficiencies in the data destruction phase, such as not providing an account cancellation function and not deleting users' personal information in a timely manner after canceling their accounts, administrative penalties were imposed on CNKI[43]. Failure to fulfill the obligation to destroy data not only leads to penalties for the company itself but also significantly increases the probability of cybersecurity risks such as citizen data breaches, which in turn affects national security.

V. EXPLORATION OF THE COMPLIANCE PATH FOR DATA SECURITY IN CHINESE ENTERPRISES

A. Improving the System to Strengthen Enterprise Behavior Orientation

Based on an in-depth analysis of the aforementioned issues, the primary challenge faced by enterprises in building a compliance system is the lack of a clear institutional orientation. To address this problem, relevant laws, regulations, and reference plans should be actively introduced to guide enterprises in establishing suitable compliance governance systems based on their own characteristics and needs. In the future, China's legislative work on data security can start from two aspects: basic regulations and administrative rules and regulations. Legal regulations should be

[41] "Guangdong's First Case! A Company in Guangzhou Was Punished by the Police for Not Fulfilling the Obligation to Protect Data Security." (2022) Guangdong Legal Website. Retrieved from https://www.gdzf.org.cn/yasf/content/post_123060.html.

[42] Chongqing Guang Motorcycle Manufacturing Co., Ltd. v. Guangzhou San Motorcycle Co., Ltd. (2022). Infringement of business secrets dispute. Chongqing Free Trade Zone People's Court. Verdict No. (2022) Yu 0192 Min Chu 8589.

[43] Cyberspace Administration of China. (2023). The Cyberspace Administration of China Imposes Administrative Penalties Related to Cybersecurity Review on CNKI According to Law. Retrieved from https://www.cac.gov.cn/2023-09/06/c_1695654024248502.htm.

imposed on key aspects such as data ownership confirmation, circulation, and transaction security.

In terms of basic regulations, legislation needs to clarify the ownership, use rights, and management rights of data, providing a solid legal foundation for data transactions. This includes detailed provisions on data classification, data ownership, and legitimate methods of data acquisition, to ensure the circulation of data under legal and secure premises.

In terms of administrative regulations and rules, the focus should be on regulating the data circulation market, establishing strict market access standards, clarifying the rules and procedures for data transactions, and increasing penalties for violations. This aims to promote the healthy development of the data market while ensuring data security, thus guaranteeing the continuous improvement of the industry.

B. Intensifying the Internal Compliance Mechanism

The deficiencies in the internal management system of enterprises have seriously affected their data security and compliance. In order to enhance the data management capabilities of enterprises and reduce potential risks, enterprises must immediately proceed to improve their internal management systems, clarify the responsibilities and authorities of various departments and personnel, and establish scientific and reasonable data processing procedures. At the same time, enterprises should also strengthen employee training and awareness efforts to ensure that every employee fully understands the importance of data security and compliance and puts it into practice.

Currently, the "Compliance Management Measures for Central Enterprises"[44] provide a template for state-owned enterprises to establish a sound compliance management system tailored to their actual situation, including compliance systems, improving operational mechanisms, cultivating a compliance culture, and strengthening supervision and accountability. Private enterprises should learn from this approach to strengthen their internal management system. Regarding data security and compliance issues, private enterprises should deeply understand and draw on the core philosophy and practical experience of the "Compliance Management Measures for Central Enterprises" to build and improve their own compliance management system.

C. Identify the Compliance Process of Data Processing

To ensure that data complies with existing processing procedures and to reduce data breaches and other security risks, enterprises must clarify the compliance process for data processing. The "Information Security Technology - Security Capability Requirements for Big Data Services"[45] provides regulations for every aspect of the entire data processing chain, serving as an important reference for enterprises in handling data today. This standard not only provides clear guidance for data collection,

[44] State-owned Assets Supervision and Administration Commission of the State Council. (2022, August 23). Measures for the Compliance Management of Central Enterprises. Decree No. 42 of the State-owned Assets Supervision and Administration Commission of the State Council. Effective from October 1, 2022.

[45] National Information Security Standardization Technical Committee. (2023). Information security technology: Security capability requirements for big data service (GB/T 35274-2023).

storage, processing, and transmission but also emphasizes the importance of key security measures such as data encryption, access control, and security auditing.

To strictly implement the data classification and grading system, enterprises should follow the "Data Security Technology - Data Classification and Grading Rules"[46] for standardized classification and grading of data after collecting it. These rules help enterprises reasonably classify data grades based on sensitivity, importance, and value, thereby implementing more refined data management and protection measures.

Based on data classification and grading, enterprises also need to establish detailed data processing procedures and security policies to clarify access rights, encryption measures, backup strategies, and emergency response plans for each level of data. By implementing these measures, enterprises can ensure that data is fully protected during transmission, storage, and processing, effectively preventing the risk of data leakage and misuse.

After improving the aforementioned processes, enterprises should also regularly review and update their data security management systems and procedures to adapt to the constantly changing security threats and technological environment. Continuous enhancement of data security training and awareness raising is necessary to ensure that employees in the corresponding sectors understand and follow data security regulations, collectively maintaining the data security of the enterprise.

CONCLUSION

In the context of the rapid development of the digital economy, Chinese enterprises are facing increasingly severe challenges in data security and compliance. This study conducted an in-depth exploration of the core issues related to data security and corporate compliance among Chinese enterprises, revealing critical problems such as inadequate self-regulation of corporate data compliance, imperfect internal management system, and the risk of violations throughout the entire data lifecycle. To address these challenges, this paper systematically explores effective data security and compliance governance pathways, including improving the system to strengthen corporate behavior guidance, intensifying internal compliance mechanisms, and identifying the compliance process for data processing. These measures aim to ensure that enterprises fully comply with laws and regulations when processing data, thereby effectively guaranteeing the security and compliance of corporate data. This study not only provides strong theoretical support and practical guidance for Chinese enterprises in data security and compliance governance but also offers some reference for addressing corporate data security and compliance issues globally.

[46] National Information Security Standardization Technical Committee. (2024). Data security technology: Rules for data classification and grading (GB/T 43697-2024).