Essay

Legal Boundaries Of Data Protection

zhang sheng Sun *

Posted Date: 19 February 2024

doi: 10.20944/preprints202402.1062.v1

Keywords: Data protection; Legal boundary; Privacy; Personal information security

 doi:10.20944/preprints202402.1062.v1

Essay

Legal Boundaries of Data Protection

Zhangsheng Sun [1,2]

[1] School of Political Science and Law, Xinjiang Normal University, No. 100 Guanyuan Road, ShuimogouDistrict, Urumqi, Xinjiang, 830017, China; 15939756236@163.com

[2] South China Normal University School of Law 378 Waihuan West Road, Panyu District, Guangzhou 510006, China

Abstract: With the development of Internet, big data and artificial intelligence technology, personal information protection has become the focus of social attention. The legal boundary of data protection has become increasingly prominent, involving the collection, storage, use, transmission and disclosure of personal information. This paper aims to explore the legal boundary of data protection, analyze the legal basis, legal principles and legal provisions of personal information protection, and put forward corresponding legal suggestions, in order to provide reference for the improvement of China's data protection legal system.

Keywords: Data protection; Legal boundary; Privacy; Personal information security

1. Foreword

1.1. Research background

The study of the legal boundary of data protection is an important and practical subject. With the rapid development of the Internet, big data and artificial intelligence technology, data protection has become a hot issue of global concern. The Chinese government attaches great importance to data protection, and has issued a series of laws and regulations to strengthen data security protection. This paper will discuss this issue in detail, in order to provide a useful reference for the study of the legal boundary of data protection.The legal boundaries of data protection need to be clearly defined. The legal boundary of data protection refers to which actions are legal and which actions are illegal in the process of data processing. The study of the legal boundary of data protection is of great significance for the formulation and improvement of data protection laws and regulations. In China, the legal boundary of data protection mainly involves the following aspects:

Protection of personal privacy rights. Personal privacy right is the core issue of data protection. In China, the right to personal privacy is protected by law, and no one can be infringed upon by any organization or individual. Therefore, the personal privacy rights must be fully respected and protected when processing the data.Legitimacy of data collection. Data collection is the premise of data protection. Only legal data collection can ensure data security. In China, data collection must comply with laws and regulations, follow the principles of legality, legitimacy and necessity, and must pass through the consent of the collected person [1]. Legitimacy of data use. Data use is an important link of data protection. Only only legitimate data use can ensure data security. In China, the use of data must comply with laws and regulations, follow the principles of legality, legitimacy and necessity, and must be authorized by the data controller.Security of data storage. Data storage is the key link of data protection. Only by ensuring the security of data storage can data leakage be prevented. In our country, data storage must comply with laws and regulations, follow the principles of safety and reliability, and must take necessary security measures.Legitimacy of data sharing. Data sharing is an important part of data protection. Only legal data sharing can ensure data security. In China, data sharing must comply with laws and regulations, follow the principles of legality, legitimacy and necessity, and must pass through the consent of the data controller and the shared person.

 doi:10.20944/preprints202402.1062.v1

In conclusion, the legal boundaries of data protection are a complex and challenging subject. In China, the legal boundary of data protection mainly involves the protection of personal privacy right, the legitimacy of data collection, the legitimacy of data use, the security of data storage, the legitimacy of data sharing and so on. In order to better protect the data security, the Chinese government should strengthen the research on the legal boundary of data protection, formulate and improve the relevant laws and regulations, and strengthen the supervision of data processing activities. At the same time, data controllers and controlled persons should also strengthen self-discipline, enhance the awareness of data security protection, and jointly maintain data security [2].

1.2. Purpose and significance of the study

The study of the legal boundary of data protection is an important legal research topic, involving data privacy, data security, data transaction, data use and other issues. The study aims to sort out the research status of legal boundary of data protection, analyze the significance of legal boundary of data protection, and provide theoretical guidance and practical reference for the practice of data protection in China.The study of the legal boundary of data protection is an interdisciplinary issue involving multiple legal fields, which requires in-depth study of relevant legal systems and regulations, and understanding the technology and application of data protection, as well as the social and cultural background of data protection. This study will use literature research, case analysis, field research and other methods to deeply study the legal boundaries of data protection.

Organize the current status of the legal boundary research of data protection, understand the main problems and challenges of the current legal boundary research of data protection, and provide a basis for the follow-up research;Analyze the significance of the legal boundary research of data protection, including the improvement of the legal system of data protection, the promotion of data protection technology, and the guidance of data protection practice, etc.Provide theoretical guidance and practical reference for China's data protection practice, promote the improvement and development of China's data protection legal system, promote the innovation and application of data protection technology, and improve the level and efficiency of data protection practice;This study will deeply study the legal boundary issue of data protection and provide theoretical guidance and practical reference for the practice of data protection in China.

2. The basic concept of data protection

2.1. Definition of data protection

Data protection is an increasingly concerned topic in today's society. With the continuous development and popularization of Internet technology, the security issues of personal privacy information, important data and sensitive data have also become increasingly prominent. Therefore, data protection has become an important global issue, and governments and enterprises have formulated corresponding laws and policies to protect data security. This paper will explore in detail the definition of data protection and its legal boundaries.Data protection refers to the legal, safe and effective management and protection of the collection, storage, use, transmission, and disclosure of personal privacy information, important data and sensitive data [3]. Among them, personal privacy information refers to the personal identity, address, phone number, email and other personal identity information, important data refers to the national security, social stability, economic development has important influence of data, sensitive data refers to the national security, social stability, public interests, etc.

In terms of data protection, there are several legal boundaries to consider as described below:

Legitimacy of the data collection. Data collection must comply with the provisions of laws and regulations, and must be carried out with the consent of the collected person or as stipulated by law. For example, when collecting personal privacy information, the recipient must be informed of the use of the information and not beyond the necessary scope.Legitimacy of data use. The use of data must comply with the provisions of laws and regulations, and must be carried out with the consent of the user or stipulated by law. For example, after collecting personal privacy information, it must

 doi:10.20944/preprints202402.1062.v1

be used in accordance with the prescribed purpose and period, and shall not be leaked, tampered with, damaged, etc.Legitimacy of data transmission. Data transmission must comply with the provisions of laws and regulations, and must be carried out with the consent of the transmitted person or under the circumstances prescribed by law. For example, in the transmission of important data, the necessary security measures must be taken to prevent data leakage, tampering, damage, etc.Legitimacy of data disclosure. Data disclosure must comply with the provisions of laws and regulations, and must be conducted with the consent of the disclosures or the law. For example, when disclosing personal privacy information, the disclosed person must be informed of the use and protection measures of the information, and must not beyond the necessary scope.Technical boundaries of data protection. The technical boundary of data protection refers to what technical measures should be taken to ensure the security of data in the process of data protection. For example, when collecting personal privacy information, encryption technology should be used to ensure the confidentiality of information, and secure storage technology should be used to ensure the integrity of important data.Data protection is an important issue in today's society, and its legal boundaries need to be fully considered. In terms of data protection, we must abide by the provisions of laws and regulations, and take the necessary technical measures to ensure the security of the data, so as to maintain the security of personal privacy information, important data and sensitive data [4].

2.2. The importance of data protection

The importance of data protection is increasingly prominent in the current society, which involves national security, social stability and citizens' rights and interests. In the digital age, data has become an important resource of increasing value. However, the importance of data protection also means that data must be protected while being restricted and controlled, which involves the legal boundary of data protection. This paper will discuss the importance of data protection in detail, and focus on analyzing the legal boundary issues of data protection.Data protection is related to national security. In the digital age, data has become an important strategic resource with an increasing value. Therefore, the security of the data protection has become an important issue of national security. If the data is leaked or maliciously attacked, it will lead to the disclosure of state secrets, damage to economic interests and other problems, thus posing a threat to national security. Therefore, the issue of the legal boundary of data protection must be fully valued.Data protection is related to social stability. In the digital age, data has become an important social resource, and its application scope is increasingly extensive. However, the abuse and improper use of data can also pose a threat to social stability. For example, the use of personal privacy information for fraud, the use of false data for false publicity and other behaviors, will pose a threat to social stability. Therefore, the issue of the legal boundary of data protection must be fully valued.Data protection concerns citizens' rights and interests. In the digital age, data has become an important civil right, and its application is increasingly extensive. However, the abuse and improper use of data can also violate civil rights. For example, the use of personal privacy information for illegal tracking and the use of false data for illegal investigation will infringe on citizens' rights and interests. Therefore, the issue of the legal boundary of data protection must be fully valued.The legal boundary issue of data protection needs to be fully valued. In the digital age, the protection of data involves national security, social stability and civil rights, and its importance is self-evident. Therefore, the corresponding laws and regulations must be formulated to effectively protect and manage them. At the same time, it is also necessary to strengthen the research on the legal boundary issue of data protection to improve the legal level of data protection [5].

2.3. Basic principles of data protection

Data protection is an increasingly important issue in today's society, involving personal information, privacy, security and other aspects. To ensure the validity and legitimacy of data protection, the basic principles of data protection are crucial. This paper will detail the basic principles of data protection and focus on the principles of legality, necessity, purpose specificity and minimum harm.The principle of legality refers to the compliance with relevant laws and regulations

 doi:10.20944/preprints202402.1062.v1

in the collection, processing and storage of data. This principle is the basis of data protection and a basic requirement for data processors to follow. The principle of legality requires that the data processor obtain prior consent of the individual with the collected data and comply with relevant laws and regulations, such as the EU General Data Protection Regulation (GDPR), during data processing.The principle of necessity means that in the collection, processing and storage of data, there must be clear, specific and legitimate purposes, and must ensure that the processing and use of data do not cause harm to personal privacy. The principle of necessity requires that the data processors must reasonably and appropriately process and use the data, and must take the necessary measures to protect personal privacy. The principle of necessity is the core of data protection and the basic requirement that data processors must abide by.The purpose-specific principle is ensuring in collecting, processing, and storage that data processing and use is limited to the original purpose and that it must not be abused or used for other purposes. The purpose-specific principle requires that the data processors must reasonably and explicitly process and use the data, and must take the necessary measures to prevent the abuse or improper use of the data.The minimum harm principle is that the necessary security and protection measures must be taken to collect, process and store data to minimize the risk of data leakage, destruction or loss. The minimum damage principle requires that the data processors must take the necessary security measures, such as encryption, access control, etc., to protect the confidentiality, integrity, and availability of the data. The minimum damage principle is the key to data protection and a basic requirement that data processors must follow.

In conclusion, the basic principles of data protection include the principles of legality, necessity, purpose specificity and minimum harm. These four principles complement each other and form the basis and core of data protection. Data processors must strictly abide by these principles, ensure the legitimacy and security of data processing activities, and protect personal privacy and data value [6].

3. The legal framework for data protection

3.1. Overview of China's data protection legal system

With the rapid development of technologies such as the Internet, big data and artificial intelligence, the protection of personal information has become an important global issue. The Chinese government attaches great importance to data protection, and has gradually established a complete set of legal system for data protection.

First of all, China's data protection legal system mainly includes the Network Security Law, the Personal Information Protection Law and other laws and regulations. Among them, the "Network Security Law" is China's first law specifically for network security issues, clarifying the basic principles, basic tasks and basic systems of network security, providing a legal basis for data protection work. The "Personal Information Protection Law" provides detailed provisions on the protection of personal information, including the collection, use, storage, deletion of personal information and other links, to protect the legitimate rights and interests of personal information.Secondly, China's data protection legal system also includes a series of departmental regulations and normative documents. For example, the relevant provisions in the Cyber Security Law involve data security, cross-border data transmission, data backup and recovery, and many other aspects. In addition, the implementation of the Personal Information Protection Law also requires governments at all levels and relevant departments to formulate corresponding implementation rules and specific operational norms, and further clarify the specific requirements of data protection work [7]. In addition, China's data protection legal system also includes the coordination of international law and domestic legislation. In the context of globalization, China's data protection legal system needs to be in line with international laws and draw lessons from the advanced international experience. At the same time, it should also take into account the actual situation of domestic data protection and formulate a legal system for data protection in line with national conditions.In general, China's data protection legal system has formed a complete set of legal system, providing a strong legal guarantee for the data protection work. However, with the

 doi:10.20944/preprints202402.1062.v1

development and application of new technologies, the data protection legal system also needs to be constantly improved and adjusted to meet the new data protection needs.

3.2. Overview of the international data protection legal system

Data protection is one of the important legal issues facing today's society, which involves the collection, storage, use, transmission and protection of personal information. The International Data Protection Legal System is an important legal framework designed to protect personal privacy and data security. This section will detail an overview of the international data protection legal system, including the laws and regulations included in the international data protection legal system and its reference significance for global data protection.

The international data protection legal system includes the EU General Data Protection Regulations (GDPR), the California Consumer Privacy Act (CCPA) and other laws and regulations. Among them, the GDPR is a data protection law enacted by the European Union, which came into effect on 25 May 2018, and aims to protect the privacy rights and data security of EU citizens. The GDPR stipulates the collection, use, storage, transmission and deletion of personal data, and sets strict standards and procedures for data protection. The implementation of GDPR has had a profound impact on global data protection, and provides a useful reference for other countries and regions to formulate data protection laws.CCPA is A data protection law enacted by California that came into effect on November 1,2018, aiming to protect the privacy rights and data security of California residents. CCPA provides for regulations on the collection, use, sharing and sale of personal data, and sets up strict standards and procedures for data protection. The implementation of CCPA has had a positive impact on global data protection, and provides a useful reference for other countries and regions to formulate data protection laws [8]. In addition to the GDPR and CCPA, the international data protection legal system also includes other laws and regulations, such as the European Convention on Human Rights (ECHR), the European Privacy Directive (GDPR), etc. The ECHR is a data protection law enacted by the European Court of Human Rights and sets out the basic principles and standards for personal privacy and data protection. The GDPR is a data protection law enacted by the European Commission, which stipulates the collection, use, storage, transmission and deletion of personal data, and sets strict standards and procedures for data protection. These laws and regulations provide a useful reference for global data protection.

The international data protection legal system includes the EU General Data Protection Regulations, the California Consumer Privacy Law and other laws and regulations, which provides a useful reference for the global data protection. These laws and regulations provide a useful reference for global data protection, help to protect personal privacy and data security, and provide a useful reference for other countries and regions to formulate data protection laws [9].

3.3. The development trend of the legal framework for data protection

With the rapid development of digitalization and informatization and the advancement of globalization, data has become an important factor of production and strategic resource. Data protection has become a global issue, countries are strengthening data security protection, protect the privacy of citizens. The development trend of the legal framework for data protection mainly includes the following aspects:

Strengthen data security protection:Data security protection is the core content of the legal framework of data protection. In the current context of digitalization and informatization, data security problems are becoming more and more prominent, such as hacker attacks, data leakage, data abuse and so on. Therefore, strengthening data security protection is an important trend in the development of the legal framework of data protection.

Improve the legal system for data protection:The development of the legal framework for data protection needs to be continuously improved and strengthened. Countries should, according to their own actual conditions, formulate and improve the legal system of data protection, strengthen the supervision and management of data protection, and improve the efficiency and effect of data

 doi:10.20944/preprints202402.1062.v1

protection. At the same time, international cooperation on data protection should be strengthened to promote the establishment and improvement of the global legal system for data protection.

Strengthen the awareness of data protection:The awareness of data protection is an important factor in the development of the legal framework of data protection. In the context of digitalization and informatization, people are more and more dependent on data, and pay more and more attention to data protection. Therefore, the publicity and popularization of data protection awareness should be strengthened to improve the public's awareness and understanding of data protection, so as to promote the development of the legal framework of data protection [10].

4. Strengthen the research on data protection technology

Data protection technology is an important support for the development of the legal framework of data protection. Under the background of digitalization and information, the research and application of data protection technology is more and more important. Countries should strengthen the research and development of data protection technologies to improve the efficiency and effect of data protection, so as to promote the development of the legal framework of data protection.To sum up, the development trend of data protection legal framework mainly includes strengthening data security protection, improving the legal system of data protection, strengthening data protection awareness, strengthening data protection technology research and other aspects. Only by strengthening data protection can we effectively protect citizens' privacy and promote the development and progress of society.

4.1. Research status of the legal boundary of data protection

Research on data protection legal boundaries originated in Europe and originated from concerns about legal issues such as personal information and privacy. In the information age, data has become an important factor of production, and its protection problem has gradually attracted people's attention. With the rapid development of the Internet, big data, artificial intelligence and other technologies, the way, scope and quantity of data are used have changed greatly, which brings new challenges and problems to data protection.The main contents of the legal boundary research of data protection include the laws and regulations of data protection, the technical means of data protection, and the ethical and legal issues of data protection. Among them, laws and regulations are the basis of data protection, involving personal information protection Law, data Protection Law, network security Law and other laws and regulations. These laws and regulations provide legal basis and norms for data protection, and provide guidance and guarantee for the implementation of data protection.In addition, the technical means of data protection is also an important part of the data protection legal boundary research. With the increasing importance of data protection, the technical means of data protection have also been widely concerned and applied. For example, data encryption, data desensitization, data watermark and other technical means, can effectively protect the privacy and security of data, prevent data leakage and abuse.The ethical and legal issues of data protection are also the important contents of the legal boundary research of data protection. The ethical and legal issues of data protection involve personal privacy, commercial secrets, public interest and so on. In the process of data protection, the interests of all parties are needed to be balanced to ensure the rational use and protection of the data. At the same time, it is also necessary to strengthen the legal supervision, strengthen the law enforcement of data protection, and improve the level of legal guarantee of data protection.

In short, the legal boundary research of data protection is a research topic involving multiple fields and multiple levels, which needs to comprehensively consider multiple factors of law, technology, ethics, and business. With the increasing importance of data protection, the legal boundary research of data protection has also received more and more attention and research. In the future, with the continuous development and progress of data protection technology, the research of data protection legal boundary will continue to deepen and improve.

 doi:10.20944/preprints202402.1062.v1

4.2. Main contents of the research on the legal boundary of data protection

It is an important research field, involving many aspects, such as data classification, cross-border data transmission, and data security. This paper will discuss in detail from these aspects.Data classification is an important part of the study of data protection legal boundary. Data classification refers to the process of classifying and managing data in order to better protect data security and privacy. Data classification needs to take into account the sensitivity, use and storage location of the data, so as to take corresponding protection measures. In terms of data classification, the data subject has the right to choose whether to disclose its personal information, and has the right to request the modification and deletion of its personal information. At the same time, the data controller has the responsibility to ensure that the data classification and protection of the data comply with the relevant laws and regulations [11].

Cross-border data transmission is also an important part of the legal boundary research of data protection. With the development of globalization, the cross-border transmission of data has become an irreversible trend. However, the cross-border transmission of data also poses many legal and security issues. Cross-border transmission of data requires compliance with relevant data protection laws and regulations, including the rights and obligations of data subjects, the responsibilities and obligations of data controllers, and the legality and security of cross-border data transmission, etc. In addition, the cross-border transmission of data also needs to consider the will and consent of the data subject, as well as the relevant laws and regulations.Data security is also an important part of data protection legal boundary research. Data security refers to measures taken to protect data from access, tampering, theft, and destruction by unauthorized personnel. Data security needs to take into account the storage, transmission, processing and use of data, and needs to take corresponding technical and security measures [12]. In terms of data security, the data subject has the right to require the personal information to be protected, and has the right to require the personal information to be modified and deleted. At the same time, the data controller has the responsibility to ensure the security and privacy of the data and take necessary security measures to prevent data leakage and attacks.It is an important research field, involving many aspects, such as data classification, cross-border data transmission, and data security. Data classification needs to consider factors such as the sensitivity, use and storage location of the data, so as to take corresponding protection measures. Cross-border transmission of data requires compliance with relevant data protection laws and regulations, and takes into account the will and consent of the data subject, as well as relevant laws and regulations. Data security requires the corresponding technical and security measures to protect the data from unauthorized personnel access, tampering, theft, destruction and so on.

4.3. Methods and techniques of legal boundary research of data protection

The study of the legal boundary of data protection is an important subject involving multidisciplinary fields, including law, computer science, sociology and many other aspects. The study of data protection legal boundary aims to explore the legal boundary in the data protection legal system, that is, how to use and manage data reasonably while protecting personal privacy and data security. This paper will detail the methods and techniques of data protection legal boundary research.Literature analysis is a method of studying the legal boundary of data protection law. Mainly through combing and analyzing relevant literature, we understand the development process, legal principles, legal norms and other contents of data protection laws, so as to provide a theoretical basis for research. Methods of literature analysis include literature review, literature comparison, literature analysis, etc. The advantage of literature analysis is that it can quickly understand the basic situation and the latest progress in the research field, which can provide reference for subsequent research.Case analysis is a method of studying the boundary of data protection law. It mainly uses the analysis and research of specific cases to explore the problems and challenges of data protection law in the practical application. The methods of case analysis include case study, case comparison, case analysis, etc. The advantage of case analysis is that it can dig deep into the specific problems of data protection laws and provide practical guidance for the formulation and improvement of data protection laws [13]. Empirical research is a method of legal boundary research of data protection.

 doi:10.20944/preprints202402.1062.v1

Mainly through the collection and analysis of actual data, it discusses the effects and problems of data protection law in practical application. The methods of empirical research include questionnaire survey, data analysis, experimental research, etc. The advantage of empirical research is that it can obtain a large amount of practical data and provide more objective and accurate conclusions for the research.Blockchain technology is a technical means of data protection legal boundary research, which can effectively protect personal privacy and data security. Blockchain technology stores data on multiple nodes in a decentralized way to realize the secure sharing and transmission of data. The advantage of blockchain technology is that it can effectively prevent data leakage and tampering, and provide more reliable technical support for data protection.

Artificial intelligence technology is a technical means of the legal boundary research of data protection, which can effectively realize the automatic management and analysis of data. Through machine learning, natural language processing and other technologies, artificial intelligence technology can quickly identify and analyze the patterns and laws in the data, providing more intelligent and efficient support for data protection. The advantage of artificial intelligence technology is that it can effectively improve the efficiency and accuracy of data protection and provide more advanced technical support for data protection [14]. The legal boundary research of data protection is an important subject involving multidisciplinary fields, including literature analysis, case analysis, empirical research and other methods, as well as advanced technology means such as block-chain and artificial intelligence. Research can effectively protect personal privacy and data security, promote data sharing and application, and promote the development of digital economy.

5. Research significance of the legal boundaries of data protection

5.1. The guiding role of the legal boundary research of data protection on the practice of data protection in China

Clarifying the legal boundary of data protection: Research on the legal boundary of data protection helps to clarify the legal status, scope and content of data protection, and provides theoretical basis and practical guidance for the formulation and improvement of data protection laws in China.Guiding data protection legislation: Through the in-depth study of the legal boundary of data protection, it can provide suggestions on the legal system of data protection for the legislature of Our country, and help to formulate more scientific, reasonable and effective data protection laws.Guide data protection law enforcement: The legal boundary research of data protection can provide law enforcement departments with guidance on the scope of application and law enforcement procedures of data protection laws, and help to improve the efficiency and accuracy of law enforcement.Guide enterprise data protection practice: Legal boundary research of data protection helps enterprises to understand the requirements of data protection laws and regulations, guide enterprises to formulate appropriate data protection strategies, and ensure the compliance operation of enterprises.Guide the public awareness of data protection: The legal boundary research of data protection can improve the public's understanding of the data protection law, guide the public to establish a correct concept of data protection, and form a data protection pattern with the participation of the whole people [15].

5.2. The influence of the legal boundary of data protection on the international legal system of data protection

The study of data protection legal boundary has an important influence in the international data protection legal system. This research not only provides a useful reference for the international data protection legal system, but also provides an important reference for its development.The study of data protection legal boundary provides a new perspective and thinking for the international data protection legal system. Traditionally, the international data protection legal system mainly focuses on the protection of personal privacy and data security, while the study of data protection legal boundary pays more attention to the use and management of data, as well as the balance between data protection and privacy protection. This new perspective and idea provides a new thinking

 doi:10.20944/preprints202402.1062.v1

direction for the international data protection legal system, and helps it to better adapt to the development of the data era.The study of data protection legal boundary provides new legal standards and norms for the international data protection legal system. In the study of the legal boundary of data protection, data protection is no longer just a separate concept, but intersects and integrates with many legal fields, including privacy, security, intellectual property and other fields. This crossover and integration provides new legal standards and norms for the international legal system of data protection, and helps it to better protect the multiple interests of data.The study of data protection legal boundary provides new legal practice and cases for the international data protection legal system. The study of data protection legal boundary not only focuses on theoretical research and legal norms, but also focuses on legal practice and case analysis. This new practice and case can provide a useful reference for the international data protection legal system, and help it to better solve the legal issues and disputes in the actual data protection [16].

The study of data protection legal boundary provides a new legal system and mechanism for the international data protection legal system. In the study of the legal boundary of data protection, new legal systems and mechanisms have been proposed, such as data sharing and data exchange mechanism, data security evaluation and audit mechanism. These new legal systems and mechanisms provide a new basis and framework for the international legal system of data protection, and help it to better adapt to the development of the data era.The impact of data protection legal boundary research on the international data protection legal system is multifaceted, including providing new perspectives and ideas for the international data protection legal system, new legal standards and norms, new legal practices and cases, as well as new legal systems and mechanisms. These influences provide an important reference and reference for the development of the international data protection legal system, and help it to better adapt to the development of the data era.

5.3. The promoting role of data protection legal boundary research on the development of China's data industry

With the continuous development and application of information technology, data has become an indispensable part of modern society. Data is not only widely used in various fields, such as finance, medical care, education, etc., but also has become an important asset for enterprises and individuals. However, as the use and protection of data receive more and more attention, the legal boundary problem of data protection also gradually emerges. This paper will discuss in detail the promoting role of data protection legal boundary research on the development of data industry in China.Research on the legal boundary of data protection helps to promote the healthy development of China's data industry. With the wide application of data in various fields, the problem of data protection is becoming increasingly prominent. How to protect the data security, privacy, intellectual property rights and other issues have become the focus of social attention. Data protection legal boundary research can better understand and master the legal provisions and standards of data protection, so as to promote the healthy development of the data industry [17]. The legal boundary research of data protection helps to improve the competitiveness and innovation ability of the data industry. In the data era, data has become an important asset and competitive advantage of enterprises. However, as the legal boundaries of data protection become increasingly strict, enterprises need to constantly improve and innovate to cope with legal risks and challenges. Data protection legal boundary research can help enterprises to better understand the legal requirements and standards, so as to improve their competitiveness and innovation ability.Data protection legal boundary research helps to promote the development and innovation of the data industry. In the process of studying the legal boundary of data protection, new technologies and methods can be continuously explored and innovated to cope with the legal requirements of data protection. These innovations and explorations can help the data industry to achieve better development and innovation, thus promoting the progress and development of the whole industry.

The study of data protection legal boundary plays an important role in promoting the development of data industry in China. It can not only improve the competitiveness and innovation

 doi:10.20944/preprints202402.1062.v1

ability of data industry, but also promote the development and innovation of data industry. Therefore, it is necessary to strengthen the research of data protection legal boundary to promote the healthy development of China's data industry.

6. Challenges and prospects of the legal boundary research on data Protection

6.1. Challenges of the legal boundary research of data protection

The study of the legal boundary of data protection is a problem involving data security, technology update and legal system perfection. In this field, consideration should consider how to balance the relationship between personal privacy and public interest, and effective legal framework should be developed to protect personal privacy and data security.Data security is an important challenge in the study of data protection legal boundaries. With the growing importance of data privacy, measures are urgently needed to protect the data from attacks and leaks. However, data security is a changing issue and the legal framework to adapt to new security threats. Moreover, due to the continuous updating and development of technology, the legal framework needs to be able to keep up with technological developments in order to protect the data from the latest security threats [18]. Technical update is also an important challenge in the study of the legal boundaries of data protection. As technology continues to update and evolve, ensure that the legal framework can keep up with technology to protect data from the latest security threats. Moreover, due to the continuous update and development of technology, it is necessary to ensure that the existing legal framework can adapt to the new data use methods to protect personal privacy and data security.The improvement of legal system is also an important challenge in the study of legal boundary of data protection. At present, the legal framework has some shortcomings, such as the lack of clear legal responsibility, the lack of effective data protection mechanism. The study of the legal boundary of data protection is a problem involving data security, technology update and legal system perfection. A balance between personal privacy and public interest and an effective legal framework to protect personal privacy and data security. The existing legal framework needs to be constantly updated and adapted to accommodate new security threats and technological developments to ensure that the legal framework is able to protect personal privacy and data security [19].

6.2. The future prospect of the legal boundary research of data protection

The legal boundary research of data protection is an important research direction in the field of data science in recent years, involving the basic principles, legal framework, technology application and other aspects of data protection. With the improvement of data protection awareness and the continuous progress of technology, the research on the legal boundary of data protection will also continue to develop, and the future research will develop in the direction of data classification, data cross-border data transmission, data security and so on.Data classification is an important direction for the future data protection legal boundary research. Data classification refers to the classification, classification, identification and management of data to meet the requirements of data security and privacy protection. Data classification can help enterprises and organizations to better manage and protect their data, and reduce the risk of data leakage and abuse. In the future, the research on data classification will be more thorough, involving the standards, methods, technologies and other aspects of data classification [20]. Cross-border data transmission is another important research direction. With the development of globalization, cross-border data transmission is becoming more and more common, but it also brings problems such as data security and privacy protection. In the future, the research on cross-border data transmission will pay more attention to the transmission rules, security mechanism, privacy protection and other issues, so as to ensure the security and legitimacy of cross-border data transmission.Data security is an important direction of the future data protection legal boundary research. Data security means to protect the data from unauthorized access, leakage, damage and other risks. As the problem of data security becomes increasingly prominent, the research of data security will become more important. In the future, the research on data security

 doi:10.20944/preprints202402.1062.v1

will pay more attention to data security technology, security strategy, security supervision and other issues, in order to improve the level of data security.

In the future, the research of data protection will develop towards data classification, data cross-border transmission, data security and other directions. The in-depth research of these research directions will help to improve the legal framework of data protection, guarantee the security and legitimacy of data, and promote the development of data science.

7. The conclusion

The study of data protection legal boundary refers to the balance between data protection and privacy protection, exploring the legitimacy and rationality of data use and protection, as well as the legal and regulatory framework of data security protection. In this area, the rights and responsibilities of data users and the legal restrictions and provisions for data protection are needed to be considered. The study of data protection legal boundary is of great significance to the data protection practice in China. With the development of Internet and big data technologies, data collection, storage, use and transmission have become increasingly important, and research on the legal boundaries of data protection can help us better understand the legal and regulatory framework of data use and protection and how to balance the interests between data users and data protection agencies.In the future, it is necessary to strengthen data security protection and improve the data protection legal system. Data security is one of the core issues in the legal boundary research of data protection. With the frequent occurrence of data leakage and attacks, data security protection measures, such as encryption, access control and data backup. At the same time, it is necessary to strengthen the improvement of the legal system of data protection, such as formulating stricter laws and regulations, strengthening data protection supervision and enhancing the public's awareness of data protection.

References

1. Guo Feng, Huang Xiaoyi. The Internet Contract and the Construction of International Rules in cyberspace [J]. Information Security in China, 2020 (1): 30-33.
2. Guo Chengzhi. Inspection and assumption of the personal data protection framework in China [J]. Journal of Tianjin Sino-German University of Applied Technology, 2020 (2): 119-123.
3. Guo Wenqiang. On the legal positioning and protection path of data [J]. Journal of Mudanjiang University, 2018,27 (12): 54-56 + 60.
4. Zhang Liping, Zhang Ying. Personal information security protection under the background of Big Data: Research on Legal Prevention [J]. Modern Commerce and Industry, 2018,39 (16): 126-127.
5. Gu Liping, Fan Shu. Data ownership and use boundaries study [J]. Scientific Research Information Technology and Application, 2018,9 (3): 34-39.
6. Peng-Ningbo. Review of domestic data privacy protection studies [J]. Library, 2021 (11): 69-75.
7. Wang Xudong, Ye Shuiyong, Zhu Bing, et al. Research and application of data security protection technology in the process of data governance [J]. Journal of State Grid Technical College, 2019,22 (1): 46-50.
8. Ruan Huiling. Research on the legal protection of personal data [J]. Legal system and Society, 2018 (23): 225-226.
9. Anonymous. Journal of Modern Communication University of China [J]. Modern Communication (Journal of Communication University of China), 2020,42 (11): 2.
10. Xu Hanming, Sun Yixiao, Wu Yunmin. Research on the legal protection of data property rights [J]. Comparison of economic and social systems, 2020 (4): 183-191.
11. Li Huaisheng. Criminal law boundaries of data openness [J]. Information Security in China, 2018 (12): 105-106.
12. Xiang Liling, Gao Qianyun. Analysis of the characteristics, basic attributes and contents of personal data rights in the era of big data [J]. Information Theory and Practice, 2018,41 (9): 45-50 + 36.
13. Li Liangwei. The feasibility analysis of data right confirmation was conducted by referring to the intellectual property legislation model [J]. Henan Science and Technology, 2021,40 (32): 154-158.
14. Ren Ying. Turn to data legislation: from data rights entry to data legal interests protection [J]. Politics and Law, 2020 (6): 135-147.
15. Li Yuan. Research on the basic principles of legal protection of personal information in the Era of Big Data [J]. Legal system and Society, 2020 (23): 10-11.
16. Miri. Research on the legal control of data acquisition and operation on privacy impact [J]. Journal of Southeast University (Philosophy and Social Sciences edition), 2018,20 (S2): 96-99.

 doi:10.20944/preprints202402.1062.v1

17. Yang Bo, Dai Rui, Chen Wu. Research on data security and backup technology in electric power communication system [J]. Automation Technology and Applications, 2018,37 (6): 36-41 + 59.
18. Cheng Lin, Huang Guangyu, Wang Zheng, et al. Research on big data pricing mechanism and transaction mode based on blockchain [J]. National circulation economy, 2019 (22): 132-135.
19. Zuo Weimin. Towards Big Data legal research [J]. Legal Studies, 2018,40 (4): 139-150.
20. Li Yongming, Dai Minmin. Research on the right attribute and legal protection of big data products [J]. Journal of Zhejiang University (Humanities and Social Sciences edition), 2020,50 (2): 26-37.