Regulation Practice and Prospect of Privacy Protection of Data Flows in China

Liping Yang , Yiling Lin , Bing Chen *

Posted Date: 10 September 2024

doi: 10.20944/preprints202409.0751.v1

Keywords: data flows; privacy protection; legislative framework; judicial practice; technical measures

Article

Regulation Practice and Prospect of Privacy Protection of Data Flows in China

Liping Yang [1], Yiling Lin [2] and Bing Chen [2,*]

[1] Center of Competition Law, Fuzhou University School of law, Fuzhou 350001, China
[2] Center of Competition Law, Nankai University School of Law, Tianjin 300350, China
* Correspondence: bing.chen@nankai.edu.cn

Abstract: Privacy protection is a fundamental guarantee for secure data flows and serve as a basic requirement for data security. A reasonable privacy protection system acts as a catalyst for unlocking the financial value of data. The current legislative framework for privacy protection in data flows in China, adhering to the principle of proportionality, establishes the "informed-consent" rule for data collection and processing, data classification and grading management measures, and remedies for data leakage and other risks. In addition, in judicial practice, typical disputes regarding personal information protection and privacy rights have promoted to clarify the scope of collecting user personal information and biometric data. Despite ongoing improvements needed in legislative, judicial and technical approaches to data privacy protection, China's commitment and practice in privacy protection of data flows are noteworthy. The existing legislation, law enforcement and technical practices are playing an increasingly vital role in realizing the financial value of data and are essential for international cooperation on data privacy protection. Furthermore, it is crucial to actively explore cooperation mechanism for cross-border data flows under the principle of data sovereignty, participate in developing international rules for cross-border data flows, and formulate different management norms for cross-border circulation of data in different industries.

Keywords: data flows; privacy protection; legislative framework; judicial practice; technical measures

1. Introduction

As a new factor of production, data has profoundly transformed the way of production, life and social governance, becoming a critical element in enhancing the core competitiveness of enterprises and unlocking the potential of market economy. In China, where the digital economy is rapidly expanding, data serves as a new production factor, contributing to the formation of new quality productivity [1]. In December 2023, China's Central Economic Work Conference highlighted the importance of "addressing issues related cross-border data flows" to promote high-quality economic development. Subsequently, in January 2024, 17 Chinese departments jointly issued the "Data Element X" Three-Year Action Plan (2024–2026), which advocates for the promotion of data application scenarios, improvement of resource allocation efficiency and cultivation of new growth drivers to achieve multiplier effect on economic development [2]. Currently, China has implemented numerous policies aimed at advancing the development and utilization of data elements. The market scale of the data exchange industry has reached RMB 87.68 billion in 2022 [3], approached RMB 120 billion in 2023, and is projected to RMB 150 billion by 2024 [4]. These figures demonstrate vigorous progress being made in data flows within China.

Privacy protection, as a fundamental safeguard for secure data flows, embodies the essential requirements of data security and enables efficient data flows. Without sufficient emphasis on privacy protection of data flows, there is a risk of data falsification, leakage, or destruction, which could infringe upon individual privacy [5]. In recent years, China has enacted several laws to protect personal data privacy, including the Cybersecurity Law and the Personal Information Protection

 doi:10.20944/preprints202409.0751.v1

Law, all of which mandate the "informed-consent" for data collection and processing. In addition, the integration of privacy protection into the Anti-Monopoly Law and the development of remedies for data privacy violations have sparked significant discussion in China. Despite these efforts, there are still many privacy leakage incidents in practice, which is mainly due to the fact that the legislation on data privacy protection is not yet perfect, coupled with the incomplete legislative framework for data privacy protection and the under-utilization of civil public interest litigation and other judicial systems,leading to the low willingness of data enterprises and individuals to circulate, and ultimately affects the release of the value of data.This paper examines the fundamental role of data privacy protection in enabling secure data flows and analyzes the current legislative framework and judicial practices in China. By the examination and analysis, this paper concludes that the key to fully realizing the value of data lies in the development of more comprehensive legal systems for data privacy protection, the enhancement of judicial systems for anti-monopoly civil public interest litigation, the advancement of technical approaches for data flows tracking and the exploration of cross-border data flow mechanisms at the international level.

2. Privacy Protection as the Fundamental Guarantee of Data Flows

The privacy protection system is the core system to promote secure data flows. In addition to facilitating secure data flows, a complete privacy protection system elevates the commercial value of data, helping data fully release its value in secure circulation.

2.1. Promoting Secure Data Flows

The "Data Element X" Three-Year Action Plan (2024-2026) jointly issued by 17 departments states that "we will implement the data security laws and regulations, improve data classification and grading protection systems … strengthen the personal information protection and improve the capability of data security guaranty" [6]. The statement demonstrates the necessity of data security and personal information and privacy protection to release the value of data. All participants in data trading must be responsible as personal information processors and fulfill their obligations of protecting personal information in accordance with the law [7].

In practice, data anonymization is the most effective way to protect privacy. Since it is almost impossible to identify specific natural persons after anonymization, the security of personal information is maximized and personal information is avoided from being leaked, which facilitates more secure data flows. In the healthcare industry, the government grants the property rights of public medical data that is personal medical data collected by the government departments to market players under the authorized operation mechanism, and market players then develop medical data products for circulation and trading after anonymizing the public medical data [8]. For instance, the Xiamen Municipal Health Commission authorized the Xiamen Health and Medical Big Data Co., Ltd. to develop medical data products by incorporating medical data elements, as a result, a real-world research data product on endocrine and metabolic diseases have been successfully traded on the Fujian Big Data Exchange in March, 2024 [9]. In this transaction, Xiamen Health and Medical Big Data Co., Ltd. is the product provider, Beijing Intelligent Decision-Making Medical Technology Co., Ltd. is the demander, and Fujian Big Data Exchange guarantees the transaction processes as a platform. All data products traded on Fujian Big Data Exchange Province comply with the principle of legality and compliance in the whole process of data collection, convergence, cleaning, analysis, sales, purchase and application, and are used without being seen to ensure the data security privacy respect.

The Business Procedures on Data Cleaning, De-identification and Anonymization (for Trial Implementation) states that "regulating data cleaning, de-identification, and anonymization helps to enhance the data availability, credibility, circulation and traceability, and promote the advanced and high-quality supply of data elements, making a significant contribution to establishing a compliant, efficient, and exchange-trading and over-the-counter combined data element circulation and trading system" [10]. It can be said that de-identification and anonymization are the precondition for data products to be listed, the prerequisite for data asset registration and trading, and the principle for

 doi:10.20944/preprints202409.0751.v1

data application and unlocking secondary derived value in modeling. The first reason is that data cleaning ensures data usability. Data cleaning is the process of using a certain method to correct the identified data problems and identify the standardization, completeness, consistency, accuracy and accessibility of the data to improve the data quality. As the foundation of subsequent data development and utilization, data cleaning is conducted followed by data de-identification and anonymization. The second reason is that de-identification is the key to data desensitization. Data de-identification is the process of processing data and disabling data to identify associated identifiers of a specific natural person without additional information. Data de-identification emphasizes the "unidentifiability" of identifiers, that is, the relevant information content of data is desensitized, such as by removal, replacement and fuzzy replacement, to achieve the effect of identifying a specific natural person or related identifiers without using additional information.

Both data cleaning and data de-identification aim to anonymize data. Anonymization is the reinforced version of de-identification, emphasizing that data identifiers should meet the criteria of "irrecoverability" not only "unidentifiability" as the further processing of data de-identification. Since the difficulty for anonymized data to identify a specific natural person and a processed identifier even using additional information, anonymized data is no longer treated as personal information and can be traded as a data product. Currently, data anonymization is a key object in compliance review in China`s provincial data trading practice . Data products without going through the anonymization process cannot pass a compliance review, nor can they be traded on data exchanges.

2.2. Enhancement of Commercial Value of Data

The most important economic characteristics of data are low marginal cost and higher fixed cost, in other words, the cost of data generation is high, while the cost of data reproduction is minimal [11]. Commercial value refers to the actual or potential economic benefits brought by current or future use of data to right holders. The most essential aspect of commercial value is reflected on that right holders maintain their competitive advantage because of their holding of data. The commercial value of data is an inevitable connotation of data flows, and data without commercial value has no need to be circulated. As for the current local practices of data intellectual property registration in China, it is stipulated that the object of data intellectual property registration should be the data or datasets with commercial value. Although local normative documents use different expressions, for example, some using "commercial value" [12] and some using "practical" [13], practicality and value are closely related to each other, with practicality as the basis of value; without practicality, there is no value, and value is the result of practicality [14]. Paragraph 4 of Article 9 of the new Anti-Unfair Competition Law uses the expression "with commercial value" to replace the previous expression of "capable of bringing economic benefits to the right holder and is practical", indicating that practicability has the same connotation as commercial value [15].

In addition, the element value of data in different scenarios is different, and the element value of the same personal data or a group of personal data in different scenarios also varies. Data privacy protection is achieved through anonymization, and anonymized data can promote the commercial value of data, unlocking the scenario value in different scenarios. For example, applying unified health and medical data to three different scenarios, i.e., the precise delivery of health and medical advertisements, the development of health insurance products, and health and medical services, generates different values [16]. However, failure to protect data privacy may reduce the commercial value of data and is prone to data infringement disputes, causing the data transaction parties to be liable for damages and further reducing the commercial value of data products.

3. China's Regulatory Framework for Privacy Protection of Data Flows

China attaches great importance to the protection of data privacy. In this respect, a series of laws and regulations have been introduced, and major guidance cases have been published in judicial practice.

 doi:10.20944/preprints202409.0751.v1

3.1. Basic Legislative Framework

3.1.1. Purpose of Data Collection and Processing: Following the Principle of Proportionality

Article 6 of the Protection of Personal Information Law provides that the collection of personal information shall be limited to the minimum scope for the purpose of processing and shall not be excessively collected and that processing of personal information shall be in a manner that has the least impact on individual rights and interests. Both Article 1035 of the Civil Code and Article 32 of the Data Security Law state that the collecting of data shall be in compliance with the principles of lawfulness and justification and the data shall be collected and used within a necessary limit.

It can be seen that China's legislation expressly provides that data collection and processing shall be subject to the principle of minimum necessary. This means that data controllers and processors must collect personal data only for specific, definite and legitimate purposes and process the data collected in a manner consistent with the original purposes [17]. The principle of minimum scope requires data collectors to inform the person whose data is collected of the purpose of data collection and not to use data beyond the agreed scope of purposes [18]. The reason for this limit is that the illegal processing of personal information intends to be an excessive collection of personal information, and the personal information excessively collected often encounters the risk of illegal trading or leakage; therefore, it is necessary to limit the scope of collecting personal information into the minimum scope for realizing the purpose of processing.

The purpose of data collection and processing should be justified, legitimate and reasonable.Both the principle of minimum scope of purpose and the principle of minimum necessity belong to the principle of proportionality; the principle of proportionality implies the theory of cost-benefit; the scope of data collection and processing should be limited to what is necessary to achieve the stated purpose, and at the same time, the means of collection and processing that minimize the damage to the rights should be adopted, so as to achieve a balanced effect of benefit and gain, in order to comply with the requirements of the principle of proportionality.

3.1.2. Requirements for Data Collection and Processing: "Informed-Consent"

"Informed-consent" rule has always been the basic requirement for data collection and processing in China, and is also a core principle in the field of data protection. At the stage of data collection, the data collector shall, in line with the principle of "informed consent", promptly and accurately disclose the processing of scope, methods and purposes of data. Article 1035 of the Civil Code states that the processing of personal information shall comply with the principles of lawfulness, and justification, and within a necessary limit, with the consent obtained from the natural person. Paragraph 1 of Article 14 of the Personal Information Protection Law provides that the processing of personal information is based on the consent of the individual concerned and such consent shall be given by the individual concerned in a voluntary and explicit manner in the condition of full knowledge.According to the above provisions, consent grants the personal information processor a legal basis for collecting and processing information. Item 1 of Article 1036 of the Civil Code provides that the information processor does not bear civil liability if processing information to the extent as consented by the natural person or their guardian. Such consent eliminates the illegality of information processing and is an exemption cause of personal information processing. Data use beyond the consent boundary is invalid and shall be informed again to obtain consent.

Utilization beyond the boundary of consent is invalid, and consent should be re-informed and obtained for utilization beyond the boundary of consent. However, there are exceptions to the rule of "informed-consent", and the government may collect and process personal data beyond the scope of "informed-consent" on the premise of realizing the public interest. The "public interest" can be regarded as an exemption from "informed-consent". In this case, the individual's interest gives way to the public interest, and the individual's interest is appropriately weakened so as to realize the public interest of society.

 doi:10.20944/preprints202409.0751.v1

3.1.3. Measures for Data Collection and Processing: Classification and Grading Management

Data classification and grading is the starting point for secure data flows and security governance [19]. Article 21 of the Data Security Law provides that the state shall is to establish a protection system of data classification and grading [20]. Article 51 of the Personal Information Protection Law stipulates that personal information processors shall implement classification management of personal information [21]. Articles 5, 9, and 26 of the Administrative Regulations on Network Data Security (Draft for Comment) further clarify the detailed management measures for data classification and grading [22]. In general, China's regulations classify data as "personal information" and "important data", adopt a dual-track regulation mode for personal information and important data protection system, and divide data into different security levels based on the sensitivity of data and the degree of harm to national security, social order, public interests and the legitimate rights and interests of citizens, corporations and other organizations in the event of data leakage and destruction. China has thus established a set of management systems of data classification and grading which is coordinated at the central level and implemented based on type of industry standards to realize data privacy protection.

3.1.4. Remedies for Data Flows: Notification – Protection

Article 57 of the Personal Information Protection Law provides that, where personal information has been or may be falsified, leaked or lost, the personal information processor shall take remedial measures and inform the departments and persons owing protection duties of the types of information leaked the causes and the possible harm of information leakage, the remedial measures taken by the personal information processor and the measures taken by individuals to mitigate the harm, and the contact information of the personal information processor. According to the above said provision, "informing" departments and individuals owing protection duties is the obligation of the information processor to be fulfilled in the event of security risks being exposed by data. Paragraph 2 of Article 1038 of the Civil Code provides for an information processor's stop-loss obligation, that is, in the event data is exposed to a leakage risk, the information processor shall promptly inform and report the data security supervisor and the data holder of such risk and take preventive measures to prevent second damage to the data [23]. However, there are no provisions on specific remedial measures but only a "notification–protection" framework.

3.2. Typical Judicial Practice

3.2.1. Extent to the Collection of User Personal Information

In a personal information civil public interest litigation case brought by the People's Procuratorate of Yuhang District, Hangzhou City against a network technology company limited (hereinafter referred to as a "network technology company's personal information civil public interest litigation case"), the involved application is a video mobile application of music teaching developed and operated by the defendant, the network technology company with the main function of popular musical instruments teaching through livestreaming courses. The application falls into the following illegalities and irregularities circumstances in respect of user personal information during the installation and use process: (1) the application fails to display the privacy policy in the process of downloading, installation and use, fails to prompt the users to read the privacy policies or other rules for personal information collection and through pop-up window or other obvious ways, and has no specific content of privacy policies; (2) the application refuses to provide business functions on the ground of users disagreeing the collection of unnecessary personal information or opening unnecessary authorities; and (3) the application fails to synchronously inform the users of the purposes, methods and scope of the information collection when applying for accessing to sensitive personal information including users' whereabouts and tracks.

The court held that: (1) the company violated the principle of "informed consent" due to the application failing to display the privacy policy, prompting the users to read privacy policy in an obvious way, and synchronously informing the users of the purposes, methods and scope of

 doi:10.20944/preprints202409.0751.v1

collection when collecting the users' personal data; (2) the application violated the principle of minimum scope due to its failing to inform the users of the purposes, methods and scope of collection when applying for accessing to sensitive personal information including the users' whereabouts and tracks, and failing to provide business functions on the ground of users disagreeing the collection of unnecessary personal information or opening unnecessary authorities [24]. This case reflects the feasibility and necessity of procuratorates to file civil public interest lawsuits for personal information protection in the field of consumption in the event of the damages of public interests caused by the infringement upon consumers' personal information. In addition, this case reviewed the mobile application's illegal behavior, including failure to release its privacy policy as required and follow the preparation requirements of a privacy policy, compulsory authorization, excessive access, and collection of personal information beyond a proper scope, and clarified the boundaries and scopes of the above behaviors.

3.2.2. Boundaries of the Biometric Information Collection

Biometric information is sensitive personal information due to its uniqueness and inability to be altered. An irreversible damage to the biometric information holder if a data collector collects biometric information beyond a proper scope, therefore, biometric information should be protected under a higher-level protection and collected within a more precise boundary. In the case brought by Guo against a safari park, China's first case on facial recognition, the safari park required Guo to input his facial recognition information on the ground that "the original fingerprint identification method was no longer adapted to enter the park, and those without registering in the facial recognition system will not be allowed to enter the park". Guo believed that the facial recognition information was highly sensitive personal privacy, and refused to input his facial recognition information and requested the park to refund. The Intermediate People's Court of Hangzhou held that the safari park intended to expand the scope of information processing beyond the prior agreed collection using the photos collected and requested the park to delete Guo's facial information. The court of first instance ruled that the safari park should delete Guo's facial recognition information based on the fact that the park breaching the agreed information collection and processing scope [25]. The court of second instance made it clear that "biometric information, as a type of sensitive personal information, thoroughly reflects the physiological and behavioral characteristics of natural persons with its strong personality attributes, and may lead to discrimination or accidental damages to personal or property safety if being leaked or illegally used; therefore, it is necessary to exercise more prudence and take more stringent protection measures in collecting and using biometric information", and ruled that the safari park should delete Guo's fingerprint identification information [26]. This case is a service contract dispute caused by an operator's collection and use of a consumer's biometric information to verify identity. The trial of this case embodies preliminary discussion on the legitimate use of biometric information in the field of consumption, explored and tried the rules of the deleting personal information under the existing legal framework, and responded to the actual needs of reasonable protection of personal information in the digital economy.

3.2.3. Summary and Analysis: Fewer Civil Public Interest Litigation Cases on Privacy Protection

In the network technology company's personal information civil public interest litigation case, civil public interest litigation instituted by the procuratorate serves as a significant relief method to safeguard the legitimate rights and interests of personal information. In the case of Guo v. Safari Park, Guo pursued private relief for the legitimate rights and interests of personal information through civil private interest litigation. Both cases highlighted disputes concerning the definition of the "minimum scope" of data collection and processing. The cases demonstrated that the principle of "minimum scope" is challenging for data collectors and processors to fully comprehend in practice. The primary distinction between the two cases is the methos employed to protect the legitimate rights and interests of personal information, with the former utilizing public relief through civil public interest litigation and the latter opting for private relief via civil private interest litigation.

 doi:10.20944/preprints202409.0751.v1

The table below summarizes the number of cases on personal information protection and privacy rights handled by Chinese courts from pkulaw.com [27], which provides a general overview of the specific ways of privacy protection of data flows. It should be noted that, as the Supreme People's Court classifies "personal information protection" and "privacy rights" as one type of cause of action as provided for the Regulations on Causes of Action of Civil Cases (2020) [28], the case retrieval was implemented by using pkulaw.com's judicial cases database in the following steps: conduct a preliminary retrieval with "privacy rights" as key words of "cause of action", then limit the scope to "disputes over personal rights", and finally choose "personal information protection" with a prescribed starting year of "resent four years". This approach helps better focus on cases covering both privacy rights and personal information protection.

Table 1. Number of Cases with the Cause of Action of "Personal Information Protection and Privacy Rights" Handled by Chinese Courts from January 2021 to June 2024 (Unit: piece).

	Yea	2024	2023	2022	2021	Total	
Types of Judicial Documents	Judgments	2	22	53	57	134	277
	Letter of Ruling	5	36	62	40	143	
Mode of Litigation	Civil Private Interest Litigation	7	58	102	97	264	277
	Civil Public Interest Litigation	0	0	13	0	13	

*Data source: pkulaw.com.

A survey of the cases with the causes of action of "privacy rights" in China in the past four years shows the following findings. (1) There are few cases in which disputes over privacy protection of data flows are submitted through civil public interest litigation. From January 2021 to June 2024, there were 277 cases with the cause of action of "personal information protection or privacy rights", among which 264 cases were filed through t civil private interest litigation, accounting for 95.31%, and 13 through civil public interest litigation cases, accounting for 4.69%. Most of the cases with the cause of action of "personal information protection and privacy rights" are filed through civil private interest litigation as a relief. Under private interest litigation, the individual citizens have limited ability, while personal information holders have a higher litigation status and stronger economic ability than the individual citizens, which may lead to difficulty for the citizens in obtaining reasonable relief through private interest litigation in the cases on privacy rights. However, in practice, few cases are filed through civil public interest litigation to protect personal privacy, which shows that civil public interest litigation has not been given full play privacy protection in data flows. (2) A high proportion of cases are closed by withdrawing claims. Among the 277 cases, 134 cases are closed, accounting for 48.4%, and 143 are closed by ruling, accounting for 51.6%. According to the rulings, over half of the cases are closed by withdrawing claims. The high proportion of cases closed by withdrawing claims to some extent reflects the difficulty in the evidence presentation by individuals in civil private interest litigation and reveals a long way to go to improve the judicial protection of data privacy.

4. The Prospect and Expectation of Privacy Protection in Data Flows in China

4.1. Legislation Perspective: Increasing Institutional Supply

4.1.1. Clarifying the Standards for Data Anonymization and Comply with the Principle of Proportionality

Data anonymization is a key link in the process of data flows, while there is no unified standard for data anonymization. Even if all parties prudently fulfill their data protection obligations in the process of data flows, data may still be exposed to security risks. Therefore, it is necessary to profoundly understand the meaning of "anonymization" referred to in the Personal Information Protection Law which means the cleaning of relevant data sets to remove the information contained

 doi:10.20944/preprints202409.0751.v1

in data sets that is related to specific individuals, affirm the positive aspect of using and circulating data, and specify that anonymized data may be circulated without the permission of specific individuals to the extent of complying with the Personal Information Protection Law. The Implementing Guides for Data Anonymization Processing are to be introduced in Beijing [29]; however, such guides are applicable in local but not in the whole country. In the future, the state may consider introducing unified Implementing Guides for Data Anonymization Processing, unifying the standards for data de-identification, adopting an anonymization standard for unrecoverable desensitization, and seeking the critical point for the protection of personal data privacy and the full release of data value under the anonymization standard for unrecoverable desensitization.

Completely anonymizing data is technically challenging, but it is both feasible and reasonable to anonymize data following the principle principle of proportionality [30]. The principle of proportionality looks at the link between ends and means.That means the collection, processing and use of data must be confined to the minimum necessary scope of purposes, with any data falling outside this scope being fully anonymized. It should also follow the principle of minimum necessity, choosing the anonymity that minimizes the impact on the individual and achieves "Pareto optimality". For instance, for medical data, patients' privacy protection can be bordered by the safeguarding of their sensitive personal information which refers to the personal information that can be used to accurately identify the related patients when combined with patients' other information. Given that the scope of sensitive personal information defines the boundary of a patient's privacy protection, medical data should only be circulated after the sensitive information has been anonymized.

4.1.2. Strengthening Enterprises' Disclosure Obligations and Optimizing the "Informed-Consent" Rule

The informed-consent rule is a fundamental precondition for data collection and usage in the digital economy and a cornerstone for personal information protection. At the stage of data collection, to adhere to the informed-consent rule, data collector must promptly and accurately disclose the processing scope, method and purposes of data. However, in practice, the implementation of the informed-consent rule often devolves into formalism, necessitating further clarification of enterprises' disclosure obligations under this rule. For example, in the realm of medical data, especially biogenetic data, information is frequently collected without a clear intended use in medical research and may be repeatedly employed in various research studies. This creates a challenge for medical data collectors, who may be unable to precisely determine the extent of consent previously granted, thereby complicating the application of the traditional informed consent rule.

The "generalized informed-consent" rule is a better way to promote data flows than the traditional "informed consent". Under the generalized informed-consent mode, data collectors are required to inform the collected persons that their data will be used in future scientific research activities that do not need to obtain the collected persons' consent again when conducted; in other words, one consent of the collected persons can be applied to all future ethical, moral and legal scientific research activities. The generalized informed-consent rule enables data collectors and data users to save notification costs facilitates the development of scientific research activities [31].Considering the potential infringement by generalized informed-consent" upon patients' privacy, the author suggests a provision relating to "strong disclosure obligations of data collectors and processors, and strengthening of the obligations of data holders and users in disclosing the scope and methods of data use" to be added in the Data Security Law, expecting change the generalized informed consent rule from a one-time informed consent to a long-term informed consent. By the above means, In the case of the exposure by data to leakage risks in use, individuals will have the right to withdraw their consent or re-authorize consent and the right to limit the scope of use of data, so as to protect the legitimate rights of individuals to the greatest extent, and refrain data users obtaining generalized consent from using data by blur the scope of use of data to improperly circulate data which may infringe upon individuals' privacy or public interests.

 doi:10.20944/preprints202409.0751.v1

4.1.3. Refining Classification and Grading Standards and Developing More Types of Protection Measures

Reasonable data classification and grading standards are the basic guarantees for secure and efficient data flows [32]. The most important aspect of data classification is to distinguish key data, core data and general data, and to give higher-level protection to key data and core data. The Data Security Law, the Personal Information Protection Law and other laws then in effect provide general provisions on data classification and grading; while the Data Security Technology — Rules for Data Classification and Grading jointly issued by the State Administration for Market Regulation and the Standardization Administration of China on March 15, 2024 defines the data classification rules in terms of the framework and methods for data classification, specifies the methods for the data classification, and clarifies the specific procedures for data classification and grading [33]. In practice, there are also many data classification and grading standards for various industries, such as the Information Security Technology — Guide for Health Data Security, the Guide for the Development of Industrial Data Security Standards System (2023), and the Provisions on the Administration of Data Security (for Trial Implementation). The data classification and grading are conducted to apply appropriate levels of protection measures to various categories and grades of data; therefore, it is necessary to refine the data classification and grading standards in light of specific scenarios and industries, highlight the identification of key data, core data and the general data containing personal information in the data classification and grading standards, and refine the protection of data security and data privacy [34]. Based on the concept of data classification and grading, general data containing personal information can be protected by being divided into sensitive personal information and non-sensitive information and attaching importance to the exercise of personal data rights and interests and the protection of personal privacy. The personal data processors are expected to apply different processing standards and protection methods for personal sensitive information and non-sensitive information, further fulfill their responsibilities and duties, protect data privacy to the maximize extent, and improve the efficiency of and maintain the security of data flows.

4.1.4. Connecting Multiple Regulators and Building a Collaborative Mechanism

Generally, information processors are supposed to take remedies including notice–deletion and repairing vulnerabilities; data platforms are supposed to be obliged to protect information security, enhance the accountability system, connect the risk of data leakage with legal risks, and urge data platform personnel and data processors to intensify the protection of data privacy. In addition, local governments are suggested to establish a collaborative supervision mechanism for data privacy protection to further promote the protection of data privacy. The collaborative supervision mechanism for data privacy protection may be composed of administrative departments such as competition enforcement authorities, consumer protection authorities,the administrative departments for technical prevention, county/district people's governments, and Industry sectors with supervisory and management responsibilities, with the county/district people's governments playing a leading role in the collaborative supervision mechanism, collaborative enforcement by other sectors to supervise the compliance by data collectors and data processors with the relevant standards.

4.2. Judicial Perspective: Introducing Anti-Monopoly Civil Public Interest Litigation to Protect Data Privacy

4.2.1. Data Privacy as a Non-Price Competition Factor

The fundamental goal of the anti-monopoly laws is to protect competition, and consequently, anti-monopoly remedies are established based on injury to competition. This means that the inclusion of data privacy in the scope of anti-monopoly protection must follow anti-monopoly laws' main goal of protecting competition and specifying of the injury to data privacy and specific injury to competition. However, it is still difficulty to evaluate the impact of operators' conduct on market competition from the dimension of data privacy.

 doi:10.20944/preprints202409.0751.v1

Although controversial, data privacy has become an important non-price competitive factor in the digital economy. Traditional competition violations tend to result in tangible economic damages, such as excessive payments made by consumers due to high prices, which are easier to assess and quantify. However, in terms of user satisfaction, updating iteration speed, ease of use, efforts of privacy protection, amount of advertising and other quality measurement indicators, anti-monopoly law enforcement agencies are particularly expected to pay attention to the level of data privacy protection [35]. As privacy data has become an important competitive resource of digital platform companies, users make decisions on accepting the services or products from the platforms relying on the extent of privacy protection. In other words, data privacy protection has become an indicator to measure the quality of digital platform companies' products and services, reflecting the competitive advantage of the companies to attract consumers to choose from their products and services.

4.2.2. The Public Dimension of Violations of Data Privacy

With the continuous development of the modern market economy and the emergence of new forms of disputes, civil public interest litigation is playing an increasingly important role in privacy protection in data flows. The determination of an act harming the public interest should be based on potential risks or actual damages imposed by the act on non-specific consumers. Improper user portrait behavior in the field of the digital economy infringes upon the legitimate rights and interests of non-specific online consumers. In this field, improper collection by platforms of user portraits is typical behavior that may infringe upon the legitimate rights and interests of non-specific individuals. User portrait is a process of forming a model reflecting users' personal characteristics by collecting, aggregating and analyzing personal information and analyzing or predicting the personal characteristics of a specific natural person, which has obvious personal characteristics [36]. Due to its ability to provide precise services based on individual characteristics, user portrait is an effective channel for digital economy enterprises to push their business information. However, this process can easily infringe upon the privacy rights of non-specific consumers, the fundamental reason of which is that the balance of information between data collectors and users is disrupted. Specifically, data collectors can achieve precise digital recordings of the virtual space addresses and time nodes of user portraits by using algorithms, while consumers are unable to perceive these actions. Therefore, given the extensive sources of user portrait data and numerous consumers involved, improper collection and processing of data may damage the privacy of non-specific consumers and further damage the public interest.

In March 2023, the Supreme People's Procuratorate published the Typical Cases on Procuratorial Public Interest Litigation for Personal Information Protection, revealing a batch of typical cases [37]. In the personal information protection laws and the judicial practice of public interest litigation, the public interest attribute of personal information protection has been legally confirmed.

4.2.3. Implementation Path of Anti-Monopoly Public Interest Litigation for Data Privacy

The harm to competition addressed by the Anti-Monopoly Law is linked to the harm to public interests in public interest litigation. The amended Anti-Monopoly Law of China first clearly provides for the explicitly introduces the system of civil public interest litigation in anti-monopoly cases. It stipulating that "where undertakings engage in monopolistic practices and harm the public interest, the people's procuratorates at or above the level of city divided into districts may institute civil public interest litigation to the people's courts in accordance with the law" [38]. In addition, the Notice on Implementing the Anti-Monopoly Law of the People's Republic of China and Actively and Steadily Carrying out Public Interest Litigation Procuratorial Work in the Anti-Monopoly Field issued by the Supreme People's Procuratorate emphasizes the importance of fully understanding the significance of these new provisions on procuratorial public interest litigation. The notice calls for targeted efforts in anti-monopoly public interest litigation, particularly in cases of serious infringements on consumer rights and interests [39]. In this context, the scope of damage to competition under the Anti-Monopoly Law is expected to be appropriately adjusted and expanded, especially in relation to the digital economy and individual cases . The assessment of price

 doi:10.20944/preprints202409.0751.v1

competition factors could be given greater consideration, including the analysis of specific harms related to data privacy protection and consumer choice. Beyond the traditional focus on economic efficiency under anti-monopoly competition damage theory, the acceptance scope of anti-monopoly civil procuratorial public interest litigation should be broadened. This expanded scope would encompass monopoly behaviors, including platform monopolies, that may cause may harm broader public interests such as the right to fair transactions, consumer choice, personal information rights, and public health. Such an approach aligns with the role of prosecutors as representatives of public interests [40].

Article 60 of the Anti-Monopoly Law states that the people's procuratorates at or above the municipal level of the districts in which they are located may initiate anti-monopoly civil public interest litigation.This provision limits the prosecutors of anti-monopoly civil public interest litigation to the people's procuratorates at the level of municipal city and above, avoiding abuse of litigation, but also falling into the drawback of too narrow a scope of prosecutors of anti-monopoly civil public interest litigation. In the area of consumer protection, the Interpretation by the Supreme People's Court of Several Issues Concerning the Application of Law to the Trial of Cases of Civil Public Interest Litigation in Consumption states that consumers associations may file consumer-related civil public interest litigation against business operators who infringe upon the rights and interests of numerous non-specific consumers or engage in other actions damaging the public interest [41]. Filing public interest litigation enables consumers associations to safeguard the legitimate rights and interests of consumers. The participation of consumers associations in consumer public interest litigation and the favorable social benefits they obtained also provide a useful reference for developing the anti-monopoly civil public interest litigation in data privacy. In the future, consumers associations may be considered included in the scope of prosecutors to work together with procuratorial authorities to protect consumers' data privacy.

4.3. Technology Perspective: Establishing Data Flows Tracking Systems

Tracking of data flows is of positive significance for the protection of the security of the subject data, the assurance of the data flows within a reasonable scope, and the protection of the legitimate rights and interests of the data stakeholders. Establishing data tracking guarantee mechanism helps ensure more secure data flows. The author suggests adding provisions on the data flows tracking system, determining various data tracking subjects under the overall planning and coordination of competent authorities, defining the scope of data tracking and providing for the processing method for derivative data tracking in the Guide for the Security of the Cross-domain Control of data flows.

4.3.1. Clarifying Multi-Party Tracking Subject

The requirements of classification and grading management of data security protection are suggested to be improved at the national level, together with a data leakage notification system and the supporting data leakage regulations or guides to be formulated. The provincial data administrations may act as tracking subjects of data flows to share data on the provincial government information resources sharing website, public data opening network and other data platforms. In addition, as data flows involves anti-monopoly supervision, consumer protection and the protection of data rights and interests, data tracking subjects should also include cyberspace administrations, market regulation administrations and other administrations. The provincial data bureau should play the role of overall planning and coordination in data flow tracking, and may, for example, establish a system of joint working meetings on data flows which may be convened and presided over by the provincial data bureaus [42].

4.3.2. Authorizing Trackable Scope

In the process of tracking data flows, tracking entities shall comply with Article 27 of the Cyber Security Law without engaging in any activities endangering cyber security, such as stealing network data, and shall ensure that the tracking technologies they apply do not steal network data outside the

 doi:10.20944/preprints202409.0751.v1

agreed scope of tracking [43]. If, in the process of tracking, machines automatically capture the network data outside the agreed tracking scope, the tracking entities shall immediately inform the transaction subjects and relevant departments. Provincial data bureaus shall, following the requirements of classification and grading protection, take relevant technical measures for security protection of data to prevent data loss, falsification or leakage. Meanwhile, the data of the relevant database shall be supplemented completely in a timely manner, and a subject database and a label database of data information shall be established.

4.3.3. Stipulating the Ownership of Derivative Data

Derivative data, derived in the process of informatization, have product value and intellectual achievements in nature. To some extent, derivative data reduces the data risks of the connection between personal interests and public interests and satisfies the interest demand of data buyers in purchasing data [44]. In order to better protect the tracked derivative data and prevent the misuse of the tracked data, the ownership of and the permission to use the tracked derivative data should be clearly stipulated in the relevant transaction documents. The derivative data generated in the data flows tracking shall be independent of the data subjects, and the right to the derivative data shall belong to the prior two parties to the data transactions. The subjects implementing data tracking may not use the tracked derivative data without permission.

4.4. International Perspective: Exploring a Cooperation Mechanism for Cross-Border Data Flows

4.4.1. Establishing a Safety Valve Mechanism for Cross-Border Data Flows under the Principle of Data Sovereignty

The concept of “data sovereignty” has gained significant recognition at the national level in China in recent years. In August 2015, the State Council issued the Outline for Promoting the Development of Big Data, which highlighted the importance of “data security”. Although the Data Security Law does not explicitly mention “data sovereignty,” Article 1 emphasizes the safeguarding of national sovereignty, implicitly affirming China’s claim to sovereignty over data. Adhering to the principle of data sovereignty is essential in promoting data flows, thereby enhancing both the commercial and public value of data. During cross-border data flows, it is crucial to remember that the country state retains sovereignty over its data, allowing data to circulate flows inward or outward. China’s National Security Law stipulates that cross-border data transfers must not endanger national security and establishes the principle of “informed-consent” for such transmission. Furthermore, the Guide for Data Export Security Assessment (Draft for Comments) provides national standards for assessing the security of data exports. As data flows continues to drive the growth of data-related industries, China should strengthen the security management of cross-border data transfer, uphold the principle of national data sovereignty, clarify its sovereignty over data, optimize the allocation of data resources, and strike a balance between cross-border data flows and localized data storage.

The establishment of a safety valve mechanism for cross-border data flows under the principle of data sovereignty aligns with China’s foreign policy position. This mechanism would not only facilitate the orderly circulation of data but also prevent the country’s key data (such as those containing ethnic and genetic information) from being transmitted abroad. Before engaging in cross-border circulation of data, data users should first undertake self-examination and self-assessment. First, it is recommended that a classification and grading management scheme for cross-border data be formulated. In the measures, the types of data that can be circulated across borders and the types of data that are prohibited from cross-border circulation should be clearly defined, white lists and negative lists for cross-border circulation of data should be established, and negative lists should be set up for behaviors that may hinder the free flow of data across borders, such as information leakage and unfair competition of data.[45]Secondly, data need to undergo self-audit assessment and external audit assessment before cross-border circulation. On the one hand, data-using subject should first carry out self-audit assessment. This can ensure that the data have been anonymized and de-

 doi:10.20944/preprints202409.0751.v1

identified, and will not infringe on individual privacy; it can also ensure that the data to be circulated across borders do not contain important data such as ethnogenetic information,and ensure that the data circulated across borders will not threaten national security when it flows out of the country. On the other hand, the supervisory authority will conduct external audits on the data to be circulated across the border. The content of the audit mainly includes whether the data have been de-identified, whether they contain important data related to genetic information such as genetic data, whether they contain data that may threaten national security, etc. After ensuring that the data have been de-identified and are in line with the results of the identification process, that they do not contain data related to genetic information such as genetic data, and that they do not contain data that may threaten national security, they can be subject to cross-border circulation. Thirdly, blockchain technology can be utilized to create a dedicated storage space for data that can be circulated across borders to ensure that the original data cannot be tampered with in cross-border circulation, so as to ensure the security and credibility of data circulating across borders. Finally, explore the setting of a two-way cross-border data circulation mechanism to allow the circulation of foreign high-quality data. For example, China's drug research and development is dominated by generic drugs and relies on test data of foreign patented drugs. The two-way cross-border circulation mechanism provides a channel for the inflow of foreign patented drug test data into our country, incentivizes foreign patented drug enterprises to circulate drug test data, promotes the development of generic drugs in our country, and then enhances the innovativeness of China's drug industry.

In 2021, The European Data Protection Board (EDPB) issued Recommendations 01/2020 on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data, supplementing the cross-border flow of data and adopting the principle of substantially equivalent protection. China can learn from the experience of the EU and adopt the principle of substantially equivalent protection for the cross-border flow of data, and adopt supplementary measures if the recipient of the data fails to adopt substantially equivalent protection measures.

4.4.2. Participating in Developing International Rules for Cross-Border Data Flows

In recent years, as a large data creator and consumer, China has been active in international cooperation in this area and participating in developing relevant international rules, injecting new momentum into the development and prosperity of the global digital economy. In September 2020, China proposed the Global Data Security Initiative, calling on all countries to commit to maintaining an open, fair and non-discriminatory business environment to promote and achieve mutual benefit and common development. In July 2024, China and Germany signed the Memorandum of Understanding on Sino-German Cooperation on Cross-border Data Transfer [46]. All these indicate that China attaches great importance to cross-border data cooperation with other countries and is committed to promoting the safe and orderly transfer of data cross the world.

In addition to data trading centers, cross-border data transfer also be facilitated through digital trade ports. In March 2024, the Cyberspace Administration of China issued the Provisions on Promoting and Regulating Cross-border Data Transfer, which granted authority to pilot free trade zones, enabling them to pioneer the implementing of facilitation policies for cross-border data transfer [47] Currently, China has initiated the construction of data trade ports , establishing digital trade ports within the Hainan Pilot Free Trade Zone [48],the Beijing Pilot Free Trade Zone [49] and the Shanghai Pilot Free Trade Zone [50]. The advanced development of digital trade ports is crucial for expanding the nation's opening up and fully unlocking the potential of data elements to develop new quality productivity.

At present, he primary focus in promoting cross-border data flows is the formulation of administrative regulations for cross-border data transfer. This involves enhancing the data security obligations of data holders and developing industry-specific cross-border transfer rules that balance data flows with data security. For instance, in the context of medical data which may include genetic information or other ethnically significant genetic data, there is a lack of international regulations governing the compliance of such data in cross-border transfer of medical data. Additionally, issues

 doi:10.20944/preprints202409.0751.v1

related to the authenticity and completeness of data, such as drug trial data, could lead to information asymmetry between domestic and international entities. Therefore, it is essential to seek a common understanding while accommodating differences, to collaboratively formulate inclusive and interconnected administrative regulations for the cross-border transfer of medical data, and to clarify compliance requirements. In the future, China can consider the high-quality implementation of the Regional Comprehensive Economic Partnership Agreement (RCEP), proactively docking the Comprehensive and Progressive Trans-Pacific Partnership Agreement (CPTPP) and the Digital Economy Partnership Agreement (DEPA) and other international high-standard economic and trade rules, further deepening international cooperation in the field of cross-border flow of data, and implementing the rules of cross-border data circulation and trade, so as to promote the healthy development of the global digital economy. economy.

5. Summary

Reasonable privacy protection is a fundamental guarantee for secure data flows and plays a critical role in enhancing the commercial value of data. By analyzing the legislation framework and judicial practice of privacy protection in data flows in China, the author identifies several key elements: first, data collection and processing follows the principle of proportionality; second, data collection and processing are based on the premise of "informed-consent" rule; third, the classification and grading management is adopted as a major measure for data collection and processing; and last, "notice–protection" rule serves as a remedy for data flows. In analyzing the cases of judicial practice, the author selects cases involving public interest litigation and private interest litigation as litigation means, such as the case of the network technology company's personal information civil public interest litigation and China's first case on facial recognition protection, and discusses the limits on the collection of users' personal information and the boundaries of biometric information collection. The conclusion is that civil public interest litigation is seldom involved in privacy protection cases in China.

In the future, China may consider increasing the supply of relevant systems at the legislative level, clarifying the standards for data anonymization, optimizing the informed-consent rule by strengthening enterprises' disclosure obligations, refining standards for data classification and grading, and establishing a multi-party coordinated regulatory mechanism. From a judicial perspective, given the public nature of data privacy infringement, it is necessary to introduce anti-monopoly civil public interest litigation to protect privacy in data flows. Technically, a data flows tracking system should be established to clarify the subjects and scope of data tracking and define the ownership of derivative data. Internationally, exploring mechanisms for cross-border data transfer cooperation, adhering to the principle of data sovereignty, and participating in formulating international rules for cross-border data transfer are recommended. These measures aim to achieve the dual objectives of promoting data flows while protecting data privacy and security.

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

Funding: This research was funded by the major project in Judicial Research of the Supreme People's Court of P.R.C. (grant number ZGFYZDKT202317-03)

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

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

References

1. Data was first included as a new factor of production in the Fourth Plenary Session of the 19th CPC Central Committee in 2019.
2. Chinese government's website: https://www.gov.cn/lianbo/bumen/202401/content_6924380.htm
3. GMW.cn: Data transactions reached RMB 87.7 billion ; National Data Bureau has new deployment plans. Available online: https://baijiahao.baidu.com/s?id=1783670322688616692&wfr=spider&for=pc (accessed on June 20, 2024)
4. Qianzhan Industry Research Institute: Foresight 2024: The market size, competition landscape and prospects of China's data exchange industry predicted to exceed RMB 440 billion in the future. (accessed on June 20, 2024)
5. Farayola O A, Olorunfemi O L, Shoetan P O. Data privacy and security in it: a review of techniques and challenges. *J. Computer Science & IT Research Journal,* ***2024***, 5 (3), 606–615.
6. Chinese government's website: https://www.gov.cn/lianbo/bumen/202401/content_6924380.htm
7. Section 6.1 of National Standard of the People's Republic of China–Information Security Technology–Security Requirements for Data Transaction Services
8. Feng, X. Administrative Licensing Nature and Institutional Development Direction of Authorized Operation of Public Data. *J. E-Government*, ***2023***, *(06)*, 77–87.
9. Fujian Provincial People's Government: How to realize the value of big data? First transaction of a healthcare data product completed on Fujian's exchange. Available online: https://www.fj.gov.cn/zwgk/ztzl/sxzygwzxsgzx/sdjj/szjj/202403/t20240317_6415453.htm.
10. Industry and Planning Institute of China Academy of Information and Communication technology, Beijing International Big Data Exchange: Business Procedures on Data Cleaning, De-identification and Anonymization (for Trial Implementation). Available online: http://www.caict.ac.cn/kxyj/qwfb/ztbg/202311/P020231117626922388674.pdf
11. Mark R. Patterson [USA]. Antitrust Law in the New Economy Google, Yelp, Libor, and the Control of Information. M. Translated by Lan, L. *Law Press · China.* ***2022***, 55.
12. Beijing Municipal Intellectual Office: Administrative Measures for the Registration of Data Intellectual Property Rights in Beijing (for Trial Implementation). Available on: https://zscqj.beijing.gov.cn/zscqj/zwgk/tzgg/326121372/index.html
13. Market Supervision Administration of Zhejiang Province (Intellectual Property Office): Measures for the Registration of Data Intellectual Property Rights in Zhejiang Province (for Trial Implementation). Available on: http://zjamr.zj.gov.cn/art/2023/5/31/art_1229565162_2478832.html
14. Kong, X.J. New Principles of the Anti-Unfair Competition Law (Sub-theory). *Beijing. Law Press · China.* ***2019***, 377.
15. Paragraph 4 of Article 9 of the Anti-Unfair Competition Law (2019):For the purpose of this Law, "trade secret" means technical, operational or other commercial information unknown to the public and is of commercial value for which the right holder has taken corresponding confidentiality measures.
16. Yin, C.r.; J, T.; Zhang, P. et al. Assessment and Pricing of Data Asset Value: Research Review and Outlook. *J. Big Data.* ***2021***, *7 (04)*, 14–27.
17. Chen B, Liu Y. Promotion and Advancement of Data Security Governance in China. *J. Electronics.* ***2024***, *13(10)*, 1905.
18. Liang, Z.Y. Interpretation and Application of the Purpose Limitation Principle in Personal Information Protection. *J. Journal of Comparative Law.* ***2018*** *(05)*, 16–30.
19. Hong, Y.Q. Data Classification and Grading Protection in the Vision of National Security. *J. China Law Review.* ***2021***, *(05)*, 71–78.
20. Article 21 of the Data Security Law of the People's Republic of China.
21. Article 51 of the Personal Information Protection Law of the People's Republic of China.
22. Articles 5, 9, and 26 of the Administrative Regulations on Network Data Security (Draft for Comments).
23. Xie, Z.S. Research on the Damage of Data Leakage. *J. Tsinghua University Law Journal.* ***2020***, *14 (04)*, 140–158.
24. (2020) Zhe 0192 Min Chu No. 4252, Hangzhou Internet Court
25. (2019) Zhe 0111 Min Chu No. 6971
26. (2020) Zhe 01 Min Zhong No. 10940, Hangzhou Intermediate People's Court
27. pkulaw.com is an intelligent one-stop search platform for legal information jointly launched by Chinalawinfo Co., Ltd. and Peking University Center for Legal Information. Now, pkulaw.com has a wide range of users in China, including law firms, enterprises, courts, government agencies, financial and securities institutions, colleges and universities.
28. Notice of the Supreme People's Court on the Decision to Amend the Provisions on the Causes of Civil Cases. Fa [2020] No. 346. Available on: https://www.chinacourt.org/law/detail/2020/12/id/150217.shtml
29. Beijing Municipal People's Government Website: https://www.beijing.gov.cn/ywdt/gzdt/202403/t20240312_3586932.html

30. Ehimuan B, Chimezie O, Akagha O V, et al. Global data privacy laws: A critical review of technology's impact on user rights. *J. World Journal of Advanced Research and Reviews*, **2024**, 21 (2), 1058–1070.
31. Yadav N, Pandey S, Gupta A, et al. Data privacy in healthcare: In the era of Artificial Intelligence. *J. Indian Dermatology Online Journal*, **2023**, 14 (6), 788–792.
32. Chen, B. Building a Scientific Data Element Trading System. *J. People's Forum: Academic Frontier*, **2023** (06), 66–78.
33. Data security technology — Rules for data classification and grading. Available on: https://www.tc260.org.cn/upload/2024-03-21/1711023239820042113.pdf
34. Chen, B.; Guo, G.K. The Positioning and Rules of Data Classification and Grading—An Expansion Centered on the Data Security Law. *J. Studies on Socialism with Chinese Characteristics*. **2022** (03), 50–60.
35. Yin, J.G. Legal Regulations of Abuse of Market Dominance by Big Data Operators. *J. Studies in Law and Business*. **2020** *(4), 73–87*.
36. Information Security Technology — Personal Information Security Specification (GB/T 35273-2017)
37. Online Publishing Office of the Supreme People's Procuratorate: Supreme Procuratorate Releases Typical Cases of Procuratorial Public Interest Litigation in Personal Information Protection to Protect Personal Biometric Information. Available on: https://www.spp.gov.cn/spp/xwfbh/wsfbt/202303/t20230330_609756.shtml#1
38. Article 60 of the Anti-Monopoly Law of the People's Republic of China
39. Supreme People's Procuratorate: Notice on Implementing the Anti-Monopoly Law of the People's Republic of China and Actively and Steadily Carrying Out Prosecution of Public Interest Litigation in the Field of Anti-Monopoly. Available on: https://www.spp.gov.cn/spp/xwfbh/wsfbh/202208/t20220801_569635.shtml
40. W, P.X. The Interpretive Theory of Anti-Monopoly Civil Prosecution Public Interest Litigation System. *J. Modern Law Science*. **2024** (2), 74–87.
41. Article 1 of the Interpretation of the Supreme People's Court on Several Issues Concerning the Application of Law in the Hearing of Consumer-Related Civil Public Interest Litigation
42. Wang, X.X. The Obligation of State Protection of Personal Information and its Development. *J. China Law Science*. **2021** (01), 145–166.
43. Article 27 of the Network Security Law of the People's Republic of China
44. Tian, D.Z. Jurisprudential Evidence of Derivative Data Rights in Digital Society. *J. Xuexi and Shijian*. **2022** (08), 44–50.
45. Ma,Z.F.;Su,J.Y. On Challenges and Solutions of Jointly Building a China-ASEAN Cross-Border Data Flow Governance Cooperation Mechanism under the RCEP Framework. *J. Social Sciences in Guangxi*. **2023**(08),77-84.
46. Chinese government's website: Promoting Bilateral and Multilateral Consultations and Participating in International Rulemaking China Actively Promotes International Cooperation on Cross-Border Data Transfer. Available on: https://www.gov.cn/yaowen/liebiao/202407/content_6962453.htm.
47. Chinese government's website: Provisions on Promoting and Regulating Cross-border Data Transfer [Order No. 16 of the Cyberspace Administration of China. Available on: https://www.gov.cn/gongbao/2024/issue_11366/202405/content_6954192.html.
48. Chinese government's website: The State Council of the CPC Central Committee Issues Overall Program for the Construction of Hainan Free Trade Port. Available on: https://www.gov.cn/zhengce/2020-06/01/content_5516608.htm.
49. Chinese government's website: Boosting High-Quality Development of Digital Economy, Beijing Takes the Lead in Realizing Secure and Easier Cross-Border Data Transfer. Available on: https://www.gov.cn/lianbo/difang/202401/content_6925023.htm.
50. National Development and Reform Commission of the People's Republic of China: Lingang New Area: Building an International Data Port to Create a Hub Platform for Global Data Convergence and Transfer. Available on: https://www.ndrc.gov.cn/xwdt/ztzl/cjsjyth1/xwzx/202112/t20211226_1309885.html