JOURNAL OF MODERN SOCIAL SCIENCES
Vol. 1, No. 2, Dec. 2024, 164-174
https://doi.org/10.5281/zenodo.14263589

ATRI PRESS
Connecting Scholars
Shaping Futures

Research on Data Security Governance from the Perspective of New Quality Productive Forces

Zhao Zimeng[1], **Jiang Zhongqi**[2*]

[1]*Xi'an Jiaotong University School of Law, China*
[2]*Xi'an Jiaotong University School of Law, China*
*Corresponding author: Jiang Zhongqi

Abstract

The development of new quality productive forces relies on data as a crucial element. The extensive application and in-depth integration of data have, while promoting innovation and progress in various fields, also given rise to numerous data security issues. By analyzing the inherent logic between new quality productive forces and data security governance, this paper points out the current situation and challenges faced by data security governance in China. In combination with the characterization of legal risks related to data security, it explores the value orientation and basic principles of data security governance, and constructs a multi-dimensional governance path that includes perfecting the legal and regulatory system, strengthening technological safeguards, clarifying the responsibilities of multiple entities, and enhancing international cooperation. The aim is to provide theoretical support and practical guidance for the coordinated development of data security and new quality productive forces, ensuring the safe, orderly, and efficient utilization of data in the development process of new quality productive forces.

Keywords: New Quality Productive Forces; Data; Data Security Risks; Data Security Governance

Introduction

In the current digital era, new quality productive forces are emerging vigorously, and their development is profoundly transforming the economic and social landscape. New quality productive forces, as a new form of productive forces represented by "computing power" and the like, rely on the strong support of data as a core element for their development. Data has become an emerging strategic resource following traditional production factors such as land, labour, capital, and technology, playing a crucial role in promoting economic and social development, spawning new industries, new models, and new driving forces. As a key production factor, data runs through all aspects of the development of new quality productive forces.[1] It has become a new type of national strategic resource and a critical element in forming new quality productive forces. From the optimization of automated production processes driven by production data in intelligent manufacturing, to the innovation of efficient financial services supported by transaction data in the digital finance field, and to the assistance of medical data in precise diagnosis and treatment decisions in smart healthcare, the value of data is highlighted in numerous scenarios of new quality productive forces. However, the large-scale flow, frequent interaction, and extensive application of data have also brought about unprecedented security challenges.

The Data Security Law, which came into effect in September 2021, stipulates that: “The competent departments of industry, telecommunications, transportation, finance, natural resources, health, education, science and technology, etc. shall assume the responsibility for data security supervision in their respective industries and fields. The public security organs and national security organs shall assume the responsibility for data security supervision within their respective scopes of duties in accordance with this Law and relevant laws and administrative regulations. The national cyberspace administration department shall be responsible for coordinating and supervising network data security and related supervision work in accordance with this Law and relevant laws and administrative regulations”. In the practice of data security supervision, it is difficult to trace the clues of data leakage, to screen for potential data security risks, and to track the funds of illegal data transactions. Administrative supervision may restrict the opening and circulation of data and suppress the release of data value while protecting digital security. These problems not only threaten personal privacy and corporate interests but also pose severe challenges to national security, social stability, and economic development.

The Third Plenary Session of the 20th Central Committee of the Communist Party of China emphasized “accelerating the construction of the institutional mechanisms to promote the development of the digital economy and enhancing the regulatory capacity for data security governance”. From the perspective of the development of new quality productive forces, how to achieve the balance between data security and the open utilization of data and how to effectively govern data security risks have become important issues that urgently need to be resolved. Therefore, it is urgent and important to conduct in-depth research on data security governance from the perspective of the development of new quality productive forces.

The Inherent Logic between New Quality Productive Forces and Data Security Governance

Data security governance from the perspective of new quality productive forces is an important concept emerging in the contemporary digital wave, with profound connotations and closely intertwined with the development of new quality productive forces. Driven by scientific and technological innovation, new quality productive forces prompt in-depth transformations in various industries, and data, as a key element in this transformation process, runs through every stage. Essentially, data security governance aims to construct a comprehensive, systematic, and dynamic framework to ensure that data remains in a secure and reliable state within the data environment on which the development of new quality productive forces depends. This governance system is committed to maintaining the confidentiality, integrity, and availability of data through the comprehensive application of legal norms, institutional constraints, technical support, and management means.

According to Article 3 of the Data Security Law of our country, data security means ensuring that data is in a state of effective protection and legal utilization and has the ability to maintain a continuous secure state by taking necessary measures. Data security under this definition has two implications: First, the state of the data itself is stable, that is, the integrity, confidentiality, and availability of the data are not violated; second, the guarantee ability of external factors is stable.[2]

During the data collection stage, strict compliance with laws, regulations, and ethical guidelines is required to ensure that the data sources are legal and compliant, avoiding the illegal acquisition of sensitive information such as personal privacy, corporate trade secrets, or state secrets. For example, in scenarios where Internet of Things devices are widely used, when intelligent sensors collect data, users must be clearly informed of the purpose, scope, and usage method of data collection, and explicit authorization from users must be obtained to prevent data from being stolen or misused at the source. During the storage process, advanced encryption technologies and secure storage architectures are employed to prevent data from being illegally accessed and tampered with. For instance, when financial institutions store customer transaction data, they use high-strength encryption algorithms to encrypt the data and set strict access permissions. Only authorized personnel can access the data in a specific secure environment to ensure the integrity and confidentiality of the data during storage. In the data transmission link, with the help of secure communication protocols and network architectures, data is ensured to be transmitted safely and accurately between different systems and platforms. For example, in cross-border data transmission, enterprises must comply with the data protection regulations of relevant countries and regions, adopt encrypted transmission channels to prevent data from being intercepted or leaked during transmission, and ensure that the security and integrity of the data are not impaired. When processing and sharing data, strict control of access permissions is exercised to ensure that data is only used for legal purposes by authorized entities and to guarantee the authenticity and reliability of the data. Taking medical data as an example, when hospitals conduct medical research or data sharing, they need to desensitize the data, remove sensitive information that can identify individuals, and strictly limit the scope of access personnel to ensure that medical data provides support for medical research and the improvement of medical services under the premise of legality and compliance, avoiding the illegal use of data or the leakage of patients' privacy.

Data security governance needs to adapt to the characteristics of diversified data application scenarios and complicated data flows brought about by the development of new quality productive forces. With the continuous evolution of new quality productive forces, such as the in-depth integration of artificial intelligence and the manufacturing industry, a vast number of complex data interaction scenarios have emerged. Data security governance should be able to respond flexibly to these changes, promoting the reasonable circulation and efficient utilization of data between different entities and different systems. On the one hand, it is necessary to break down data silos to achieve data interconnection and interoperability, providing rich data resources for the development of new quality productive forces; on the other hand, under the premise of ensuring security, it is necessary to ensure that data can flow smoothly, stimulate the potential value of data, avoid hindering the normal circulation and value release of data due to overemphasis on security, and thus strike a delicate balance between data security and data value release, laying a solid foundation for the continuous innovation and healthy development of new quality productive forces. Only by achieving the coordinated progress of data security governance and the development of new quality productive forces can we gain the upper hand in the fierce competition in the digital age and promote the economic and social development to a higher level.

The Predicament of Data Security Governance in China

Technical Level: Increasing Difficulty in Data Security Protection

In the current era, the development of new quality productive forces is closely related to that of artificial intelligence, big data, and the Internet of Things. Data is now in a complex environment of multi-technology integration, and the risks it faces are diverse and complex.

Artificial intelligence, relying on scientific and technological means, simulates or creates machines with "human-like" capabilities. It then derives results from vast, complex, and unordered "data sets" by means of algorithmic models and uses these results as the basis for decision-making.[3] However, this data-driven operating mode has numerous potential risks. Due to possible biases in data training or insufficiently perfect algorithm design, artificial intelligence may generate issues of algorithmic bias or discrimination when making decisions, thereby affecting the fairness of decision-making. For example, when a recruitment software uses artificial intelligence to screen resumes, it may, due to the use of mostly successful cases of a specific gender or race in the training data, lead to unfair screening results for other groups, thus limiting the diversity and fairness of talent selection.[4]

Although the extensive application of big data has created enormous value for enterprises and society, it has also brought about serious risks of privacy leakage. On the one hand, the phenomenon of excessive data collection is very common. Enterprises collect a large amount of personal data from users without their knowledge, with incomplete knowledge, or without authorization in order to obtain more information.[5] On the other hand, the improper use of data is also very common. Some enterprises use user data for unauthorized precision marketing and even engage in illegal data transactions, seriously infringing upon users' privacy rights and causing great interference to users' personal lives.

The widespread access of Internet of Things devices has exposed data to more "attack surfaces" during transmission and storage. Taking the smart home system as an example, various smart devices (such as cameras, smart door locks, smart appliances, etc.) are interconnected, forming a vast Internet of Things system. Once this system is hacked, users' living privacy will be completely exposed to criminals.[6] Hackers can easily obtain the real-time images of home cameras, remotely control the opening of smart door locks, or maliciously manipulate smart appliances. This not only poses a direct threat to users' personal safety but may also lead to unnecessary property losses.

With the development of new quality productive forces, the architecture for data processing and application has become increasingly complex, and traditional governance technologies can no longer meet the actual needs. The distributed characteristics of technological architectures such as distributed computing and edge computing make data storage and processing nodes scattered across different geographical locations and devices. This change has significantly increased the complexity of data security governance. Since security protection measures need to cover more scattered nodes, any security vulnerability in a node may be exploited by attackers, thereby leading to data leakage or system failures.

Institutional Level: The Lagging and Ambiguity of Legislation

In the context of the vigorous development of new quality productive forces nowadays, data security governance at the institutional level is facing numerous difficulties, with the problems of the lagging and ambiguity of legislation being particularly prominent, which have become the key factors restricting the effective governance of data security.

The formulation of laws itself is a "time-consuming and labor-intensive" major project, making it difficult to promptly respond to the emerging new issues of data security in practice within a short period of time. In terms of data application scenarios, taking the security of autonomous driving data as an example, with the development of autonomous driving technology, vehicles will continuously generate massive amounts of data during the driving process, such as vehicle location, driving speed, road condition information, and passenger information.[7] However, the law lacks clear regulations on the collection, storage, use, and sharing of these data, leaving a significant regulatory gap. In the event of data leakage or abuse incidents, it is difficult to effectively pursue responsibilities and protect rights and interests based on the current laws. Similarly, in the field of genetic data security, genes, as a special and sensitive type of personal information, with their huge value, have attracted the attention of many scientific research institutions and enterprises.[8] However, the law has not made clear provisions on the ownership definition, scope of use, and protection standards of genetic data, making genetic data face the risk of privacy leakage during the collection, research, and use processes.

Data security issues usually involve different legal departments, which poses many coordination difficulties in the application of laws. In terms of cross-border data flows, due to the involvement of laws of different countries or regions, the differences and conflicts between laws significantly increase the complexity of data security governance. For example, the General Data Protection Regulation (GDPR) of the European Union imposes extremely strict requirements on data protection, emphasizing the rights of data subjects and the restrictive conditions for cross-border data transmission; while the United States focuses on industry self-regulation, and its data protection rules vary significantly among different industries.[9] In such circumstances, if an enterprise wants to conduct cross-border data transmission business, it needs to simultaneously meet the legal requirements of multiple countries or regions. This not only increases the operating costs of the enterprise but also seriously hinders the free and orderly flow of data. In addition, the imperfect connection mechanisms between different laws further exacerbate the predicament of data security governance. For example, regarding the issue of data monopoly, the coordinated application rules between the Data Security Law and the Antitrust Law are still not perfect. The Data Security Law mainly focuses on the protection of personal data rights and interests, while the Antitrust Law emphasizes maintaining the order of fair competition in the market. When an enterprise forms a data monopoly advantage by collecting and controlling a large amount of data and uses it to restrict competition or damage user rights and interests, how to find a reasonable balance point between the two laws and achieve their effective coordination has become an issue that urgently needs to be resolved.[10]

Regulatory Level: Imperfection of the Management System

In the current landscape of data security governance, the problem of the imperfection of the management system at the regulatory level has already become a key factor restricting the enhancement of data security guarantee capabilities, severely impeding the leapfrog development of new quality productive forces.

As important entities in data processing and use, enterprises vary greatly in the construction of their internal data security management systems. A considerable number of enterprises have failed to establish a sound data security management system. For example, the phenomenon of chaotic data classification and grading management is quite common. Enterprises lack scientific and reasonable indicators to classify and grade data, unable to accurately identify the importance and sensitivity of different data types, thus making it difficult to implement effective and targeted data security protection measures.[11] Meanwhile, the problem of unreasonable setting of data access permissions is also very prominent. The division of permissions is either too broad or ambiguous, allowing unauthorized personnel to easily obtain sensitive data, increasing the risk of data leakage. In addition, the division of responsibilities for data security management is not clear. The responsibilities of different departments for data security management are not clearly defined. When data security problems occur, they shift the blame to each other, and there is a lack of an effective supervision and accountability mechanism, unable to form an effective collaborative management mechanism.

Apart from enterprises, some data practitioners and the vast majority of users have a serious lack of awareness of the importance of data security and generally lack the consciousness and basic skills of data security protection. In their daily work, due to varying professional qualities or weak data security awareness, data practitioners may cause data leakage due to improper operations.[12] For example, they may casually share sensitive data, transmit data containing important information to unauthorized third parties without taking necessary security measures, or neglect security norms during data processing and storage. When facing authorization requests from applications, users easily authorize them to obtain excessive personal information, such as location, address book, and chat records, without fully realizing the potential risks of these data being misused. Some malicious applications may use the user data they collect for illegal data transactions, or utilize user data for precise push notifications, advertising harassment, or even fraud.

The Characterization of Data Security Risks

In practice, the meaning of data has always been in a vague state, not only manifested in legislation. For example, in Article 37 of the Cybersecurity Law of China, "personal information" and "important data" are listed side by side; in Paragraph (4) of Article 76, network data refers to various electronic data collected, stored, transmitted, processed, and generated through the network.

However, in the Data Security Law of China, data is the record of information in electronic or other ways. Not only does there exist the problem of circular reasoning in logic, but it is also obvious that the connotations of “data” in different precursor laws are quite different. Even the expression of “data information” has emerged in the academic community. This indicates that the academic community does not have a clear understanding of “data” itself.

Meanwhile, the judicial organs in China have adopted different judgment rules for data crimes in the context of the digital economy. For example, in the case of “Kumike v. Chelaile”, both competition law liability and criminal liability are required to be borne; in the case of “Sina Weibo v. Fanyou”, only competition law liability is required to be borne; in the case of “Shengpin Company Grabbing Toutiao Videos”, only criminal liability is required to be borne. This has made the legal regulation of data crimes even more confusing.[13]

Data is a key element in the digital economy era, with rich meanings and various manifestations in different contexts. In a general sense, data is an abstract symbol that records and can identify objective events, a physical symbol or a combination of physical symbols that records the nature, state, and interrelationships of objective things. In computer science, it is the general term for all conforming media that can be input into a computer and processed by computer programs, including numbers, characters, images, sounds, videos, etc. The broadest sense of the data life cycle includes processes such as data production, collection, storage, management, use, processing, transmission, provision, public disclosure, and deletion.[14] In cross-border financial services, data is the carrier of commercial information of cross-border financial services, such as personal financial information, business operation data of financial institutions, and financial service data. Its flow is frequent and the risks are diverse. In the field of artificial intelligence, data provides the “raw materials” for the operation of artificial intelligence and is the cornerstone of the development and application of artificial intelligence. Its quality directly affects the training effect and generalization ability of artificial intelligence algorithm models.[15] At the enterprise operation level, data resources cover internal business management data of enterprises, user behavior data, data collected by Internet of Things devices, and external data related to the government, society, and upstream and downstream enterprises, running through all aspects of enterprise production and operation.[16]

As the fifth major production factor alongside labor, capital, etc., the value of data can only be realized through exchange. When data is exchanged and flows out of the country, the progress of formulating a country’s laws will inevitably lag behind the development speed of global data technology.[17] Different types of data play important roles in their respective fields, while also facing different security risks and challenges, such as data leakage, data abuse, data monopoly, etc., which require governance and protection through multiple means such as legal, technical, and managerial means. Risk management research is dedicated to studying management means of multi-level management of technical platforms and schemes and various emergency treatments, so as to better control the risks brought by technology.[18]

The focus of the characterization of legal risks lies in distinguishing the data security risks governed by the technical path and those governed by the legal path. The technical path plays a fundamental role in the data security governance system. Through technical methods such as cryptographic technology, access control technology, anonymousization technology, data desensitization, differential privacy, and privacy computing, risks of multi-source data can be mitigated. The legal governance path of data security risks stems from the funnel effect of the technical path.[19] For risks that cannot be solved solely by technical measures, the intervention of legal means is required. Even for those that can be handled by the technical path, the guarantee of the legal path is also needed. In addition, the legal path will also clarify the scale, standard, and scope of the technical path. For example, the Personal Information Protection Law has put forward the bottom-line requirements for data desensitization.[20]

IV. Data Security Governance Driven by New Quality Productive Forces

Adjusting the Value Orientation of Data Security Governance

Equal Emphasis on Security and Development. Data security is the cornerstone of the development of new quality productive forces. Only by ensuring data security can the stable development of new quality productive forces be guaranteed, avoiding the impairment of productive forces caused by security issues such as data leakage and abuse. Meanwhile, the development of new quality productive forces also provides technical and resource support for data security governance, promoting the innovation and application of data security technologies and enhancing the capacity of data security governance. In the intelligent manufacturing industry, ensuring the security of production data is the prerequisite for the stable operation of the production process, and the development of intelligent manufacturing technologies provides more advanced technical means for data security protection, such as using artificial intelligence technologies for data security monitoring and early warning.

Priority of Protecting Individual Rights and Interests. In data security governance, rights and interests such as personal privacy and property rights should be given priority in protection. The collection, use, and sharing of data must be based on respecting the will of individuals, ensuring that individuals have full rights to know, control, and choose regarding their data. When conflicts occur between the rights and interests of personal data and the commercial interests of enterprises or the interests of the state, individual rights and interests should be protected preferentially within a reasonable range to prevent personal data from being illegally used and infringed. In the digital medical field, patients' personal medical data involves privacy-sensitive information and must be strictly protected to ensure that the data is only used for legitimate medical purposes and shall not be leaked or used for other commercial purposes without the patients' authorization.

Promoting Social Fairness and Innovation. Data security governance should be committed to breaking data monopolies, promoting the fair sharing and circulation of data, providing equal opportunities for small and medium-sized enterprises and innovative enterprises to obtain data resources, and stimulating the innovation vitality of the market. Ensure the fair distribution and reasonable use of data among different entities, prevent those with data advantages from using their data advantages to restrict competition and hinder the development of innovation. By establishing a fair competitive environment in the data market, encourage enterprises and scientific research institutions to innovate based on data, and promote the wide application and continuous development of new quality productive forces in various fields. For example, in the fintech field,

DOI: https://doi.org/10.5281/zenodo.14263589
Zhao, Z., & Jiang, Z. (2024). A Research on Data Security Governance from the Perspective of New Quality Productive Forces. *Journal of Modern Social Sciences*, 1(2), 164 – 174.

promoting the fair sharing of financial data helps to promote the development of inclusive finance and provides opportunities for more small and micro enterprises to innovate in financial services.

Perfecting the Basic Principles of Data Security Governance

Principle of Legality. Data security governance must be carried out in accordance with the law, and governance measures should comply with the provisions of laws and regulations. Activities such as the collection, storage, transmission, processing, sharing, and destruction of data should all have clear legal bases and follow legal procedures. Data processors should ensure that their actions are within the scope of legal authorization and must not violate the mandatory provisions of laws and regulations. For example, they shall not collect users' sensitive data without the users' consent, nor use and share data beyond the scope stipulated by the law.

Principle of Proportionality. When implementing data security governance measures, the relationship between the effectiveness of the governance measures in ensuring data security and the burdens imposed on individuals, enterprises, and society should be weighed. The governance measures should possess appropriateness, necessity, and balance, avoiding overprotection or over-restricting the flow of data. For example, in the supervision of cross-border data transmission, reasonable supervision measures should be adopted according to the sensitivity and risk level of the data, to avoid hindering international trade and the rational allocation of data resources due to overly strict supervision; for data access control, access permissions should be reasonably allocated according to user roles and business requirements, to prevent the over-tightening of permissions from affecting the normal conduct of business.

Principle of Multiple Co-governance. Data security governance requires the joint participation of multiple entities such as the government, enterprises, social organizations, and individuals. The government should play a leading role by formulating policies and regulations and strengthening supervision and law enforcement. Enterprises, as the main entities of data processing, should assume the main responsibility for data security and strengthen internal management. Social organizations should play the roles of industry self-discipline and supervision. Individuals should enhance their awareness of data security and actively participate in data security protection. All parties should cooperate with each other and share information to form a data security governance pattern with the whole society's joint participation. For example, industry associations can formulate industry data security standards to guide enterprises to standardize their data processing behaviors; users can participate in data security supervision through reporting and other means to jointly maintain the data security environment.

Conclusion

In the context of new quality productive forces, data is rich in connotations and has a profound impact on economic and social development. Data security governance is a complex and urgent task. The existing legal provisions in China need to continuously adapt to the development characteristics of data elements. By perfecting relevant legal systems, balancing the interest relationships of all parties, and ensuring the legal, secure, and effective utilization of data, the continuous and healthy development of new quality productive forces can be promoted.

Through in-depth analysis of the connotations and challenges faced by data security governance, clarifying the value orientation and basic principles, and constructing a comprehensive governance path, including perfecting the legal and regulatory system, strengthening technical safeguards, clarifying the responsibilities of multiple entities, and strengthening international cooperation, data security issues can be effectively addressed, and the coordinated development of data security and new quality productive forces can be achieved. This will not only help protect individual rights and interests, corporate interests, and national security but also promote the healthy development of the digital economy and social fairness and innovation.

In future development, continuous attention should be paid to the new developments and new issues of data security governance. Further strengthening of collaborative cooperation in all aspects should be carried out, continuously optimizing governance strategies and measures, and continuously optimizing the data security governance system to continuously enhance the data security governance capacity. With a solid data security guarantee, a foundation can be laid for the vigorous development of new quality productive forces, promoting high-quality development of China’s economy in the digital age, occupying a favorable position in the global digital economy competition, and perfecting data security governance strategies in line with the times to ensure that data security and the development of new quality productive forces promote and progress in coordination with each other.

Acknowledgment

All contributions of the third parties can be acknowledged in this section.

Conflict of Interest

The authors declare no conflict of interest.

References

[1] WEI Xiangjian, HUANG Xinye, XIAO Luyuan. (2024). Auditing for data security governance in the perspective of new quality productivity development, Auditing Research, (05), 45-52.

[2] Cao Pantian, Yuan Ruijing. (2023). Preventive Governance of Data Security Risks in Overseas Listing of Enterprises. Hebei Journal, 43(03), 203-210.

[3] LIN Wei. (2022). Artificial Intelligence Data Security Risks and Countermeasures. Journal of Intelligence, 41(10), 105-111.

[4] JIANG Luyuan, CAO Limei, QIN Xin, et al. (2022). Fairness perception in artificial intelligence decision making. Advances in Psychological Science, 30(05), 1078-1092.

[5] Mei Y. (2024). Research on Data Security Situation and Protection. Network Security Technology and Application, (11), 51-54.

[6] Kuang Boyu, Zhang Zhaobo, Yang Shanquan, et al. (2024). HMFuzzer: A human-computer collaboration-based firmware vulnerability mining scheme for IoT devices. Journal of Computing, 47(03), 703-716.

[7] Qian Linye. (2023). Autonomous driving data security risk and legal protection. China Informatisation, (04), 65-67.

[8] SONG Sijia, SAN Chenlu, WANG Shuang, et al. (2021). Research on the privacy of genetic data and the progress of related protection technology. Journal of Medical Informatics, 42(06), 2-9.

[9] Dongfang. (2019). Comparative analysis of legal regulation of cross-border data flow in the EU and the United States and 'Chinese wisdom' to cope with the challenges. Library Journal, 38(12), 92-97.

[10] Chen B, Fu SG. (2024). Commercial utilisation of public data: market value, competitive rationale and promotion of rule of law. Journal of Beijing Administrative College, (05), 96-105.

[11] YIN Zhiwei, HE Xin, WANG Zhao. (2024). Analysis of generic data classification and hierarchical protection strategy in enterprise information lifecycle management. Electronic Technology, 53(03), 398-401.

[12] ZHANG Wenxi, YIN Wenhao, HU Xiaoyao, et al. (2024). Exploration of security protection system based on the whole life cycle of data. Software, 45(08), 169-171.

[13] Yang Zhiqiong. (2023). Challenges and Responses to the Criminal Law System of Data Crimes in China in the Era of Digital Economy. China Jurisprudence, (01), 124-141.

[14] Li Huaisheng. (2022). Adjustment of Criminal Law on the Crime of Infringing Citizen's Personal Information - Background of Citizen's Personal Information Protection Law. Journal of China University of Political Science and Law, (01), 138-148.

[15] Liu Linlin. (2024). Research on Data Security Risk Prevention System in the Era of Artificial Intelligence. Journal of Politics and Law, 41(03), 32-41.

[16] Dong Muxin, Xu Yude. (2022). Data Security and Governance Path in Digital Transformation of State-owned Enterprises - Based on Information Ecology Perspective. Finance and Accounting Monthly, (13), 132-136.

[17] Ma Qijia, Liu Feihu. (2022). Exploration of National Security Governance in Data Exit. Theory Exploration, (02), 105-113.

[18] MA Guanghua, GAO Gao Liang, MA Chenhui. (2023). Research on Commercial Data Security Risk Prevention Based on Machine Learning. Journal of Management, 36(01), 70-83.

[19] Tang, Lin-Yao. (2022). Risk Regulation and Jurisprudence Construction of Data Compliance Technology. Oriental Law Journal, (01), 79-93.

[20] Li Huaisheng. (2023). Data life cycle security risk and its criminal law response path. Journal of Soochow University (Philosophy and Social Science Edition), 44(03), 74-85.