Theoretical Research on Data Utilization—System Construction of Data Trust and Altruistic Sharing

Huang Wenchao[1,a], **Shi Nannan**[2,b]

[1]Faculty of Law, East China University of Political Science and Law, Shanghai, China
[2]Passenger Service Academy, Aviation Tourism Vocational College, Sanya, China
[a]374054554@qq.com, [b]501947296@qq.com

Abstract: *As the value of data emerges and the convenience brought by big data continues to be known, the socialized use of data is pushed to an important position. In order to enhance the dual circulation of domestic and international data, China has proposed the strategy of establishing a unified big market, which puts forward higher requirements on the protection, circulation, sharing and trading of data as an emerging production factor. Mutual trust in data is a prerequisite for the establishment of a unified data market and the social utilization of data. The construction of a data mutual trust environment requires clarifying the basic connotation of data mutual trust, realizing a safe, reliable, voluntary, equal, honest and transparent atmosphere of mutual trust driven by multiple organizational structures, institutional rules and technical guarantees, and providing the necessary social mutual trust environment for the circulation and sharing of data. Under the current legal system of personal information protection, we explore the creation of data production factor circulation theory and data altruistic sharing principle by absorbing the mechanism of production factor distribution in economics. Data altruistic sharing is not separated from the empirical law system, but is an advanced evolution of the right to data portability by using verifiable consent + multi-layered notification procedures as the path. The mutual trust and altruistic sharing of data provide an appropriate theoretical foundation and realization path for the new path of data utilization.*

Keywords: *Data trust; Altruistic sharing; Data utilization; Data production factor distribution; Data governance*

1. Introduction

China has recently implemented legal norms related to data security, network security, and personal information protection. This is a significant step towards establishing a legal framework for data protection and circulation in China, which clarifies the basic governance ideas. The aim is to protect network data security, personal privacy, and information rights, while also providing basic resource elements for the development of the digital economy and artificial intelligence applications. To achieve this goal, we are working on developing standard specifications for secure data transactions, cross-border transmission, authentication, and evaluation. We are also creating a user-friendly basic system for trading, opening, and sharing. The establishment of a unified normative system and institutional mechanism can realise fair access and reasonable use of data, and create a new pattern of mutual trust, circulation and sharing of data.

The mutual trust mechanism is the foundation and prerequisite for social operation. In the field of data circulation, the low level of trust between individuals and enterprises hinders the reuse of data. The main problems are that the "algorithm black box" of enterprises consumes the trust of individuals; the right of personal data portability and deletion hangs in the air without technical guarantee; the "data gap" between enterprises is serious, forming a platform-type data monopoly and reducing the possibility of data access and reuse. Therefore, in compliance with China's information protection legislation, it is important to create a social environment of mutual trust in data, establish a new path of data sharing for altruistic purposes, release data potential, increase opportunities for data reuse, and promote the development of the digital economy. These are important theoretical issues and practical tasks.

This paper aims to demonstrate the importance of socially utilising data by examining the theoretical flow of data circulation. It also highlights the urgent need to establish a discourse on data. The paper analyses the connotation of data mutual trust and explores its intrinsic connection with the principle of trust protection in civil law. It also proposes a mechanism for data mutual trust based on the drive of organizational structure, judicial remedy system, and technical standards. The aim is to provide a good social environment for data circulation and utilization, based on mutual trust. The current data circulation system aims to establish a new path for data sharing and circulation based on altruism. This involves exploring the circulation theory of data production factors within the traditional production factor allocation mechanism, clarifying the basic principles of data altruistic sharing, and utilizing established rules for informed consent and data portability to explain the realization path of data altruistic sharing from an empirical law perspective.

2. Theoretical Changes from Data Protection to Data Protection and Utilization

Sociologist Manuel Castor foresees that with the rise of the network society, the advent of the information technology revolution and the formation of the cyberspace order, the traditional concepts under the original social structure form are gradually being broken. With the in-depth research on the connotation and boundary of personal information, protection and use, the re-evaluation and analysis of the multiple interests, potential values, risk forms, protection methods and use patterns of personal information, and the re-measurement of the interests of data protection and use, the original concepts have gradually been transformed and the theoretical concerns have simultaneously shifted from data protection to data protection and use.

2.1. Personal Interests and Public Interests in Data

With the rise of big data, personal data has become a valuable social resource that carries multiple interests. These interests include not only the personal interests of data subjects and individual stakeholders, but also the social interests of unspecified social subjects and the state[1]. Personal information refers to the personal and property attributes of natural persons. It is a concrete representation of the freedom and dignity of individuals, and the rights and interests of individuals in their data. Legislative protection of personal data has become a consensus in various countries.

The objective collection of data has gained public recognition as a valuable tool for government decision-making, social governance, emergency response, and other public management affairs. This data is collected and utilized by government departments and research institutions, and is processed using anonymous or de-identified technology to protect privacy. The collection, processing, and use of personal information is a common practice in modern countries for administrative management and the provision of public services. However, it is important to ensure that sensitive personal information and personal information of particularly vulnerable groups are protected, as they are a matter of national security and other vital interests. It is crucial to maintain objectivity and avoid subjective evaluations, while using clear and concise language with a logical flow of information. Technical term abbreviations should be explained when first used, and a formal register should be maintained. The text should be free from grammatical errors, spelling mistakes, and punctuation errors, and any changes in content should be avoided[2]. This is specifically expressed in public health data, national security, and cyberspace order[3]. The use of data for public interest is crucial for data governance, social development, improving living standards, enhancing service quality, and fostering product innovation. The scope of public interest should be expanded to include not only the use of data for emergency situations but also for general collective interest purposes, such as education and research, credit system establishment, and personal health data for medical research, financial data for credit profiling, and judicial data for integrity system construction. Compared to individual legal interests, the public interest of data should be of greater concern to legislators and the judiciary, as it affects the welfare and development of the entire country, society, and its people.

Therefore, the protection of personal rights and interests on data is not the only value to pursue. It is also important to fully utilise the value of social data while guaranteeing the basic dignity and freedom of personal information. This will promote the best balance between personal rights and interests of data and public interests.

2.2. Data Protection Power Comes from Anticipating and Controlling Risks Rather than Giving Individuals Control of Their Data

The topic of personal data protection is multifaceted, encompassing the perspectives and demands of various stakeholders. It involves not only technical and legal considerations but also implications for business models and economic development[4]. There is a theoretical debate regarding whether data protection arises from controlling data processing risks or granting individuals complete control over their data. The availability of personal information has been a longstanding issue, but it has only recently received significant social and legislative attention. This is due to the modernization of information processing capabilities, which has led to the senseless collection, bulk processing, intelligent analysis, and social use of personal information. To protect personal information, it is important to avoid making it static and limiting its control to individuals or companies providing services or products. This approach is not conducive to improving the quality of services or product innovation. The principle of reasonable and lawful information practice should be reflected through legal intervention in the data processing relationship. In specific scenarios, joint participation of data subjects, data service providers, data enterprises, and data regulators should be realized to reduce the social risk of data[5]. The risk associated with data processing arises from the relationship between individuals and enterprises, individuals and government, and enterprises and government in terms of data processing and being processed. The legal regulation system of data protection establishes the obligation of diversified protection and grants the right to remedy the infringement of personal data rights and interests. This is because the algorithmic rules of data processing are often complex and difficult for non-professionals to understand and evaluate. It is important to ensure compliance with data processing regulations. The legal system for data protection establishes various obligations for protection and provides the right to seek redress for violations of personal data rights[6].The main distinction between risk control of data and the protection of rights granted in traditional civil law is that the latter originates from the operational law of commodity economy and direct face-to-face interaction between people. The empowerment protection model takes tangible objects as the object of study and constructs the system of rights protection or property rights change. It is important to note that personal information cannot be absolutely controlled in the data era. The overuse of personal control, particularly through excessive promotion of consent mechanisms, can be dangerous. Consent mechanisms may create the false impression that control over information can replace privacy protection. It is important to balance personal control with other privacy protection measures[7]. In addition, absolute control by the individual will inhibit the flow and reuse of data, increasing the cost to the data enterprise and ultimately shifting all costs to the consumers themselves. Therefore, giving individuals absolute rights over data to safeguard personal information is not sufficient to achieve good protection. Only the allocation of multiple protection obligations can protect the rights and interests of individuals and public interests on information in a comprehensive manner. The focus of the personal information protection system is to regulate the risks in the process of data processing.

2.3. The Aggregate Value of Data: From Resource to Asset to Capital

Data is a valuable resource that originates from various sources such as people, social organizations, regular object operations, flora, and fauna. It can be effectively collected and quantified, and its value is widely recognized. The objective existence of data allows for its measurement. It meets the basic characteristics of reality, controllability, and asset economy. Currently, a company's core competitiveness lies in its ability to handle large amounts of data and process it efficiently. The ability to predict the future is a direct result of mastering data[8]. Due to the great value of data assets, data gradually develop towards capitalization that can be traded and funded, converting the value and use value of data assets into shares or contribution ratio, and turning them into capital circulation through trading on and off the data exchange. The transformation of data from resource to asset to capital reflects the value aggregation of data from scattered and low value to convergence and high value state.

2.4. Differential Order Protection of Data Identifiers

Professor Ronald E. Leenes of Tilburg University in the Netherlands discovered that different parts within an identifier play different roles, and proposed the classification of lookup recognition and cognitive recognition identifiers[9]. Our scholar Fuping Gao goes on to propose the distinction between direct identifiers, indirect identifiers, and quasi-identifiers[10]. A direct identifier is one that can be associated with a specific individual without any additional information or cross-linking with publicly available data. Indirect identifiers are those that cannot be directly associated with a specific individual or cannot identify a specific individual alone, but can identify a specific individual in combination with other divisional forms. Quasi-identifiers are attribute information, and this broad sense of identifier is applicable to user profiling or identifying the classification labels given to individuals in user analysis. Specifically, distinguish the protection method and the strength of protection according to the degree of identification or association of personal information identifiers. The direct identifiers will be strictly protected, the indirect identifiers will be prohibited from reverse identification of information subjects, and the quasi-identifiers will be protected with a loose protection policy can be commercially processed or analyzed. In the construction of data mutual trust environment and data social utilization, we should make full use of de-identification technology to reduce the identifiability or relevance of identifiers.

3. The Prerequisite for Social Utilization of Data: System Establishment of Data Mutual Trust

Robert Post, former dean of Yale Law School, suggests that although the right to privacy presents itself as an individual right, it is essentially a specific social norm and civilizational rule recognized by social groups, and has certain social relationship properties[11]. Helen Nissenbaum further suggests that the protection of privacy is determined by social norms and circumstances, and that differential protection should be achieved in different scenarios[12]. Data protection and circulation should be dynamically measured in different national contexts, social norms, and social environments, especially since data has become an important factor of production, and the use of data has generated huge commercial value, more and more organizations and departments are recognizing the importance of data, and individuals are feeling the "crisis" of data use. Therefore, only by establishing a stable socialized trust relationship can data circulation and socialized utilization be realized smoothly.

3.1. The Basic Concept of Data Mutual Trust

The term 'mutual trust' originates from the concept of trust, which refers to a relationship between two interacting parties. While there is a significant amount of domestic and foreign research on trust, there is no consensus due to the substantial differences in political, cultural, social, and historical backgrounds both domestically and internationally. Even within the same context, trust may have different meanings and implications in various fields. The reason why it is difficult to grasp is that trust has become a presupposition in society and has been applied to all human activities. As a result, trust changes with each activity in which it is expressed. The concept of trust encompasses three dimensions: relational, temporal, and binding[13]. Specifically in data mutual trust, the relational nature between data subjects and data controllers stems from the dependency or interactive relationship that arises when providing services or products, such as the interactive relationship between people and cell phones, which collects a lot of user information when providing calls or network services on the one hand and on the other. The temporality of data trust is that the data subject uses the service or product for a period of time and generates experience on the service or product to predict the future, and data trust is determined by the consistency of user experience accumulated over a long period of time. In the IoT era, the long-term interaction between people and machines and algorithms gives rise to the relationship of human dependence on machines and algorithms, which is especially obvious in the field of auto autopilot. The long-term relational and temporal nature prompts the relationship of mutual trust between people and machines and algorithms. In terms of binding force, the binding force of data mutual trust arises from the long-term satisfaction of user experience and the expectation of data security, and the satisfaction and expectation counteract the endogenous motivation of data enterprises to create data security environment and comply with the law in data processing.

Williamson, an American economist, divides trust into three dimensions: first, the consistency of the fiduciary's actions calculated on the basis of the information available and generating computational trust; second, personal trust based on personal relationships without calculation or cost; and third, from the macro level, an institutional trust in which activity contracts are embedded in the social and organizational environment of transactions[14]. The three dimensions are three different strata of trust and the mutual trust process in which the level of trust increases sequentially. Establishing data mutual trust should also generate rational computational trust and personal trust from data subjects based on the relational and temporal nature of data mutual trust, and then generate stable institutional trust by forming the binding force of universal data mutual trust at the social level. Institutional trust is the ultimate goal in the era of big data and Internet of Things, and it is the cornerstone of data socialization. Data mutual trust is not a conjectural word, but on the one hand from the fact that mutual trust has been formed between data subjects and data controllers in practice, and on the other hand from the new interpretation and application of the principle of trust protection in China's civil law in the field of data.

3.2. The Civil Law Basis for Mutual Trust in Data: A New Interpretation of Trust Protection Theory in the Digital Age

The theory of reliance protection runs through the whole civil law system, especially playing an important role in credit, meaningful autonomy, the structure of the civil subject system, the system of legal acts, and the mechanism of reliance protection on property claims[15]. The doctrine of promissory estoppel, the doctrine of appearance of rights, Fuller's theory of reliance, and the doctrine of contractual negligence are the four sources of reliance protection in traditional civil law[16].

3.2.1. The Doctrine of Promissory Estopple

Promised estoppel is a universal binding rule that maintains honesty, trustworthiness, transaction security, and order in the commodity economy. Its core concept is that the promising party shall not renege on the promise after knowing that the promise will cause the trust of the other party, and the other party, in fact, produces legal acts according to the promise. In the field of data, the principle of specific and clear reasonableness of the purpose of processing personal information and the obligation to inform are reflected. The data collector is required to inform the user of the purpose, manner, type and duration of collecting and processing information. This is considered a commitment to its own behavioral norms. If this commitment is broken, there will be adverse consequences, giving the right to judicial remedy to the party in compliance. The primary legal consequence of a promise is the anticipation of benefit to the other party, which subsequently generates a practical and legally enforceable outcome.

3.2.2. The Doctrine of Appearance of Rights

The appearance of rights theory is a private law theory first proposed by German scholar Moritz Welschpach in his work. The key concept is that when relying on an external elementary fact to perform a legal act, if the establishment of the elementary fact is assisted by the other party, then the reliance should be protected by law[16].According to this view, external facts are the elements used to identify legal theories. The concept of appearance of agency is commonly applied in civil law to establish the appearance of rights. In the context of the internet, data companies often present themselves as capable of ensuring data security and efficient data processing. This fosters user trust and increases the likelihood of product or service usage, ultimately leading to increased data sharing. Modern internet companies often use the appearance of rights to gain users' trust. They employ smart and accurate means to demonstrate the security of their data through attractive and simple official homepages, user-friendly app interfaces, and advertising interfaces with the 'preferences' logo of common friends. However, these companies also encourage the sharing of personal information and preference data by their users[17].

3.2.3. Fuller's Theory of Reliance and The Doctrine of Contractual Negligence

Fuller's theory of reliance and contractual negligence is an important basis for damages in modern contract law. It compensates for the deficiencies of private law autonomy liability and contractual liability, and emphasizes institutional compensation for the benefit of reasonable expectation[16].In the field of data mutual trust liability, it is recommended to apply Fuller's reliance theory to establish a liability bond between data subjects and data controllers. Data subjects trust data controllers to use data in a reasonable, compliant, and safe manner. They can then claim their rights from data controllers or third parties based on the expectation benefits of data trust once the data is infringed. This mutual trust in data gives rise to a liability system that can effectively alleviate disputes over data ownership and even move away from the empowerment model. Additionally, the text should adhere to conventional academic structure and formatting, including consistent citation and footnote style. Finally, the text should be free from grammatical errors, spelling mistakes, and punctuation errors. Due to the characteristics of data, such as non-exclusivity, widespread use, and low value of unstructured single data, it is difficult to establish tenure among subjects. It is important to use clear, concise, and objective language, avoiding biased or emotional language and sticking to common sentence structure and technical terms. If the main purpose of assigning ownership is to determine attribution, then Fuller's theory of reliance can be applied. Data reliance can effectively solve the problem of determining responsibility and assumption, eliminating the need to waste time on the century-old problem of who owns personal data. This approach can effectively protect the rights and interests of personal information by generating responsibility through mutual trust in data.

In the data era, the new interpretation of reliance protection theory finds its theoretical basis in civil law. It involves the procedure of informing and the purpose-specific principle of personal information processing. This provides institutional compensation for the responsibility of personal information protection. Additionally, it elevates the data trust relationship to the responsibility relationship between data subjects and data controllers. Finally, it elevates trust from the moral level of restraint to the legal level of restraint.

3.3. The Path of Realizing Data Mutual Trust: Organizational Structure, Judicial Remedies, and Technical Guarantees

As the big data industry enters the trillion-dollar era, a specialized division of labor is inevitable, and data service providers will become important link carriers. Data disputes are frequent, and the problems of high litigation costs and difficulty of proof for data subjects are highlighted. The relationship between data subjects, data service providers, and data enterprises should clarify their respective rights, responsibilities, and benefits. Infringements of data rights and interests should have extended remedies, and technical means should be used to protect multiple interests in data. It is essential to construct a data service ecosystem, a litigation remedy system, and a technical guarantee system to establish a mutual trust environment for data.

3.3.1. Introduce Neutral Institutions to Build Data Service Ecosystem

Third-party organizations are generally considered more professional and responsible for their technical security capability and qualification capacity compared to general data subjects and data enterprises. These organizations can be categorized as data sharing organizations, data processing organizations, and data altruistic organizations. The main functions of data service companies are to collect, aggregate and transmit personal information, establish data circulation bridges, and form two-way channels between data subjects and data receiving enterprises. They also facilitate data enterprises in saving data collection costs. Data service companies are third-party organizations for data desensitization and de-identification, and have become an increasingly popular industry. The ecosystem of data services aims to create and utilise data value, express resource integration and service exchange, and achieve self-driven and continuous cycles under the constraint and promotion of external institutional factors[18].

3.3.2. Broaden the Judicial Remedies to Protect the Interests of Data Subjects

Personal data rights and interests have a strong personal nature. To establish a mutual trust environment for data, it is necessary to enhance the confirmation of data subjects, improve judicial remedies, increase judicial punishment for violations, and streamline litigation channels. Civil disputes related to personal information processing, such as contract and tort disputes, should also be considered[19].If the personal information processor violates the purpose, manner, and scope of processing as agreed in the contract, their behavior constitutes a breach of contract, and they shall bear the liability for breach of contract. The methods for assuming liability for a breach of contract may include ceasing the processing of personal information, processing personal information in accordance with the agreed-upon purpose, fulfilling the obligation of data protection, deleting personal information, transferring information to a third party, paying liquidated damages, and issuing a public apology[20]. In data infringement disputes, the presumption of fault liability is applied, and data subjects are required to prove that their personal information has been processed and infringed upon. However, data subjects often lack the professional and technical ability to prove the true subject and purpose of information processing, which makes it difficult for them to provide evidence. The implementation of the principle of no-fault liability for breach of contract and the reversal of the burden of proof reduces the burden of proof on data subjects. This is conducive to enhancing the confidence of data subjects to defend their rights. Additionally, the data subject has the right to freely choose the remedy of claiming breach of contract liability or tort liability.

3.3.3. Build Personal Data Space Application in key Areas and Implement De-Identification Technology Application

Personal Information Management (PIM) is an emerging research direction that has received attention from researchers in many fields, such as databases, information retrieval, and semantic Web. It is an important research direction in the field of privacy computing to replace manual management of personal data circulation and utilization with neutral algorithms, decentralized storage technologies, and monitorable platforms. Personal Data Spaces (PDS) is an important research base in personal information management. It is responsible for managing and maintaining personal information, as well as supporting finding and sharing operations through effective indexing and organization[21].The personal data space facilitates the collection and storage of information about data subjects. This information is then shared with data enterprises, public departments, and research institutions, either for a fee or altruistically, with the aim of maximizing the circulation and utilization of data, provided that the data subjects have given their informed consent. The personal data space is comparable to a private data box that can track and monitor the usage of data by individuals, including who is using it, when it is being used, and for what purpose. This enhances individuals' control over their data and provides an

API interface for data service providers, enabling them to offer intermediate link services. The decentralised, monitorable, and easily accessible personal data space provides a crucial platform for mutual trust in data. It replaces data enterprises in fulfilling data security obligations and creates a safe, reliable, voluntary, equal, honest, and transparent mutual trust space.

Controlled de-identification[9] or controlled linkable data has become an internationally accepted technical rule for the sharing and reuse of personal information.The true purpose of de-identification technology is to remove identifying information about individuals, rather than to conceal personal characteristics. Direct identifiers are processed to eliminate information that could identify a specific subject, ensuring the protection of basic individual rights such as privacy, dignity, and freedom. Indirect identifiers and quasi-identifiers that describe personality traits should be retained to allow for circulation and reuse without identifying a specific subject. The technical standard of de-identification provides a 'safe haven' for data processing service providers or data enterprises to publish the list of de-identified information and obtain approval from the public, industry associations, and data regulatory authorities. This can, to a certain extent, exempt or reduce the infringement or breach of contract responsibilities of data controllers.

4. A New Path to Use of Data: Data Sharing for Altruistic Purposes

The social utilization of data relies on a mutual trust environment, where data subjects and controllers have trust in the computational and institutional aspects of data circulation and sharing. This trust is ensured through multiple guarantees such as organization, judicial remedy, and technology. Chinese scholars have conducted extensive research on the circulation and sharing of data among individuals, enterprises, and governments. Various perspectives, such as public or private law, civil or criminal law, and empowerment or behavior regulation models, have been explored to provide individuals, enterprises, and governments with diverse rights and interests. This approach aims to achieve a balance between data protection and circulation. There is a lack of macroscopic analysis regarding the mechanisms of data generation and circulation in the fields of legal economics and legal sociology. Interdisciplinary research on data circulation can achieve a generalisation of research results in an international context, allowing for research conclusions on legal phenomena to extend beyond the scope of a single country or region. The research paradigm of legal economics can model various social, economic, and institutional factors through a unified economic paradigm, thus providing a relatively unified concept for understanding, analyzing, and communicating problems. In the field of data jurisprudence, data has become the fifth major factor of production. Therefore, it is necessary to study and analyze the theoretical basis and basic principles of the circulation of data, a new factor of production. This can be achieved by drawing on the existing principles of distribution of factors of production. The aim is to provide a unified discourse system and consensus on basic research for the study of social utilization such as data circulation and sharing in China. The ultimate goal is to build a basic theory of social utilization of data and digital economy.

4.1. The Fundamental Purpose of Altruistic Data Sharing

In the current legal and regulatory framework for data circulation, individuals' consent is required for the government or enterprises to share and use personal data. The principle of minimal and specific purposes of processing must be followed. In addition to the standard processing rules, the Law of the People's Republic of China on the Protection of Personal Information allows for the use of personal information without individuals' consent for specific purposes, such as handling public emergencies, protecting the life and property of natural persons in emergency situations, and implementing news reporting and public opinion supervision in the public interest. The current regulatory system overlooks data processing scenarios for altruistic purposes in non-emergency situations, particularly in the fields of medical and healthcare, social credit systems, financial and economic development, and education and scientific research. To improve China's data circulation and utilization rule system, it is recommended to establish a rule system for data circulation and sharing based on altruistic purposes. This will address the scenarios of data circulation, sharing, and reuse in non-emergency situations based on general social public interests.

Studies on altruistic behaviour in animals and humans demonstrate that self-interest does not always require harm to others. Self-interest and altruism can be combined, and benefiting others is necessary to benefit oneself. Therefore, one can better benefit oneself by benefiting others[22].In the field of data circulation, data altruistic sharing is a new approach to data sharing with the aim of benefiting others, the collective, society, and the country. It is centered around national interest, public interest, social morality, and social virtue, and is a concrete expression of the traditional Chinese virtue of 'everyone for me and me for everyone' in the data era. Altruistic sharing of data circulation has already emerged in daily life. For example, users of Gaode Maps share their personal travel data to help others save time by providing clear views of road traffic jams and accurate travel time calculations. For instance, patients willingly participate in drug trials to share their personal diagnosis and treatment data, and exchange medical advice in patient groups, with the goal of preventing others from experiencing the same illness. The sharing and circulation mode of personal data for the benefit of social management, social operation cost saving and others' health has been quietly formed, and the concept of altruism is as beneficial as self-interest, and altruism is ultimately beneficial to oneself has gained social consensus. Data theory research and legislative practice should respond to social needs, changes, and consensus. They should establish a new path of data sharing for the purpose of data altruism without changing the existing norms of data protection and circulation. This will help to realize the full development of the idea of data altruism in the construction of the socialist rule of law system with Chinese characteristics.

4.2. Theoretical Foundations of Altruistic Data Sharing

The theory of three allocations of production factors in China has become a general theoretical consensus. It was first proposed by Mr. Li Yining. The first allocation refers to the income that people receive by exchanging their means of production in the market. The second allocation is the redistribution of income by the government through macro-regulation, using taxation, support, and other policies. The third allocation is the transfer of means of production dictated by moral forces, such as voluntary donations[23]. The author's analytical structure can be used to explain the overall spectrum of data circulation and utilization within the production factors' circulation system.

The author tries to summarize the circulation of data production factors into three levels: the first level is the circulation driven by the rights (force) system based on the rights and interests of data subjects, the rights of data generators, and the national sovereignty of data, while the rights (force) system is interspersed with the supply and demand exchange relationship between data and services, the investment return relationship between data and infrastructure construction, and the affiliation relationship between data and the establishment of national discourse; the second level is based on The second level is based on government-led public data disclosure, intervention of data regulators or judicial departments on data monopoly, a way to regulate the imbalance of free flow of data market, and judicial administrative means to guarantee the value of data flow; the third level of circulation is based on the distribution of altruistic sharing behavior of data with altruism as the purpose. The third level of data altruistic sharing is the focus of discussion in this paper. Scholars have already focused on the fact that there is an invisible force driving data circulation in addition to commercial purposes and government regulation purposes, such as data moral responsibility[24], data charity[25], data donation and other research results, and the author believes that all of the above areas can be accommodated to data altruistic sharing. Whether it is for the purpose of virtue, charity, donation, or trust, the aim is to give full play to data sociality, realize data circulation, solve data monopoly, use distributive justice and corrective justice to realize the just distribution of data, and maximize the value of social utilization of data production factors.

4.3. Basic Principles of Altruistic Data Sharing

The principles of data altruistic sharing should adhere to the same basic principles and processing rules as those in the legal regulation of personal information protection. However, data altruistic sharing requires its own set of processing principles due to the different purpose, manner, result, and value of altruistic processing.

4.3.1. Voluntary Sharing Principle

Altruism is not bound by legal or moral obligations; it is voluntary and non-compulsory. Altruistic behaviour should be highly praised and promoted[26]. Therefore, the fundamental principle of altruistic data sharing is voluntary sharing by data subjects or data service providers based on altruistic purposes. No one may be compelled to share data. By promoting the development of data sharing, it provides legal clarity and a trustworthy environment for public institutions, individuals, or enterprises willing to share data.

4.3.2. Fair Data Principles

The fundamental principle of fair data is to provide data that is findable, accessible, interoperable, and reusable. The principle of fair data aims to promote data quality and data format requirements in the process of data circulation between data service providers and data enterprises. It aims to achieve non-discriminatory data access, interoperability, and reusable data, while reducing data circulation obstacles caused by data transmission requirements. Ultimately, it aims to enable barrier-free and fair utilization of data socialization.

4.3.3. Transparency Principles

The principle of transparency is fundamental to the openness and clarity of data processing. It is a prerequisite for establishing mutual trust in data and achieving selfless data sharing. The principle of transparency requires that data processing be clarified in terms of subject, purpose, scope, and duration, as well as the qualifications and abilities of data stakeholders to process data, among other aspects. This further strengthens the data subject's right to know.

4.3.4. Exclusive Prohibition Principle

Data sharing is a right of the data holder, whether paid or unpaid, and may come with or without restrictions. To ensure fairness and prevent arbitrary choices, it is important to establish clear guidelines for data sharing. In cases of altruistic data circulation, exclusive agreements between data holders and processors should be prohibited, and limitations should be placed on the right to make autonomous decisions regarding data sharing. For altruistic sharing purposes, data circulation, including sole-source data, data of public interest, and basic data, should not be restricted by exclusive clauses.

4.4. The Realization Path of Data Altruistic Sharing in the Framework of Personal Information Protection Law

The primary challenge of altruistic data sharing is how to ensure the altruistic intent of data subjects, distinguish altruistically shared data from other data processed with consent, provide data controllers with legitimacy to process data for altruistic purposes, and clarify the legal implications of altruistic data sharing. Based on the mature rule system in China's personal information protection law, the author suggests that data altruistic sharing should be integrated into the system of informed consent rules for data processing. This will clarify the rules for informed consent in relation to data altruistic sharing. Data altruistic sharing has the same legal effect as data transfer, which is equivalent to data portability but at a higher level of data sharing.

4.4.1. Establishing Informed Consent Rules for Altruistic Data Sharing

In our current personal information protection empirical law, individual consent is one of the foundations of the legality of processing personal information. Data altruism should also be based on full respect for the rights and interests of individuals, and the consent to altruistic sharing should be made to the data service provider or data enterprise in the form of signing a consent form for altruistic sharing, and all the kinds of shared data approved and agreed to in the consent form can be provided to the data service provider or the requesting enterprise for reuse and interoperability. The procedures for informed consent for altruistic data sharing should be stricter than those for informed consent for general information processing. In terms of obtaining the consent of data subjects, more rigorous verifiable consent should be adopted[27], i.e., written consent or consent with verifiable authenticity should be adopted to alleviate the problem of vain and formalized meaning of consent. In the notification procedure, multi-layered notification procedure (multi-layered notice) is adopted to replace the lengthy, complex and highly specialized notification content[28]. The establishment of the informed consent procedure for data altruistic sharing is in compliance with the basic theory of legality in the current personal information protection system, with wide social awareness and acceptance, and easy to carry out the practical operation of data altruistic sharing in the field of data circulation as soon as possible.

4.4.2. Legal Effects of Altruistic Data Sharing

The legal effect of altruistic data sharing is that it facilitates data transfer. This enhances data transfer control for data subjects and reduces the divide between data enterprises, thereby promoting competitiveness and innovation. Additionally, it reduces social operation costs and greatly enhances data economic efficacy from a socio-economic perspective. Altruistic data flows begin with the data subject's will and occur based on the data processor's processing behavior. Data portability is a data flow system established by EU countries and China's empirical law. Data altruistic sharing is similar to data portability in terms of data transfer effect, but there are subtle differences between them. The purpose of altruistic data sharing is to promote data of general social interest in a safe and orderly processing environment, and to allow fair access and use of the data by enterprises or institutions in need. The language used in this text has been made more objective, concise, and clear, with a logical flow of information and consistent technical terms. The text adheres to conventional academic structure and formatting, with clear citations and footnotes. The language is formal and free from grammatical errors, spelling mistakes, and punctuation errors[29]. No new content has been added beyond what was provided in the original text. It is important to note that personal data is not the only type of data included in data portability; it also includes data on the provision of services or operations by enterprises[30]. The analysis indicates that altruistic data sharing improves the data subject's control over data transfer to meet the general interests of society. It requires a one-time generalized consent to license the data controller to flow its data and ultimately results in the legal effect of data flow and reasonable use.

5. Conclusion

In recent years, the data protection and circulation system has matured. However, a social environment of mutual trust regarding data has not yet been established. This makes it difficult to create an ideal country where data stakeholders voluntarily share and circulate data, and to truly realize the full potential of data resources. Based on the evolving theory of data circulation, this paper explains the necessity and inevitability of socialized data utilization for the creation of a national data unified market and international data discourse. It proposes the establishment of a mutual trust environment for data through institutional, organizational, technical, and judicial remedies as a guarantee system. This will provide a social atmosphere of mutual trust for the social utilization of data. The theory of data circulation cannot be nourished by interdisciplinary theoretical research results of law and economics or law and sociology. The theory of data circulation at the macro level is formed by drawing on the mechanism of production factor distribution to find an accurate social function positioning for altruistic sharing. Data sharing for altruistic purposes concerns the public interest of society and is an important national data strategy for self, altruistic, and social benefits. It will become the main channel of the social utilization path of data in the near future., the data protection and circulation system has gradually matured, but a social environment of data mutual trust has not yet been built, making it difficult to build an ideal country where data stakeholders voluntarily circulate and share data, and to truly realize the deep utilization of data resources. Guided by the changing trend of data circulation theory, the urgent need to build a national data unified market and international data discourse, this paper elaborates the necessity and inevitability of socialized data utilization. It establishes an environment of mutual trust in data based on institutional, organizational, technical and judicial remedies as a guarantee system, and provides a social atmosphere of mutual trust for the social utilization of data. The theory of data production factor circulation cannot be nourished by the interdisciplinary theoretical research results of law and economics and law and sociology, and the theory of data circulation at the macro level is formed on the basis of drawing on the mechanism of production factor distribution to find an accurate social function positioning for altruistic sharing, and data sharing for altruistic purposes concerns the public interest of society, which is an important national data strategy for self, altruistic and social benefits, and will become the path of data socialization in the near future. In the near future, it will become the main channel of the social utilization path of data.

References

[1] GAO F P, YIN L M. Interests of Personal Information on Data: Paradigm Shift from Protection to Governance [J].Zhejiang Social Science,2022(01):58-67,158.

[2] GAO Z H. Public Interest Considerations for Personal Information Protection: A Perspective on Responding to Public Health Emergencies[J].Oriental Jurisprudence, 2022(03):17-32.

[3] JING l J. The Expansion and Limit of the Scope of Protected Collective Legal Interest in Information and Cyber Crime[J].Politics and Law, 2019(11):57-68.

[4] ZHOU H H. Exploring the way of incentive compatible personal data governance: legislative direction of China's personal information protection law[J]. Legal Studies, 2018, 40(02): 3-23.

[5] DING X D. The Dilemma and the Way Out of Private Law Protection of Personal Information [J].Legal Studies, 2018, 40(06):194-206.

[6] MEI X Y. Social Risk Control or Personal Rights Protection[J].Global Law Review, 2022, 44(01): 5-20.

[7] LI Q. From Individual Control and Product Regulation to Cooperative Governance :On the Paradigm Shift of Personal Information Protection[J].Journal of East China University of Political Science and Law,2022,25(02):100-111.

[8] MEI H. The Theory of Data Governance[M].Beijing:People's University of China Press,2020:17.

[9] GAO F P.The Institutional Basis for the Circulation and Use of Personal Information: A Perspective on Information Identifiability[J].Global Law Review, 2022, 44(01):84-99.

[10] GAO F P. Big Data Knowledge Map: Basic Concepts and Systems of Data Economy [M]. Beijing: Legal Publishing House, 2020: 139-142.

[11] POST R C. The Social Foundations of Privacy: Community and the Self in the Common Law Tort [J]. California Law Review, 1989,77(05):957-1010.

[12] Nissenbaum H. Privacy in Context: Technology, Policy, and the Integrity of Social Life[M].New York: Stanford University Press, 2009:56.

[13] ZHAI X W. Trust, Modernity, and the Choice of Social Governance Models[J]. Journal of the Party School of Hangzhou Municipal Committee of the Communist Party of China,2020(06):4-10.

[14] Williamson O E. Governance Mechanisms[M].Translated By Shi Shuo,Beijing:Machinery Industry Press, 2016:253-272.

[15] Zhu G X.The Principle of Trust Protection and its Construction in Civil Law[M].Beijing:People's University of China Press,2013:156.

[16] Zhu G X.A Review of Trust Protection Theory and Its Research[J]. Legal Business Research, 2007(06): 71-82.

[17] Waldman A E. Privacy as Trust[M].Cambridge:Cambridge University Press,2018:79-80.

[18] Xue X,Zhao Y X.Construction of an Open Data Service Ecosystem for Major Public Health Events Based on the Public Science Model[J]. Library and Intelligence Work,2022,66(04):33-44.

[19] CHENG X. Understanding and Application of the Personal Information Protection Law[M] Beijing: China Legal Publishing House,2021:100.

[20] YANG X J.The Study on the Problem of the Mode of Default Liability Protection on Personal Information Right[J]. Journal of Northwestern University (Philosophy and Social Science Edition), 2019, 49(04):66-73.

[21] Zhou B, Zhong S L. Research and Implementation of Information Tagging in Personal Dataspaces[J].Computer Engineering & Science,2010,32(01):92-96,108.

[22] YE Z X. The Study on the Altruism Puzzle and Its Contemporary Enlightenment[J].Journal of Huazhong Normal University (Natural Science Edition),2010,44(04):662-665.

[23] SUN C C.A Three-fold Ethical Path to Achieve Common Wealth[J].Philosophy Dynamics, 2022(01): 13-20.

[24] YAN H X. Analysis of Moral Responsibility in the Data Age: From Trust to Construct [J]. Exploration and Controversy, 2022(04):37-46,177.

[25] LINAG Z W. Data Philanthropy: Its Category and Legal Framework[J].Journal of Shanghai Jiaotong University (Philosophy and Social Science Edition),2022,30(02):63-77.

[26] YAO D Z. Altruism and Moral Obligation[J].Social Science Front,2015(05):24-30.

[27] CHENG X. Creating a Legal Shield of Protection for Personal Biometric Information[J].People's Forum, 2020,24(08):118-120.

[28] WANG H Y. Research on the Protection of Minors' Personal Information in the Era of Big Data [J]. Library Construction,2020(03):60-66.

[29] FU X H. European and American Legal Practices on Data Portability and Localized Institutional Design[J].Hebei Law Science, 2019,37(08):157-168.

[30] SUN Y Y. Study on the Object of Data Portability Rights: Structure, Effect and Sinicization [J].Journal of Henan University of Economics and Law, 2022, 37(03):78-90.