CHAPTER 3

The Concept of Data Rights

Data is a fundamental resource in a modern society. Its value has been well recognized. Meanwhile, the digital age has also brought unprecedented challenges to civil law, real right law and other traditional laws. Traits of data like personality and property have become unavoidable legal issues. In the legal academia, debates have been made on data rights and their ownership for a long time. Theories have been established regarding the new personality rights, intellectual property rights, data property rights, etc. These theories and ideas, although well-established, cannot cover all the features of data rights. Our research finds that data rights are a comprehensive combination of data personality rights and data property rights. The right of possession is the essence of real rights while the right to share is the essence of data rights. With the development of big data, data rights and their ownership have become global issues. The introduction of data rights law will become an important cornerstone for mankind stepping into the era of data rights from the era of property rights.

Theories of Data Rights

While data rights develop from idealistic to actual ones, discussion on data rights is definitely inevitable. In consideration of the threat brought by rapid development of the Internet and big data, it is particularly important and urgent for us to strengthen the protection of data rights by legislation. In the legal academia, heated discussions have been made on data rights and their ownership. Although no consensus has been reached so far, the mainstream views generally fall into four categories: theory of a new type of personality

right, theory of intellectual property, theory of trade secrets, and theory of data property rights.

Theory of a new type of personality right

The traditional personality right refers to a right with the subject's inherent personality interests as the object for the purpose of maintaining and realizing the equality of personality, personal dignity and personal freedom. It is a traditional civil right (Hu 2011). "The personality right is the right to the personality of the right holder himself, that is, the rights and interests a person has in the society are protected by law since personality is an integral part of a person, including the rights of life, body, freedom, chastity, reputation, portrait, name, credibility, etc." (Zheng 1988). There are relevant provisions in the *Constitution of the P.R.C.* and the *General Principles of the Civil Law*. In accordance with Article 38 of the *Constitution of the P.R.C.*: "The personal dignity of citizens of the People's Republic of China is inviolable. Insult, libel, false accusation or false incrimination directed against citizens by any means is prohibited." The *General Principles of the Civil Law of the P.R.C.* stipulates the protection of personality rights including the rights of name, portrait, reputation and privacy.

Personality rights are an open-ended system of private rights (Wang 2015). With the improvement of science and technology and social development, the scope and content of the rights are constantly evolving. Big data has been widely and deeply utilized in various aspects such as economic operation mechanism, social lifestyle, national governance capability, national defense and army building. Data has become increasingly and prominently important and, meanwhile, brought new challenges to data protection. In the process of data processing, some personal private information which is not expected to be disclosed by the owner can be extracted, and the "data image" of the subject can be obtained through data-fusion and association analysis. The more data are provided, the more specific the image will be. In reality, illegally sorting out fragmented data, such as videos, social media content, personal account information, location information, and online consumption information, can undermine personal interests, such as the rights of life, name, etc., which form an integral part of personality rights.

Personal data protection has gone far beyond the scope of traditional personality rights. Traditional personal data protection is mainly regulated by the system of privacy. Despite overlapping in content (for instance, both data rights and privacy aim to protect the data owner's personal dignity), the two rights are fundamentally different: first, privacy means disclosure of personal information is absolutely forbidden, whereas data rights refer to the protection granted to data during the process of data controlling, using, benefits gaining and sharing; second, privacy emphasizes the passive protection of individual privacy, while data rights stress actively guiding the utilization of personal data in social activities; third, unlike the object of privacy in which there are specific personality rights to names and portraits, etc., when a person changes his or her mobile phone number, home address, etc., he or she can still be traced with the reference of other data. Wang Liming and other scholars state that personal information, identifiable and sometimes collected for public interests and other purposes not related to property, should not be simply defined as a property right (Wang 2012). Given the content and features of personal data right, it should be deemed as a new type of personality right. This idea was developed on the grounds as follows.

First, the commercialization of personality rights is widespread. The traditional personality rights focus on spiritual interests instead of physical value. Under the development of market economy, some of the personality rights are being commercialized. With the improvement of the appraisal mechanism of property value of the personality rights, people at large have begun to pay attention to the spiritual rights, which increases the commercial value of personality rights featured with *res incorporales*. For instance, the names and portraits of renowned people are licensed to be used for commercial purposes for the sake of the effect of celebrity. At the same time, the storage, dissemination and utilization of personal data in the cyberspace are open, immediate, and convenient. Fragmented data, through association analysis and data-fusion, can be spliced into a "data person" and, subsequently, the results of the "data person" analysis can be used for commercial purposes. The commercialization of personality rights has prevailed in the society of market economy (Wang 2013), which made it necessary to reconsider the traditional personality rights.

Second, the existing personal information protection systems are not sufficient for personal data protection. Personal information was initially part

of privacy protection, but with the development of information technology, personal information was given personality value. The system of privacy is therefore apparently insufficient to protect personal data. The determination of the legal nature of personal information rights relates to the composition of the protection mechanism of personal information, especially the civil rights system. On November 15, 2017, the Civil Law Office of the NPC Legal Affairs Committee issued *The Chapter of Personality of the Civil Rights of the People's Republic of China (Draft)* (Internal draft), in which the provisions regarding personal information are of great significance to the improvement of legal system and judicial practice.

Third, the legislation on personal data rights is of great significance. In traditional civil right system, property rights are the kernel of civil rights. However, in the era of big data, the right to personality has drawn more and more attention in the society. It is therefore necessary to establish a new personality right system in modern civil law to adapt to the development of the information age. The right to personal data should cover the protection of both spiritual interests and property interests of the personality, that is, a data subject can, for a commercial purpose, trade his personal data in the market of data products as long as his personality is not damaged. In case of an infringement on property interests, the losses incurred by the data subject can be calculated at market prices (Wu 2016).

The theory of intellectual property rights

Some law scholars found that data is inextricably linked to the protection of intellectual property rights since data is reproducible and reusable. They suggested that the theory of intellectual property rights can apply to data rights. The theory of intellectual property rights cannot provide complete protection to data due to the limitation of the theory of immaterial objects, but, with the technological development, creation and processing of data by data subjects, such as association analysis, data fusion and data mining, a new data set or a personal database comes into existence and bears a trait of originality to a certain extent. It therefore should be deemed as intellectual property rights.

Data property rights are similar to information property rights, whereas information property rights are an extension of intellectual property rights

(Zheng & Zhu 2006). With the development and widespread use of information technology, many laws regarding the protection of information processing technology and transmission technology have been enacted, but little attention has been paid to the protection of information itself. In the *Outline of Intellectual Property Strategy* promulgated in Japan in 2002, information property and intellectual property were said to be the most important assets of the twenty-first century. "Information property rights" and "intellectual property rights" are the same in meaning (ibid.). The third wave of the technological revolution has brought about a revolutionary change. Information has become the main property, replacing land, machinery and other tangible property. However, information property rights are protected mainly under the traditional intellectual property law.

In cyberspace, infringements of patent, the rights to information network dissemination, business models, source code, etc., occur frequently. The *Special Report on the Big Data of IP Infringements* (hereinafter referred to as *Special Report*), issued by the Supreme Court in September, 2017, showed that, in 2015 and 2016, copyright cases accounted for 50.2 percent of intellectual property cases in China; and three quarters of them were cases involving infringement on right to information network dissemination or right to display. The statistics in the *Special Report* showed that the time the court spent on cases of passing off others' patents, infringement of patent of invention, and infringement of software copyright exceeds the average case-handling time. And the lawsuits involving IP infringement were settled mainly by withdrawal of complaints. Issues involved in the big data lawsuits handled by the court are such as the original data subjects were unclear, the legal nature of data rights was undetermined, people did not know what cause of action they could have to protect their rights, etc. Under the current legal framework, neither theoretical discussions nor judicial practices have provided definite answers to these questions.

In a word, what the law protects shall be fixed in a particular media and in a certain form (Li 2013). The protection of data rights related to big data includes copyright, patent for business modes and data analysis, trademark of data products, trade secret, etc. Different data rights can be protected by different competences in IP systems, based on the rights and interests in data resources.

The protection model of products with originality. Throughout the whole process from data creation to utilization, four types of protection of rights and interests are involved. First, data which is collected, transmitted and stored in the database is eligible for copyright protection. Second, data, through association, fusion, mining analysis, maximize their value, and are eligible for trade secret protection. Third, creative techniques and methods that are created in the process of data processing are eligible for patent protection. Fourth, data products fixed in software are eligible for copyright protection of computer software.

The protection model of products without originality. Data without originality is also collected and processed at substantial costs. Scholars of traditional theory of originality propose to exclude from copyright protection collected and arranged data with high-value-density but no originality. Neighboring rights protection can be extended to objects that copyright protection cannot cover, so data collectors or possessors are granted neighboring rights. The era of big data is the era of data explosion. The cost of finding effective data in the data torrent gradually outweighs the creativity of expression. Most datasets established for collection and dissemination of effective contents are not original. Meanwhile, the rapid development and widespread application of data mining technology, intelligent technology and business modes have made data play an increasingly important role in all areas of economic and social development. Datasets, as special objects, although not eligible for the protection under copyright law or unfair competition law, can be protected by neighboring rights, given its features of non-originality and high value density.

The theory of trade secrets

In the era of big data, the global data volumes are exploding every day. Data is easy to be obtained due to its attribute of easy dissemination. Today, with the rapid development of digitization, trade secrets are mainly manifested in the form of data. Unlike in the traditional network environment, trade secrets in the era of big data are easier to be disclosed. And under the traditional legal framework, the security of trade secrets has become an outstanding and tricky issue mainly due to the circumstances, such as legal restraints on

data transactions, especially data transactions involving trade secrets, are lacking; a large number of trade secrets data is stored in a unified server, being susceptible to attack; the complete trade secrets can be obtained from scattered corporate data by big data mining technology; corporate employees are prone to disclose important enterprise information for lacking awareness of data protection; data storage and transmission are hard to be controlled due to its easy-to-store and easy-to-disseminate features, which goes against the protection of trade secrets and corporate rights; high technology in the era of big data makes infringement more elusive, its impact is more complicated and serious, and protection of trade secrets more difficult. All these issues have posed more challenges to the existing laws and regulations.

The *Anti-Unfair Competition Law of the P.R.C.* provides for the trade secrets protection, but fails to define the "right to trade secret." Meanwhile, the *General Provisions of the Civil Law* has included trade secret into intellectual property and gives a definition thereto. A trade secret has trade value. It is confidential and non-exclusive. On the one hand, a trade secret shall be unknown to the public. Once a trade secret falls into the public domain or is disclosed, its trade value will be lost. This characteristic makes it obviously different from traditional intellectual property. On the other hand, trade secret right is relative and non-exclusive. Once a third person obtains a trade secret by proper means, he shall have the same right with the prior owner. Data also has economic value. It is also confidential and non-exclusive. Under certain circumstances, data may be deemed as a trade secret. A trade secret has three elements: value, confidentiality and manageability, but in the era of big data, many new circumstances have posed challenges to the requirement in the following aspects.

First, conflict in confidentiality identification. The conflict in confidentiality identification mainly refers to the conflict of privacy with accessibility and the conflict of confidentiality with transparency. Conflict between privacy and accessibility. Unlike in the traditional network environment, the era of big data has brought about new changes: there emerges a great many new types of media, the information access channel is more diversified and extensive, and data acquisition has become extremely easy. Thus, whether a particular data is confidential has become controversial, making it difficult to identify the confidentiality of trade secrets. In the production management of enterprises, network information technology is widely used.

Social network software, WeChat, QQ, e-mail and other business information dissemination methods, online cloud service data processing methods, and corporate employees' communication by the social network software on business sensitive information, etc., have increased the risk of disclosure of trade secrets to varying degrees. These kinds of business sensitive data are inadvertently transformed into network data in daily work. And the features of network data being easy to be accessed undermines the confidentiality of trade secrets.

Second, conflict between confidentiality and transparency. All data stored in the cloud is completely transparent to cloud service providers. The account password of the enterprise user is useless for the cloud service provider. Data stored in the cloud by enterprise users is actively and voluntarily uploaded. Generally speaking, such voluntary disclosure of trade secrets is not legally protected. If enterprises do not pay attention to this transparency feature of big data, it is likely that trade secrets are exposed to potential risks at law.

Similarly, an enterprise transmitting its trade secrets to a third party does not constitute voluntary disclosure of the secrets. Nor does it mean that the enterprise gives up the confidentiality of the trade secrets. As long as the data is not disclosed or used by others, and the right holder has taken other protective measures and kept it confidential, the trade secrets data shall still be under protection of the trade secret law. Therefore, express confidentiality agreement on trade secrets protection is crucial when it comes to the storage and transmission of trade secrets data. Second, "reasonable confidentiality measures" are difficult to identify. Manageability is an indispensable element of trade secret. The law requires right holders to take reasonable measures to protect trade secrets.

However, in big data applications, it's hard to identify whether some acts fall under the category of "reasonable confidentiality measures." For instance, if a rights holder uploads trade secret data to a password-protected cloud, will the act adversely affect the protection status of the trade secrets? Some scholars hold that "reasonable confidentiality measures" have been taken if the data is stored in a private cloud and "reasonable confidentiality measures" have not been taken if the data is stored in the public cloud. It does not make any difference whether the password is an ordinary one or not, since, unlike public cloud, private cloud itself features isolation of

other users. However, some other scholars assert that public cloud service providers provide ordinary password protection (accessible only through a username and password) while providing service to customers, so there are "reasonable confidentiality measures" as long as other people are aware of these confidentiality measures which can ensure the user's trade secret data cannot be obtained easily by the search engine. In addition, the technical level of cloud service providers also can affect the identification of "reasonable measures." The characteristics of dynamic sharing of cloud service data make data management very challenging. If the technical level of cloud service providers is too low, unauthorized data access and network attacks will threaten users' data security, resulting in users' data being easily stolen, which directly affects the identification of "reasonable measures."

In addition, it is difficult to determine the scope of the objects. With the emergence of mobile communication devices such as smart phones, the mobile Internet has developed rapidly, and its powerful data generation capability has become one of the main driving forces for the development of big data in the world. Nowadays, obtaining and sharing data has become an important part of human social life. According to statistics, there are about 5 billion mobile communication users in the world. These users are potential information recipients and consumers. Such a large user group means unimaginable business value. Through social network platforms (such as Weibo and WeChat public account), enterprises can promote business and gain business benefits. Moreover, as the enterprise enhances its account management, the online relationship circle of the account is increasingly expanding and maturing and, consequently, the influence of the enterprise will continue to expand. Moreover, these social network accounts, as representatives of the enterprise on the network, are an integral part of the enterprise and hence are irreplaceable. Therefore, the protection of corporate social network accounts by the trade secret law is a demand of many enterprises. As a result, the object scope of trade secret extends from enterprises to corporate social network accounts, giving rise to the problem of the expansion of the object scope. Judged from the cases which have been handled, this practice has not been supported by the court yet. However, with the development of big data, it is likely that the data that was not deemed as a trade secret in the past will be included in the object scope of trade secrets protection.

Theory of data property rights

In accordance with the theory of data property rights, data is property in nature. It is a new type of property. Under the background that the current legal systems of personality rights, intellectual property rights and trade secrets are insufficient to provide reasonable protection for data, it is of great practical significance to establish data property rights through legislation. "Data banking" and "data conventions" which appeared as early as 2008 show that the global market of big data, with data as the transaction object, has been formed, and it is well-accepted that data is a new type of property.

Data is not a "thing" in the Real Right Law. Therefore, data property right and real right are not identical. Data property rights cannot be regulated by the real right system. The concepts of "a thing" and "real right" were proposed in the German Civil Code in the second half of the nineteenth century, in which "a thing" is defined as a tangible object and "real right" as the right to dispose a tangible object. These definitions are made on the basis of the idea that the ownership to interests in a thing is determined by the ownership to the thing. The right to economic interests in the thing and the thing itself shall belong to the same subject. Ownership to a "thing" constitutes complete real rights while the thing is the object to which the real rights are attached. Under the general doctrine of jurisprudence in China, a "thing" is characterized with its exclusivity and disposability. The exclusivity of real right is determined by the physical form of a thing. At the same time, the subject of a "thing" is unique and a "thing" cannot be owned by two subjects. One subject's control over the "thing" constitutes exclusion of others on the "thing." The exclusivity of real right is attributed to the two factors: 1. the physical form of a "thing" objectively determines the actual monopoly in possession of the "thing," that is, it can be owned only by one person rather than two at the same time; 2. in the process of use, the value of the "thing" itself and its use will be reduced overtime. When one gains profits from the "thing," others will be excluded from gaining profits from it at the same time.

Contrary to a "thing" which has physical form, the most striking feature of data is its non-physical form. Data is different in nature from electricity, heat or other "non-physical" objects under the *Real Right Law*. Each unit of electricity or heat can be owed by one subject at one time. And electricity

or heat as an object can be consumed by its subject. Meanwhile, the non-physical data can be copied indefinitely nearly at zero cost and without any loss. The value of data does not lie in data itself but its contents. Therefore, data theoretically is not exclusive in terms of possession and disposability. In the development of data industry, since data can be infinitely copied without any loss, it has become an internal demand of the data industry for using data as sufficiently and frequently as possible.

The non-physical form makes controllability of data differ from exclusivity of a thing. Although data can be copied and used indefinitely, it does not mean that data is uncontrollable. A rights subject may control the data in his or her possession in accordance with the law. Other subjects may be authorized by the rights subject to use the data within certain scope. Thus, the possession and control of data is not physical monopoly. Unlike property which can only be owned by one subject at one time, data can be owed by two or more subjects at one time.

In a word, data is a new type of object which has no physical form and is non-exclusive and non-depleting. Take personal data for example, individuals, enterprises, and government agencies can use the same personal data at the same time. Although personal data is targeted at individuals, the three subjects do not conflict with and exclude from each other in disposing the same data. Of course, enterprises shall meet certain requirements before using the data; government agencies may use it for the purposes of national security, social management and provision of public services. In addition, the value and the use value of the data are not reduced when it is used. Therefore, in terms of attributes, data and a "thing" in the Real Right Law are inherently different. Besides, data property rights shall not be interpreted as an expansion of real rights. The concept of ownership is derived from the integration of a person and a "thing." Its value lies in identifying who owns a "thing," and establishing the complete possession of and control over the "thing" by the subject. It can be seen that tangible objects are the basis of real rights system and the theories on real rights system. But it is obviously inappropriate to apply real rights theories to data property rights. To apply the theories of things and ownership to other *res incorporales* will inevitably cause a theoretical dilemma. The transfer of rights is a manifestation of transfer of property of all kinds in a civil relationship. Thus, as long as the ownership is defined by law, *res incorporales* can be understood from the perspective of

ownership and transfer of ownership, regardless of the framework of objects and ownership. Data property and tangible property are owned and disposed in different ways. Therefore, the real rights system, which is applicable to tangible property, cannot be applied to data (see Table 6).

Table 6. Theories of Data Rights.

Theory	Main ideas, reasons, and drawbacks
Theory of a new type of personality rights	Main ideas: Personal data rights fall into the category of personality right. It is a specific new type of personality right.
	Reasons: First, in terms of the connotation of the right, personal data right shall protect personal interests. The subject of data has a right to possess and dispose their personal data, which is the special connotation of the right. Second, in terms of richness of the object of the right, citizen's personal data generally include personal general data, personal private data, and personal sensitive data, some of which, such as name, portrait, privacy, has become specific personality rights for which, unlike other data, the protection mechanism of personal data rights is unnecessary. Third, in terms of the effectiveness of the protection mechanism, if a personal data right is deemed as a property right, it is unnecessary to protect against infringements on personal data of individuals; if it is deemed otherwise as a personality right, then on the one hand, the protection is necessary in ensuring that distinctions are not made on the way of calculation due to the difference in people's identities, thus in conformity with the principle of equality of personality; on the other hand, citizens may claim for compensation for spiritual damage in accordance with Article 22 of the *Tort Law*. Finally, from the perspective of comparative law, personal data protection laws all over the world mainly aim at protecting citizen's personal interests.
	Drawbacks: The personality rights of a natural person are exclusive and unmarketable. Any economic value produced therefrom cannot be deemed as property; otherwise, the value of identity as a natural person will be derogated.
The theory of intellectual property rights	Main ideas: Personal data rights fall into the category of intellectual property rights and, therefore, can be protected by copyright and neighboring rights.
	Reasons: First, databases or datasets with originality in selection and arrangement may be deemed as a copyrightable compilation. In

Theory	Main ideas, reasons, and drawbacks
	accordance with Article 14 of the *Copyright Law of the P.R.C.*, the copyright of a compilation with originality in selection and arranging of the contents of any works, excerpts of works, data which does not constitute a work, or other materials shall belong to the person who compiles the work. The "originality" therein does not refer to that in contents but in selection and arrangement of the contents. Second, databases and datasets without originality can be protected under the system of neighboring rights which are granted to the people who disseminate the works. German laws expressly provide that the system of neighboring rights applies to the protection of databases. The holder of a database who has made substantive investments in collecting data and establishing the database shall have the neighboring right to the compilation as a compensation for the labor and money the holder spent on the collection and arrangement of the data.
	Drawbacks: The low identification rate of data and the unique ways to realize its value make data difficult to become an object of intellectual property right. First, the identification rate of data is inferior to any of the objects of intellectual property right in creativity and novelty. Once the low-identification-rate data is illegally used, it is difficult to be discovered and redressed in a timely and effective manner. "There is no right without relief." Lack of relieves makes effective protection of data impossible even if rights are granted. Second, the value of intellectual property lies in the benefits gained through monopoly of economic use or circulation. The value of data is more manifested in the mining of potential information. The value of intellectual property object lies in the "results" of intellectual creation, which are valuable themselves, while the value of data with no value in itself lies in the instrumental "utilization," that is, operational control and content analysis.
The theory of trade secrets	Main ideas: Personal data is analogous to trade secrets and can be deemed as trade secrets under certain circumstances.
	Reasons: First, commercial benefits can be obtained by appropriating commercially valuable trade secrets. At the same time, trade secrets are non-public and non-exclusive due to its non-exclusive possession and control. Therefore, once it is disclosed and known by a third person, its commercial value to the original right holder will be diminished. Second, through the mining and analysis of data, corresponding commercial benefits can also be obtained and therefore data has

(*Continued*)

Table 6. (*Continued*)

Theory	Main ideas, reasons, and drawbacks
	economic value. Appropriation of data by a third person means that data is out of the control of the original holder and consequently the third person has the same rights in the data. Therefore, data is non-public and non-exclusive. Third, with the help of big data technology, complete trade secrets can be obtained by analyzing the fragmented commercial data, leading to the disclosure of trade secrets.
	Drawbacks: Trade secrets are characterized by being unknown to the public and bringing economic benefits to the right holders while data in cyberspace is accessible to the public, that is, most data are not trade secrets. In addition, the mere including data in trade secrets will seriously hinder circulation and application of data, which makes the achievement of the value of data impossible.
The theory of data property rights	Main idea: "Data property right" is a new type of property right. It means that each citizen has right to the commercial value of his own personal data.
	Reasons: With the advent of digital age, personal data has in fact the function of safeguarding the property interest of the subject. At this time, what should be done is to recognize at law and in theory that the subject has property rights in his personal data. Some scholars take the citizens' personal data right as a kind of ownership, that is, citizens have the right to possess, use, benefit from, and dispose of their own data.
	Defect: If a personal data right is deemed as a property right, its commercial value would be over-emphasized and the protection of citizens' personal data could be ignored. The latter is actually the primary goal of the personal data legal system and the most realistic demand of citizens. In addition, if the "person" in "personal data" is neglected, equality of personality will be inevitably impaired since "business is business." "People's information are different in value due to their different economic conditions, but their personality should be equally protected."

Definition of Data Rights

The aforementioned theories of a new type of personality rights, intellectual property rights, trade secrets, and data property rights, though reasonable to some degree, fail to exhaust all the circumstances that should be covered by

the data rights system. Data rights shall not be considered from a perspective of one particular right. Instead, Other perspectives shall also be taken into consideration. Meanwhile, data rights shall also be defined in the aspects of the subject, object, civil rights, state sovereignty, sharing rights, etc.

The subject and object of data rights

A. THE SUBJECT OF REAL RIGHT VS. THE SUBJECT OF DATA RIGHTS

Both Roman law and Germanic law defined the scope of real right with restrictions. In the period of Roman law, the subject of real right referred to a natural person who had all or part of the personality. Only those who had a complete personality could exercise full real rights. A slave as an object of real right could not be the subject of real right. In the period of Germanic Law, the subject of real right is divided in a top-down approach in correspondence with his hierarchical identity. Although people with different identities have different real rights, kings, lords, free people and serfs were all regarded as the subjects of real right. In China, as the *Book of Songs* said, "Of all that is under Heaven, no place is not the king's land; and to the farthest shores of all the land, no man is not the king's subject." In the feudal dynasty before the Republic of China, the subject of real right referred to the ruling class represented by the king or the emperor. Later, under the influence of Confucianism, parents and patriarchs became the representatives of real right subject, but they were also severely restricted. Since the modern times, under the impetus of social progress, the subject of real right has no restrictions in terms of social hierarchy. The *Real Right Law* stipulates the subject of real right as rights holders and imposes no restrictions on the subject of real right. In China, the subject of real right refers to the state, collective, legal persons, unincorporated organizations and individuals.

Data rights refer to the legal right of the subject requesting or claiming for the possession of data by the claimant, for the return of data, or for the recognition of particular facts (behavior) of data. The subject of data rights is a particular person of right, that is, a particular person or a person responsible for collecting, processing, transmitting, and storing the data. The said "person" includes natural persons, legal persons, unincorporated organizations, etc. However, the rights of different right subjects should

be different. For example, the copyright holder in the Copyright Law has copyright and full personal and property rights to the work. The one who creates a work by adapting, translating, annotating, and organizing existing works also has copyright with the prerequisite that no infringement is made on the copyright of prior works; the performer and producer of audio and video recordings must obtain the dual permission of the copyright holder for the performance and recording of the adapted works, and also enjoy certain rights of performers and producers of audio and video recordings. Therefore, for the subject of data rights, the uses of the data can be classified, and specific rights can be granted or restrictions on rights can be imposed.

B. THE OBJECT OF REAL RIGHTS VS. THE OBJECT OF DATA RIGHTS

The object of rights is the object pointed to by the contents of rights, or the object to which the rights are exercised. It indicates the circumstances under which the subject of rights can act or not act on an external object (material object or spiritual object). This kind of object always co-exists with the rights themselves. The object of real right is the object of real right enjoyed by the real right holder. The object of real right has the following characteristics.

First, the object of real rights is a thing. The so-called thing only refers to tangible physical property. The elements of physical property are as follows: the thing is physical; it exists independent of the human body, except as otherwise provided by law; it is capable of being controlled by man; it has use value and exchange value and thus can meet the spiritual and material needs of people. Things are physical, so they are also called tangible property or *res corporales*. None of non-physical property can be called *res incorporales*. Some of them can only be called intangible property rather than *res incorporales*. Sound, light, electricity and heat do not have a physical form, but are still physical, fall under the category of physical property. They, as special manifestation of physical property, are extensions of tangible property. Deeming them as intangible property from the perspective of human sense is understandable, but what the book intends to emphasize is that there is no such a thing as a *res incorporale* defined in real right law. The theory of *res incorporale* not only conflicts with the semantic rules, but is also likely to cause confusion of the basic principles in civil law.

Second, the object of real rights must be specific. A specific thing refers to a unique one which has special traits and cannot be replaced by other things. Real rights are the rights enjoyed by a particular right holder to control a thing, and the thing under control must be specific or definite. Things which are not specific are not controllable to a particular right holder. The so-called real rights hence do not exist. Therefore, the real rights owned by a right owner must refer to the rights and interests in a specific physical object, such as land, houses, refrigerators and color TVs. Meanwhile, any transfer of real rights shall be demonstrated by registration or delivery. If the object of real rights is not specific, registration or delivery cannot be made. It, therefore, can be concluded that the legal relationship of real rights has a natural and logical requirement that the object of real rights must be specific. A species, in contrast to a specific thing, is not the object of real rights; but when specified, for instance, by selection or delivery, it will become the object of real rights.

Third, the object of real rights is controllable. The real rights lie in controlling the property and enjoying the interests therein. This concept is obviously different from the obligatory rights. The real rights refer to the control of a person over a thing while the obligatory rights refer to the rights of a person to make a claim to another. The control of a subject over a thing means that the subject, through no media, can impose his will upon a thing as an object, that is, the right holder is capable of controlling a thing without any influence from others.

Fourth, the object of real rights is exclusive. The real rights can be fully obtained only by excluding others from interference including illegal interference of both public powers and private rights. A right holder may exercise his real rights at his own will. He is free to dispose his property. No prior consent or interference by a third party is needed. When an infringement occurs, the right holder may claim for relieves including injunction, restitution and compensation.

Compared with real rights, data rights belong to a new type of right relationship with a focus on the rights and obligations of the subject of data rights to the data. For data, the requirements of specificity, controllability and exclusivity of real rights are difficult to satisfy, so data cannot be a "thing" as the object of real rights. In addition, data, unlike intellectual property, is hard to be identified, and the methods to realize its value are

comparatively unique. All these factors prevent data from becoming the object of intellectual property rights. Therefore, a new type of rights relationship between people and data should be established independently of real rights and intellectual property rights.

The object of the data rights is specific data, especially datasets. In the data society, a single datum is no more than a meaningless digital symbol. Only a specific dataset is valuable. Data is different from the thing defined in civil law. Generally speaking, the so-called object refers to the *res corporales* and natural forces that exist independently of the human body, and can be controlled by human to meet the needs of human society. Because data is intangible, it is difficult for civil subjects to achieve complete control over it. The control is actually very limited. In addition, data is not fully deliverable. Data is easily retained in the transaction process due to its feature of reproducibility, which makes it difficult be absolutely exclusive. Although the storage and transmission of data will take up space, this space is virtual rather than physical. Therefore, data is different from things and does not fall under the category of a "thing," but this feature does not hinder data from meeting certain social needs. Data right holders have the right of control over the use of data sets in the similar way they use things.

Data rights: A new type of civil rights

A. WHAT ARE DATA RIGHTS?

With the advent of the big data era, data has now become an objective and independent reality. Nonetheless, being something not tangible but digitalized symbols, data falls outside the category of "property" as defined in the *Property Law*. Since the *Property Law* governs the ownership and use of tangible properties, data is not something within its parameter. In an era of big data like nowadays, citizens enjoy such rights, that is, data rights. Data rights comprise a number of rights with regard to data, such as the right to own, collect, store and utilize data, the right to data privacy and the right to be informed. Those who enjoy data rights, that is, citizens, may automatically enjoy a wide range of rights as could be seen encompassing rights of personality and rights of property (see Figure 3).

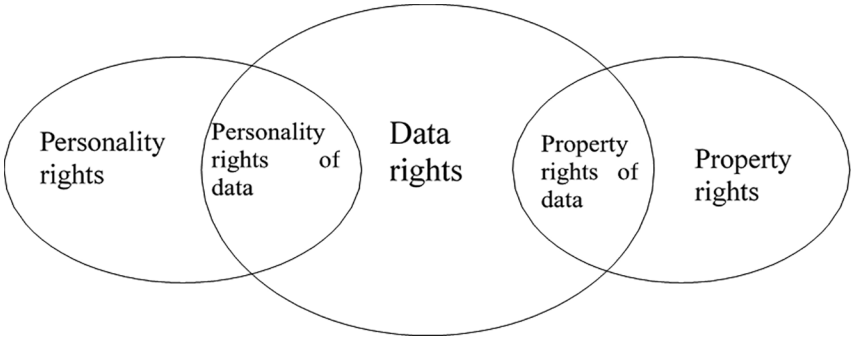

Figure 3. The Relations of Data Rights.

Data rights embody the personality rights of citizens. In most traditional civil law theories, personality rights are inherent, inalienable and imprescriptible rights enjoyed by the subject, which are in nature passive and defensive, exclusive of property attributes. The objects of personality rights are elements that compose an individual's personality. Personality rights belong exclusively to the subject and are with no direct property attributes. Personal data, as an inherent element that composes the personality of an individual, plays the crucial role of maintaining one's personal dignity. To begin with, personal data of a citizen is a kind of personally identifiable information that are exclusively owned by a specific natural person and that traces to a particular natural person. The personal data of a citizen can be used to identify the person. Also, a citizen's independent control over his or her personal data reflects individual personal dignity. In terms of content, data right could also be defined as a right of personality. However, unlike traditional rights of personality, the nature of data rights is derivative. Data rights are derived from traditional personality rights. The object and content of data rights are also different from those of traditional privacy right. Therefore, data rights are not only a new and independent category of rights, but also irreplaceable by traditional personality rights and privacy right in term of functions. The personality rights of a citizen embodied in personal data determines that, as the object of personality right, personal data must be protected and secured.

Data rights also embody property rights. Personal data often contains great value. Such values may mean great economic benefits for obtainers of

personal data when it is exploited by another party other than the legitimate owner of such personal data. In the past, due to limited economic and technological resources, personal data had not been commercialized and its potential economic value underestimated. Now, with the advancement of information technology, people come to realize, exploit and tap into the potential economic value of personal data. Data has gradually become a category of resources. Since every resource has its property attributes, data rights should be viewed as falling into the category of property rights and thus properly protected.

Data rights are independent from other types of rights. Data rights shall not be simply identified with personality rights or property rights, but are more like an integration of the two while remaining independence. In fact, contents of data protection could be found in both personality right law and property right law. These two kinds of laws are with different means and focus and cannot completely substitute each other. With regard to data rights, property law and personality law are not "either-or" but "both-and." Personal data of citizens, as the object of data rights, epitomizes the personality and property attributes of data rights. Nevertheless, personal data is not the only object of data property rights. Other data with economic value may also be considered as objects of data property rights. Along this line of thought, the personality rights and property rights may play concerted role in the protection of personal data; while other data with economic value could only be related to property rights.

B. CORRELATION AND GAME PLAYING BETWEEN DATA RIGHTS

Data rights tend to be recognized along with the producing of data, and have been attracting wider attention with the reality of big data. As big data evolves, new types of data rights emerge, including not only conventional rights such as information property rights and the right to privacy, but also new rights. All too often, for each type of data rights, the information involved and the subject of right are different from one another. Different data rights are interconnected, intertwined and interdependent. Such an interaction or game playing among those rights give rise to a new regime of rights that may bring huge impact on various aspects of our social life.

In addition, the most recent information technologies, such as big data and mobile Internet, have facilitated digitalization of our society and continuously lowered the cost of data collection, storage and utilization. As the main source of data, people produce data in every single minute throughout his or her life. Data exists in huge quantity and vast diversity. With the help of powerful computing capacity of machines, data users can easily sort out the correlations of different data and identify every single trace of a particular person's life or lives of a group of people. Going one step further, these data can even be used to predict future behaviors and thus producing economic benefits. Hence, it is necessary to provide sufficient protection for data rights against illegal collection and utilization of personal data.

Furthermore, mass data indicate mass values. Personal data in large quantity and diversified forms could be rather valuable in both strategic and economic terms. Without effective collection, storage, cleansing and digging, personal data can hardly be turned into end products, nor can data technology be effectively upgraded. Therefore, data rights not only reflect the personality rights and property rights of individuals, but also influence the development of digital economy of a nation. For data companies that have a pressing demand for dealing with personal data, in particular, it is of crucial importance to specify whether they are eligible for obtaining personal data, if the data are obtained through legitimate channels, and what types of rights they possess. To some extent, data rights protection and the relevant regime may play a vital role in data traffic and the development of the entire data industry.

C. PREDICAMENT OF PROTECTING DATA RIGHTS

The existing regime of legal rights is defined by real-life concrete elements. This right regime is human-centric and constantly evolves with the outside world. New legal relations will take shape when changes happen in the outside world. In the era of big data, data rights could be perceived as such kind of emerging legal relations. Data rights are not a set of independent rights but rights derived from the virtual world that could hardly be handled within the existing concrete legal regime.

First, take a look at the limitations of the personality right theory. Personality right, such as the right to name, image and reputation, plays a

very limited role in terms of the protection of personal data. Processing of personal data, such as names and images of individuals, doesn't always constitute a violation of personality rights. According to traditional civil law theories, the personality right is purely a right with spiritual ramification. With the expansion of commercialization, personality rights begin to take on attributes of properties. People began to realize and uncover property rights embodied in the rights to name and image. However, the key function of personality rights remains intact. Data rights consist of both personality and property rights, and both spiritual rights and property rights of individuals shall be subject to protection. Under such a category of rights, relations among the possessor, processor and users of data shall be balanced. Therefore, data rights should cover not only the spiritual and property rights and interests of data possessors, but also the property rights and interests of data processors and users.

Let's then examine the limitations of the privacy right theory. Personal data does not equal privacy because the latter does not cover the extended meaning of data rights. Privacy refers to the right of individuals to seclude information about themselves, their personal activities and personal space. Such information entails no public interests and is not made public. Personal data may already be disclosed to the public or fall within the sphere of public order, whereas the protection of its privacy may thus be restricted by public interests. A very small portion of personal data would be kept in confidentiality and the majority is non-confidential. "Genetic information, medical records, health check documents, criminal records, home addresses, private activities"[1] and other sensitive information are protected by the privacy law. However, personal data, such as name, telephone number and address, once disclosed by its owner, may not be protected by the privacy law no matter how it is utilized by a third party. Once disclosed to the public, technical desensitization of personal data increases the complexity of privacy protection. It is then difficult for an individual to resort to the privacy law and to enjoin other people from using his or her personal data. Consequently,

1 The Supreme People's Court. 2014. *Provisions of the Supreme People's Court on Several Issues concerning the Application of Law in the Trial of Cases involving Civil Disputes over Infringements upon Personal Rights and Interests through Information Networks* [EB/OL] (October 21) <http://www.court.gov.cn>.

personal data would not be protected by means of seeking relief from the property law. In a word, in terms of the processing of personal data, the existing privacy rights and interests can only offer very limited protection mechanism for personal data.

The limitations of the property rights theory will be addressed in the following paragraph. When data rights are concerned, the theory of property rights delivers its functions mainly through an emphasis on the right to control data rather than the right to use data. Data lacks the independence of a civil object; thus, it is contradictory with the principle of "one ownership for one object" (meaning that one and only one ownership can be established for an independent object). Individuals are the primary producer and source of data. When these original data are collected, processed and analyzed by other parties, individuals are no longer the sole contributor, actual possessor or controller of data. In other words, individuals are only providers of data. Without the network services and technical support provided by data collectors, data cannot be generated and the information embodied in data will not exist.[2] "All data rights and interest allocations in data provided in our laws need appropriate codes to decipher" (Mei 2016). This means that, individuals don't enjoy comprehensive property rights of their personal data. Nor can they do transactions of data, or exercise data rights in accordance with property laws. All in all, the property rights theory has obvious limitations in the protection of data rights.

What about limitations in the theory of creditor's rights? The theory of creditor's rights advocates the protection of virtual property by using the law of contract and emphasizes the contractual relations between network service providers and their subscribers. In terms of data creditor-debtor relations, the owner and the collector of data may have contractual relations. However, given the complexity and dynamism of data rights, the data owner and other data users may not be able to strike a contract for the benefit of third-parties. Even if such a contract is established, out of consideration for interests, data users often exclude the lawful rights of data owners when drafting the contract. Without contractual terms on data rights, data owners lack

2 For instance, on August 19, 2013, when Yahoo China stopped its email service, all of its users could not log in or use Yahoo mail and all the emails and other content stored in its email server could not be accessed any longer.

the legal basis to request the nullification of the right exclusion clause. In the eyes of the parties to contract, data is not viewed as a contractual object, but an invisible object. Unless the legal status of data is clearly sorted out and properly defined, a series of problems will not be resolved in the protection of data rights using contractual clauses.

Finally, limitations of the theory of intellectual property rights will be discussed here. Intellectual property rights do not cover the protection of personal data. So far, there is no such a country around the world that uses intellectual property rights to address the protection of personal data. Scholars who proposed the inclusion of personal data to the scheme of intellectual property protection only find it easier and more feasible to protect the relevant rights of data users but not those of data possessors. Since there is an intrinsic connection between data and knowledge, data rights and intellectual property rights share many similarities. Meanwhile, data rights protection aims to facilitate data use while ensuring open access to data. It is thus fair to say that IP law is the closest right protection regime relating to the protection of data rights. Yet, in essence, it is impossible to apply IP laws here in the matter of data rights protection. First and foremost, data does not meet the originality requirement of IPRs; secondly, intellectual property protection cannot ensure the monopolized commercial utilization of data for obligees. Besides, IPRs follow the principle of exhaustion of rights, which means that owner of an IP right does not have absolute control over his or her patented products. However, data rights are reproducible and not exhaustive. In sum, IP protection would not be the same as the protection of data rights.

Data sovereignty: A new type of national sovereignty

Cyberspace is also under the reach of law. It also has sovereignty. At the Third World Internet Conference, President Xi Jinping proposed the concept of cyber sovereignty. *Cybersecurity Law of the People's Republic of China* also provides for the principle of cyberspace sovereignty. Sovereign equality is the basic principle established by the UN Charter in the physical international space. Respect for cyberspace sovereignty is the extension and development of this principle in virtual cyberspace. Data is the core existence

of cyberspace; whose security is beyond the traditional security scope and rises to the level of national security. Nowadays, many countries and regions, including China, have put forward the requirements for localization of data storage. Like cyberspace sovereignty, data sovereignty has become a new type of national sovereignty. Defending national data sovereignty in the global data torrent is an unavoidable key issue in the era of big data.

A. THE CONNOTATION OF DATA SOVEREIGNTY

Data sovereignty refers to a country's highest jurisdiction in generating, collecting, transmitting, storing, analyzing, and using all the data in the forms of text, pictures, audio, video, code, programs, etc., generated by individuals, enterprises, and related organizations within the jurisdiction area of a country. The connotation of data sovereignty is mainly reflected in the three aspects: data control rights, independent development rights of data industry and data technology, and data legislative rights.

First, data control rights. Cyberspace is composed of data. It can be said that data sovereignty is the core of cyberspace sovereignty. With the development of human society, following territorial land, sea, air, and space, cyberspace has gradually become a new territory for the development of all countries. Whoever can control the data can take the initiative in cyberspace. In the era of big data, data ownership will become a key factor for sovereign countries to have a voice in the international arena. In future, a country without data sovereignty will have difficulty in controlling the data resources of its domestic society, and it will be extremely vulnerable to violation, control or attack by other countries with data powers. The data security issue therefore may even threaten the security of national sovereignty.

Second, the independent development rights of data industry and data technology. With the development of big data, a new hegemonism probably engenders, that is, data hegemony. Developed countries have always controlled the high-end information technology (including software products, chips, etc.) by, which developing countries have depended on. For instance, China-US trade war reflects China's dependence on US chip technology. In the era of big data, data developing countries are also likely to rely on data products from data developed countries. And data developed countries will continue to strengthen this dependence, thereby turning data developing

countries into data colonies and implementing data hegemony. Therefore, the power to independent development in the data technology and data industry is a manifestation of a national data sovereignty, which belongs to the internal affairs of a country.

Third, data legislative power. The state, with the control of data, must protect the data security of the country by formulating corresponding laws and regulations in the data field. This is the data legislative power which represents a country's independent data management, which means that a country can, without interference from external powers, formulate its own data development strategy and data regulations and systems, and decide relevant matters in sovereign data field. Within the scope of international law treaties, the power of being free from any state's restraint and interference and taking the complete control over the domestic data management is an important manifestation of national sovereignty in the era of big data.

B. DATA SOVEREIGNTY AND NATIONAL SECURITY

Human beings are entering a digital age. In the fields of human economic development, social life, scientific research, even national defense and military, etc., the new generation information technologies, such as big data, cloud computing, and artificial intelligence, have been widely used. As a key factor, data has become the same as natural resources such as electricity and land. To become an important strategic resource of a country, the focus of national competition is also shifting from traditional resource competition to data resource competition. The volume of the data and the application capabilities will become an important manifestation of the competitiveness of the country in future. "The new round of powerful countries competition is largely to enhance the influence on and dominance over the world situation through big data" (Miao 2015).

With the development of big data, the game between countries around data control and utilization is becoming increasingly fierce. Many countries and regions have made big data development and application as a national strategy, and have launched big data development strategic plans to seize data resources, such as the *US Big Data Research and Development Plan*, the *EU Open Data Strategy*, the *Japanese Declaration of Building the Most Advanced IT Country*, and the *Australian Public Service Big Data Strategy*. In addition,

many countries and regions have implemented data localization policies and launched a data defense war. For example, countries such as India and Iran require domestic data to be stored within the country, and not to be permitted to cross the border. Russia requires localization of electronic communication and social network data of its citizens. The relevant data protection laws and regulations of the EU stipulate that data may be sent to countries or regions outside the EU provided that it is protected by local laws or contracts.

As data sovereignty becomes a new element of national sovereignty, data security has become a new focus of national security. Especially in the context of increasingly fierce data competition between countries, data sovereignty maintenance and data security protection are the content extremely important for national security. The "Prism Gate" incident fully exposed the fact that the United States used the core technology to commit network theft. With the help of big data and other means, the United States has upgraded its surveillance system over global data. Other countries are facing threat to national information infrastructures and important institutions which contain huge amount of data, such as water, electricity, transportation, banking, finance, health, commerce, and military.

In the face of data security threats caused by the lack of data control rights, many countries and regions have continuously enhanced their data security capabilities through various measures. At the same time, the establishment of data sovereignty is the fundamental way to improve data security capabilities, and the fundamental guarantee for preventing and reducing the attack on the national secrets, trade secrets and citizen privacy by external forces. Security is the bottom line of national sovereignty. In the era of big data, data sovereignty is fundamental to national security, economic development and social stability. In national sovereignty, data sovereignty should be placed in an important strategic position. Therefore, sovereign states should improve their data control capabilities as soon as possible and guarantee national security in the era of big data.

C. PONDERING THE SYSTEM OF DATA SOVEREIGNTY

National data sovereignty is a comprehensive system featured by multi-relation, democracy and diversity. In terms of digital features, there are multiple subjects of interests at the same time, which is an intrinsic feature

of digitization. From the perspective of digital functions, the efficiency improvement brought by digitization is effective and urgently needed for all aspects of human society, and consequently its function must be diversified. Therefore, when formulating the data sovereignty system, we should take a comprehensive approach in dealing with data security issues, and analyze them from a multi-dimensional perspective.

Conflicts, especially the conflicts between "free flow of data" and "data localization," exist in data sovereignty in the aspect of cross-border data flow. For instance, in July 2016, the EU and the United States resolved the disputes in cross-border data transmission regulation through the *EU-US Privacy Shield Agreement*, but in the end, the problem was solved only with temporary reconciliation but not settled fundamentally at all. The following year, the European Commission issued the *A Proposal for a New Regulation on the Free Flow of Non-personal Data*, requiring the countries which are involved in the trade to provide adequate privacy protection standards. In May 2018, the *General Data Protection Regulations* (GDPR) issued by the European Union went into effect. The act made strict regulations on cross-border data transmission. Different countries have different policy direction for cross-border data transmission. Compared with the "free data flow" tendency of the United States and the European Union, countries such as India, Iran, Russia, and Australia are more inclined to "data localization." Therefore, when formulating the data sovereignty system, we should also take into full consideration the conflicts existing in the current cross-border data flow.

At present, although China has no specific laws and regulations protecting the sovereignty of national data yet, the *Cybersecurity Law of the People's Republic of China* promulgated in November, 2016, has unprecedentedly proposed the concept of cyberspace sovereignty. It enriches the scope of sovereignty enjoyed by China and takes cyberspace sovereignty as the natural extension and performance of China's national sovereignty in cyberspace. Raising the concept of cyberspace to the level of national sovereignty is more conducive to safeguarding the legitimate rights and interests of our country from the violation of other countries or foreign organizations. Any acts, including illegal intrusion, theft, destruction of computers and other service equipment or the provision of related technologies in the field of cyberspace in China will be deemed as infringement of our national sovereignty. Although the *Cybersecurity Law of the People's Republic of China* does not

mention national data sovereignty, it clarifies the cyberspace sovereignty. In the cyberspace, data is the only "thing" that exists. In this sense, cyberspace sovereignty and data sovereignty are consistent. Before the establishment of the national data sovereignty system, the continuous improvement of the *Cybersecurity Law of the People's Republic of China* can maintain national data sovereignty legally in a more timely and effective manner.

Essence of data rights: A shared right

The technical structure and networking features of the digital society determine its internal characteristics – decentralization and borderlessness, that is, openness, equality, collaboration and sharing. Such distinctions also set the ecological base of the era, that is, "people first," as well as the core features of our time – "sharing." "Sharing" is exactly the fundamental distinction between data rights and property rights.

A. FROM "ONE OWNERSHIP FOR ONE OBJECT" TO "MULTIPLE OWNERSHIPS FOR ONE DATA"

The principle of "one ownership for one object" is a fundamental feature of the property rights. With more advancing technologies, more diversified forms of objects begin to surface, so is the case of the categories of rights *in rem*, which also indicates the ever-increasing complexity of differentiation between rights and functions of ownership. In reality, the traditional principle of "one ownership for one object" is challenged by "multiple ownerships for one object" and "one ownership for multiple objects," which have also been indirectly acknowledged or obscurely recognized by law to some extent in adjudication practices. The unique features of data, such as reproducibility, inexhaustibility and special publicness, make "multiple ownerships for one data" possible. Thus, allowing any subject of data to have absolute control over such data violates the principal of sharing. With the transformation of the era and technological advancement, when the cost of things continues to decline and even drops to zero, the exclusive ownership of properties will become obsolete. This is even more true for abundant data resources with zero marginal cost. Its natural features, such as non-property object with multiple owners, determine that the essential prerequisite for "making

the best use of data" is sharing. Sharing, with "multiple ownerships for one data" as its main feature, becomes an inevitable trend. In the long run, scare resources tend to become more abundant. As a result, scarcity in resources will be replaced by trends of exchanging and sharing. "When seen through the lens of technology, few resources are truly scarce; they're mainly inaccessible" (Diamandis & Kotler 2014).

B. BORDERLESS SHARING

As the Internet breaks the limits of time and space, the borders between the virtual world and reality and between digital and material worlds are diminishing. Digital space has become a new realm and new sphere of human life. Compared with real world, digital space is more elastic, immediate and reversible in time, as well more compressible, fluid and sharing in space. The advent of digital space gave rise to a two-dimensional space structure featured by a combination of both the real and the virtual. The digital space reflects the essential power of data openness and sharing, pushing humankind to march towards a borderless future. In a borderless society, things tend to be rearranged and borders between them melted, private nature of private property rights weakens, replaced by sharing and co-ownership. Elements of production flow more quickly and innovations are more frequently seen and encountered. More elastic organic structure makes it possible for the relationship between people and organizations to evolve from the traditional exchange type to a type featured by sharing. According to Jeremy Rifkin, an economist and thinker from the United States, in the future society, we will not simply exchange value, rather, we will share value. In the past, no face value will be added to things without transactions and exchange. However, in the future, such an exchange mode will be replaced by sharing."

C. TRUST AND ALTRUISM FORM THE BASES FOR THE SHARING OF DATA RIGHTS

Openness is the premise for sharing and trust is its essence; the fundamental spirit of sharing is altruism, which originates from empathy.[3] Trust is the

3 In the Empathic Civilization, Jeremy Rifkin pointed out for the first time that: human being is a species with empathy. The core of human history is a struggle between

accumulation from concepts, regulations, laws, governance, etc., serving as lubricants and adhesives of social order and lowering the cost of social collaboration and transactions. Trust provides an indispensable basis for the sharing of data rights. Building upon universal values and consolidated trust, the sharing society will become an important social form of the future. Altruism, as a spontaneous and voluntary action of individuals to increase the benefits of others, will become the core of the future. The greatest common divisor of altruism is the integration of data rights, data utilization, data protection and data value. Altruism helps to improve people's awareness and willingness to share data rights, thus facilitating the positive interaction and transformation of sharing behaviors of people.

D. "THE RIGHT TO OWN" AND "THE RIGHT TO SHARE"

Property rights are essentially ownership rights. Property rights include the right to own, use, dispose and collect earnings from properties. The right to own property is the *de facto* control of property, which is also the most fundamental essence of ownership. Without the right to own, the right to use, dispose and collect earnings from property will all be affected. It is with the right to own, that the other three rights to property can gain grounds for their functions.

During the time of a planned economy, all things and materials shall be shared among people who are not supposed to own but only have the right to use property. In a market economy, as privatization and private ownership become more popular, individuals began to have the right to own things and ultimately possess them. In a sharing economy, ownership is no longer a matter of attention. What's more important is whether other people have the right to use things. The core of a sharing economy is, through networking, to share the right to use and to collect earnings from previously exclusive properties with other people so as to obtain economic benefit (He 2017). The transferral of the right to use things and sharing make

---

empathy and entropy. "We now face the haunting prospect of approaching global empathy in a highly energy-intensive, interconnected world, riding on the back of an escalating entropy bill that now threatens catastrophic climate change and our very existence." To resolve this empathy/entropy paradox requires us to have a fundamental rethinking of our philosophical, economic and social models.

underused items useful again. The necessary premise is that the owners of underused things are willing to transfer the right to use their properties. Essentially, it is still a matter of who has the "right to possess." Therefore, the most important property right is the right to possess and the underlying rationale is the exclusiveness of properties, which determines that there cannot be two subjects of right to one property. Hence, possession is the only way to realize property rights.

The essence of data rights is the right of sharing. Unlike property rights, multiple subjects could be subject to the data rights since data has infinite reproducibility and with zero cost and zero wastage. As such, the right to possess does not affect the control and utilization of data. Even if people don't have the right to possess data, they may still have the right to use, to dispose of and to collect earnings from data. Moreover, in the era of big data, the real value of data lies in its infinite use within a permissible scope. The infinite use of data is also the basis for the development of the big data industry, the big data technology and its application. It determines that sharing is the fundamental requirement for the era of big data and the sharing right is the essential data right. If the exercise of data rights is subject to the right to own, the use of big data will face more constraints. If so, further development and wider application of big data will be out of the question. By doing so, the original intention for using data rights to protect and develop big data will be violated or even ruined.

To be shared or to be possessed, is the fundamental distinction between data rights and property rights. The rationale behind it lies in the fact that when the right to use a property is transferred from A to B, A can still preserve the right to possess and the right to control this property. In this way, the legal interests of the property owner will remain intact. Data rights cannot be preserved the same way. Once the right to use data is transferred from A to B, B acquires complete possession of the data and A loses control of it. There is no sense to protect the right to possess data. To generate and maximize value from data, we have to share data with other people. In this process, the conflict between the right to share and the right to possess will be inevitable. Thus, the right to share is important for data rights, just as the right to possess is for property rights. It is extremely true as we now shift from "exploiting the use of each item of property to a maximum degree" to "making the best use of every piece of data."

Attributes of Data Rights

Data rights, distinguished from traditional types of ownership, are a new type of ownership manifesting the diversity of ownership. Different types of data have different ownership, so does the data at different stages of their life cycle. Data rights are characterized by private right attributes, public power attributes, and sovereign attributes. To be more specific, data rights consist of sovereign rights that embody the dignity of a state, public power that represents the public interest, and data rights that highlight personal well-being. The legal attributes of data rights should be analyzed from the perspective of both private law such as individual rights and public law such as national security.

The private right attributes of data rights

The attributes of a right are determined by the basic content of the right. China lacks a centralized and systematic legal system regarding private rights or rights with the attributes of private rights; instead, it adopts a decentralized one in which different types of private rights are separately prescribed in different legal norms (Ma Rui and Li Jianhua 2014). Data are incorporeal things, and their private right attributes, as a prerequisite, need to be specified first. In the whole private rights system of ancient Rome, the theory of *res incorporales* in the property rights system proposed that our understanding of the object should not be limited to the forms of the existence of things. The intellectual property is recognized by modern laws, indicating that the property rights based on abstract things are finally established. The private right attributes of data rights which are established on the basis of "data persons" are mainly manifested by the data rights holders in defending their data rights. Data rights are a synthesis of personality rights and property rights, and the dual interest attributes of data personality rights and data property rights are endowed with economic value. Therefore, the private right attributes of data rights is specified mainly for the purpose of further demonstrating that the protection mode of personality rights or property rights should be adopted to protect data rights.

A. DATA RIGHTS: A NEW CIVIL RIGHT

Data rights value the independent personality and freedom of conduct of the individuals, which is consistent with the basic value orientation of private rights that individual interests should be protected and freedom of conduct should be enjoyed and realized by the individuals. First of all, data rights feature independent personality rights. Personality rights, as one of the civil rights prescribed in the *General Provisions of the Civil Law*, refer to a civil right enjoyed by the civil subjects in accordance with the law to protect their personal dignity against any violations. Personal data come from natural persons and are endowed with certain personality interests. Any collection, use, processing or transmission of personal data by other persons without the consent of the data subjects not only infringes upon the rights of disposal and decision making of the data subjects but also impairs their personal dignity. Secondly, personal data has property interests. The aggregation of massive data and information can generate considerably valuable information through analyses and researches. When businesses use these information for commercial purposes and the benefits are generated, profit distribution can be a big issue. The interest chain will break if the information subjects in the interest chain do not receive the due rewards. For natural persons, whose information is of commercial value, the right holders, they have the exclusive right to dispose of their personal information.

Specifying the attributes of data rights serves the purpose of fully protecting data. Nowadays, "data are of value" has become a consensus, while the frequent leakage, illegal trading and use of data on a large scale have gradually formed a black industrial chain, making the protection of personal data a top priority for future development. In terms of legislation, China has not yet directly stipulated the personal data rights. The laws and regulations regarding information security seem to have formed a certain scale in quantity, but they are still insufficient to constitute an independent, complete, systematic and well-organized system. The protection of the right to personal information is prescribed in different legal norms such as the *Constitution*, *Criminal Law*, *Criminal Procedure Law*, *Civil Procedural Law*, and *Law of the PRC on the Protection of the Rights and Interests of Consumers*. At the beginning of 2003, the State Council Information Office entrusted the Research Group on Personal Data Protection Law from the Institute of Law of the Chinese

Academy of Social Sciences to work on the project regarding the *Personal Data Protection Law*. In 2005, the recommended draft was completed, but it has not entered substantive procedures. The harassment cases caused by the leakages of personal data are proportional to the development of society, economy and information. The theft, disclosure and illegal use of personal data, ballooning in large quantities, should be regulated by private law. Without the regulation of civil law, the orderly and safe flow of personal network information cannot be guaranteed, and personal data will fail to receive effective protection. Consequently, incorporating personal data into civil rights is of immediate significance to protect the private data of citizens.

The kernel of data rights protection is how to regulate the collection, use, processing and transmission of personal data by controllers and processors of personal data. The *Cybersecurity Law of the People's Republic of China*, effective on June 1, 2017, prescribes the basic legal system regarding the protection of the right to personal information of citizens. The law serves the purpose of safeguarding the personal information security of citizens, preventing theft, disclosure and illegal use of the personal information of citizens and ensuring the orderly and safe flow of the personal network information of citizens in accordance with the law. Article 111 of the *General Provisions of the Civil Law of the People's Republic of China*, which was enacted and promulgated in the same year, prescribes that the personal information of an individual shall be protected by law. On May 25, 2018, the EU General Data Protection Regulation came into effect. Regulation mainly highlights the principle of "Data Rights the Supremacy" and greatly enriches the data rights and protection mechanisms of the data subjects. In addition, the Regulation have imposed strict restrictions on the use of personal data by data controllers and processors, increased the legal liability of data controllers and processors for personal data management, and enhanced penalties for any violations of GDPR (Wang Chunhui 2018).

B. THE PROTECTION OF DATA RIGHTS FROM THE PERSPECTIVE OF CIVIL LAW

Citizens' awakening of civil rights awareness and the continuous discussions of the attributes of data rights contribute to the improvement of the conditions of data rights protection. During that process, more and more functions of data rights are created and incorporated into the private rights system.

One rights object may have multiple values. The protection of data rights as private rights should conform to the times and bear the characteristics of openness. "Reconstructing an open and flexible private rights system" has become a new demand in the era of big data.

The relevant regulations and policies on the protection of personal information promulgated by the US government can trace back to the *Privacy Laws of the United States*. The Act prescribes in detail the collection, use, disclosure, and confidentiality of personal information by the "administrative agencies" for the purpose of regulating the federal government in processing personal information so as to ease the conflict between personal privacy and public interest. In 2012, the United States enacted and promulgated the *Consumer Privacy Act*,[4] requiring operators to protect the personal information of the consumers in accordance with the principles of transparency and purposiveness. Besides, the United States has formulated relevant federal laws regarding the protection of personal information in the areas of finance, communications, education, vehicle management, and medical care. In a word, the so-called privacy rights in American laws are relatively open and constantly enriched, and the so-called privacy refers to an individual's control over of the personal information of his own.

The development of the right to personal information in the EU can be deemed as a process in which the EU constantly adjusts its judicial system to apply the ever-changing data processing technology. The EU, as a large organization that has discretion of data, regards the respect for private life and privacy as a fundamental right. The *Privacy and Electronic Communications Directive 2002* promulgated by the EU prescribes that electronic communications, especially by Internet service providers, have the obligation to

4 On June 28, 2018, the California State Congress passed the *2018 California Consumer Privacy Act*, which took effective on January 1, 2020. It is reported that this is the "most severe and comprehensive" personal data privacy protection act in the United States so far. The act mainly involves two aspects. One is to stipulate that consumers have more control over the collection and management of their personal information; the second is to define a red line for the way companies collect and process data. The act is a milestone in the evolution of US privacy law, both for the US and the European Union. The direct response of GDPR also shows that the United States is more concerned about privacy protection, and legislators will take concrete actions to accelerate personal data governance.

protect the users' information; and individuals shall have the right to be informed and the right to consent, which means that the service providers shall inform the users of their intents of the data processing and the users have the right to refuse or withdraw the consent. In 2016, the EU drafted a new regulation on data protection, the *General Data Protection Regulation*. The *Regulation* has formulated stricter regulatory provisions and imposed more severe penalties for the protection and supervision of personal data, and thus solved the problem of unclear punishments in the *Privacy and Electronic Communications Directive 2002*. The *Regulation* came into effect in May 2018. As German scholars pointed out, the protection of personal information in the EU is characterized by intergeneration. The first-generation law on protection of personal information was formulated to respond to the emergence of electronic data processing within the government and large companies; the second-generation law centered on the personal privacy of citizens; the third-generation law focused on discretion of personal information and ensured the right to be enjoyed by the citizens; the fourth-generation law is currently under way to adjust the weak negotiating position of individuals in the exercise of their rights (Zhang & Han 2016).

Although China lacks uniform regulations on the right to personal information, relevant provisions can be found in civil law. Article 127 of the *General Provisions of the Civil Law* of People's Republic of China prescribes: "Where any laws provide for the protection of data and network virtual property, such laws shall apply." It officially acknowledges data as a legal right and for the first time explicitly incorporates data into the scope of civil rights protection. The relevant declaratory clause[5] (Article 111) provides a more authoritative guarantee for personal data and privacy, making an important step forward in legislation on the protection of personal data in China. The *General Provisions of the Civil Law* of People's Republic of China explicitly protects the right to personal information, which is of immediate

5 Article 111 of the *General Principles of the Civil Law of the People's Republic of China* provides: The personal information of natural persons is protected by law. Any organization or individual who needs to obtain personal information of others shall legally obtain the information and ensure the security of the information, and shall not illegally collect, use, process, or transmit the personal information of others, and may not illegally buy, sell, or disclose the personal information of others.

significance to protect the dignity of citizens, protect citizens from illegal intrusion, and maintain the regular public order. Network operators and other commercial organizations should strictly abide by the law. The right to personal information is a crucial civil right enjoyed by citizens in the Internet age. Any organization or individual shall not illegally collect, use, process, or transmit the personal information of others, nor illegally buy, sell, provide, or publish the personal information of others.

The core of the protection mode of personal data is to find a balance between the full protection of personal data rights and the facilitation of the commercial use of personal data. Firstly, in terms of the static protection of data, we should focus on the foundation of rights and determine that personal data and privacy rights are basic personality rights. Secondly, in the process of data flow, we should, on the basis of justice, distribute the rights and interests fairly and reasonably in the collection, use and sharing of data. In general, the "EU Model" is more inclined to the protection of personal data, while the "American Model" is more in line with the need for free circulation of data. The two models have their own advantages and disadvantages. In the legislation on data rights, China should embrace the advanced practices of various protection modes, pay attention to the connection and coordination with other relevant laws, avoid vertical repetition or horizontal crossover, and eliminate legislative contradictions and conflicts so as to formulate reasonable system design.

The public power attribute of data rights

A. FROM PRIVATE RIGHTS TO PUBLIC POWER

Rights are private in nature. Fundamental law rights, public law rights, private law rights, and social law rights are all established to manifest and protect personal interests, as opposed to public power that embodies and protects public interests. Right are inherently the interests and qualifications of individuals. The "individual" is fundamentally private, and thus the rights are private (Duan Fan, 2016).

The essence of power is public. Whether it is a political power, economic power or social power, its subjects are public institutions and social

organizations, and its object is the public interests protected by law. The power is modified by "public" rather than "private," as President Xi Jinping emphasized: "Public power is for the people, and nothing of it may be used for private purposes" (Duan Fan, 2016).

From the perspective of the social contract theory, Rousseau believes that state power is obtained through transferring "natural rights" of individuals. He holds in his famous book entitled *The Social Contract* that no state power is not premised on the delegation of the powers (rights) and recognition by the public (Xi 2008). As the French enlightenment thinker Locke puts it: "Humans, to make up for the defects of the natural state and defend their own natural rights, signed a contract to voluntarily give up part of their power, and handed it over to someone or some people who agreed to it. A state hence emerged. This is the origin of and reason for legislative and executive powers." The private rights and public power that constitute the life of human society are the unity of opposites.

The mainstream theory holds that public power and private rights are mutually reinforcing. Public power is the backup force and guarantee of private rights, while private rights are the basis and origin of public power (Wang Jianmin 2015). In the process of the exercise of public power, to suppress the abuse of it, the principles must be upheld, including that the administration shall be done in accordance with the law and subject to supervision, that a government official may not act beyond his power delegated, and that statutory obligations of the government must be performed. The ideal state which has a perfect legal system is one in which the public power and private rights are always in balance. As the main symbol of the state, public power is the fundamental premise of all functional administrative activities of the country and bears the following basic characteristics: first, the subject of public power is the public rather than individuals. In other words, commonality is the core connotation of public power, embodying a kind of publicness, sharing and intercommunity. Second, the object of public power is public affairs. The affairs related to private rights should not be interfered with by the public power; otherwise violation of private rights is committed. Third, The source and basis of public power is the public interests. Public power is delegated to the government to assume public responsibilities and serve the public interests; otherwise public power is likely to become privatized or private.

B. DATA RIGHTS HAVE THE PROPERTY OF PUBLIC POWER

Public power is featured with commonality and collectiveness. It can be defined as a kind of collective power with the state and its government as the subject and with the maximization of public interest as the value orientation, aiming at powerfully maintaining the order of participation in public affairs (Tao 2015).

The data rights have the property of public power. First, in terms of the results of data rights, in the virtual network world which is a mirror world of the real world, public power has new carrier space and can be excised in new forms. While enjoying the convenience of the network and technology, the public are unable to get rid of the worries of malicious attacks, the shackles of dark power and the fear of no place to hide in the network world. The high level of integration of virtual cyberspace and the actual physical society has made them independent from each other but meanwhile mutually influential. The result of the exercise of data rights will have impact on the public interests protected by law, so data rights have a property of public power. Second, the protection of data rights needs public power. Data rights protection should be intervened by public power and protected simultaneously by various bodies of law, such as constitutional law, criminal law, administrative law, and civil law. Therefore, to respect the data rights of public and private entities, it is necessary to clarify the procedures of law enforcement of public power subjects so as to ensure the legitimacy of their demand for data.

The idea of data rights was proposed by British Prime Minister David Cameron, who said in a speech: "The new right to data is the most exciting. It will ensure that people have the right to make claims to the government for various kinds of data for the sake of social innovation or business innovation. You will have sufficient information to understand how the government works, how the money is spent, and how effective our work is. Let's hold ourselves to account, making joint efforts to create a model of modern democracy by using and developing the data." Cameron believes that data right is a fundamental right that every citizen of the information age should have. In reality, the government, as the representative of public power, is actually the largest data controller. The introduction of data right is in line with deontology, that is, the practice of citizens making claims to

the government for data rights is a relief, prevention and negative claim, mainly to protect citizens from infringement on their private rights by public power and other large data controllers. Therefore, data rights, as a kind of public power, should be included in the list of legal rights and established as a fundamental right in the constitution.

C. SELF-EXPANSION OF DATA PUBLIC POWER

The core of the rule of law is to regulate public power and protect private rights. Public power itself is inherently mandatory and expansive and therefore should be restricted. Public power is a managerial power over the people. Once out of control, it is likely to cause detriment to the private rights of the people.

In practice, conflicts between public power and private rights occur frequently, such as the abuse of public power directly infringing on private rights, the new types of public goods provided by the government impairing the public's existing interests; government provides new public products that harm the existing interest of the public; the "supply-orientation" of government public services conflicting with the public's needs; the government's omission to act causing detriment to the public interests. The contributing factors include the inertia effect of the traditional idea of strong public power and weak private rights, the neglect of institutional design and the ineffective supervision and accountability.

In the era of big data, the absence of the data rights system and the natural self-expansion of public power lead to the abuse of public power over data, which causes detriment to private rights to varying degrees mainly in the following two aspects: First, public power is used for private purposes. In the era of big data, the flow of data between and among industries and sectors in the cyberspace involves data producers, receivers and users. Data flow involves a number of practical locations, such as the place where the data is sent, received and delivered, the destination, and the place where the service facility is provided. The boundaries of the rights and power of multiple governance subjects are blurring, so public power and private rights show mutual intrusion to a certain extent. Only when the citizens are subject to the control of data public power can they enjoy the freedom to exercise data private rights. However, in reality, data public power is often

used for private purposes, which affects the security of data private rights. Data public power is used for private purposes in two ways: one is the abuse of data public power, violating the procedures and rules of regular use of data and infringing the freedom of citizens to exercise their private rights; the other is the detriment to data private rights of citizens due to power rent-seeking or rent-setting by some platforms. Second, the center of public power shifts. In the physical world, public power is always superior to private rights, so the forceful inherent expansion of public power tends to compress the space of private rights. Such conflicts continue in cyberspace. The development of modern information technology has added weight to the information asymmetry between the government and citizens, and is heavily biased towards the party that is empowered. For example, the technology of personal identification or authentication using the inherent physiological or behavioral characteristics of the human body has made rapid progress in recent years, making the privacy of personal information more and more fragile and difficult to maintain without the protection of the legal system.

The inherent nature of self-expansion of public power makes it more likely to continuously expand its power boundaries, so that public power and private rights intrude on, compete with and counterbalance each other in cyberspace. In addition, since public power stems from private rights and the total number of private rights is fixed, the relationship between private rights and public power is a trade-off, with the two being interconnected and complementary (Ruan 2012). Civil rights are the foundation of state power while state power is the guarantee of civil rights. Rights are not the gifts from the state but the justification for the existence of state power. Consequently, it should be deemed that rights are the source of power, and power emerges to consolidate and defends rights. When data private rights conflict with data public power, public power shall have precedence over private rights. For instance, when the rights protected by the law concerning privacy and disposal principles conflict with national security, government regulation, public security, public interests, judicial procedures, and judicial independence, the latter shall take the priority. Data private rights and data public power should be strictly divided. Only by regulating data public power and preventing its abuse can data private rights be truly protected. However, regulating data public power does not mean weakening its authority. Instead, it refers to regulating the exercise of data public power

through relevant rules and procedures, which will improve the exercise of public power instead of weakening its authority.

The attribute of sovereignty of data rights

A. FROM THE NATIONAL SOVEREIGNTY TO DATA SOVEREIGNTY

The connotation of national sovereignty is increasingly expanding with the progress of society. In accordance with the classical political science theory, national sovereignty means that the state has the supreme power within the territory and has the power to independently decide its development direction and equally participate in international activities (Sun 2016). Sovereignty is the most important and fundamental right of the state. It is inherent to the state rather than being conferred by international law, and is the only power recognized and protected by the principle of national sovereignty. Sovereignty, as an inherent power of the state, is manifested in three aspects: the supreme power within the territory, the power of independence, and the power of self-defense against aggression outside of the territory.

Cyberspace has broadened the boundaries of the state. A "state" is deemed to be the spatial entity with most sovereign property that is capable of exercising jurisdiction within its territory (Sun & Zhang 2015). As history evolves, the concept of sovereignty also updates its connotation and framework in real time. In the 1990s, the Internet boom started. Network globalization made it possible for information to break through traditional territorial boundaries and freely spread across borders. Information has become an emerging productive force. Since the beginning of the twenty-first century, the era of big data has arrived, thanks to the exponential growth model driven by Moore's Law, the digitalization of everything driven by low-cost technology, the large-scale convergence of data driven by cloud computing models, and the extensive "human-machine-object" connection driven by ubiquitous mobile broadband Internet. No matter how advanced big data technology is and how great the globalization of network data is, cyberspace as a "new territory" should not be left alone without the regulation of law.

The idea that "national sovereignty is applicable to cyberspace" has become an international consensus. The United Nations established the

Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security (the UN GGE), successively in the periods between 2004 and 2005, 2009 and 2010, and 2012 and 2013, to "research existing and potential threats in the field of information security and possible cooperation measures against the threats" and reached important consensus on the peaceful use of cyberspace and cyberspace national sovereignty. In 2015, the UN GGE released a research report again, reaffirming and enriching the content of cyberspace national sovereignty. In 2012, the OECD conducted a systematic study on the cyber security strategies of 10 countries including the United States, the United Kingdom, Australia, Canada, Japan, the Netherlands, France and Germany. It was found that the network security policies of most countries gradually embodied a so-called "sovereignty consideration." *National Security Law of the People's Republic of China* adopted in 2015 provides for the cyberspace sovereignty for the first time. On November 7, 2016, China promulgated *the Cybersecurity Law of the PRC* mainly for the purpose of maintaining cyberspace sovereignty. In the *National Cyberspace Security Strategy* and *The International Strategy of Cooperation on Cyberspace* promulgated afterwards, "respecting and maintaining cyberspace sovereignty" is the overarching principle of cyber security, providing a fundamental guidance for China in dealing with domestic and international network affairs (Zhu 2017).

Data sovereignty is the extension and expansion of cyberspace sovereignty. As an important element of cyberspace, data has become a national basic strategic resource, which is as important as natural resources, information resources and intellectual resources. The existing information sovereignty has been unable to adapt to massive data dissemination and use in the network space under the national control and the impact thereof. Data sovereignty therefore is established, which refers to the ownership, right of control, jurisdiction and right of use of the state's domestic data and the cross-border data owned by the nationals in the context of big data and cloud computing. Data sovereignty is embodied in the highest control over data within the territory and equal and independent data processing rights outside of the territory (Sun 2016). Data is closely related to the survival of the state and is an integral part of the state. It is a requisite for the formation of the state. The state's exercise of sovereignty over the data owned by it manifests the independence and autonomy of the state.

B. NATURE OF DATA SOVEREIGNTY

Data sovereignty is an important component of national sovereignty. The basic element of cyberspace – the free flow of data – makes global data resource sharing possible. It facilitates human production and life, but at the meantime, may also pose great challenges to sovereign states in safeguarding national sovereignty. With the integration of the virtual network world and the real world, the control and use of digital resources will have an enormous impact on the national economy, politics, culture, etc. As a necessary supplement to national sovereignty, data sovereignty enriches and develops the connotation and denotation of traditional national sovereignty. It is an inevitable choice to adapt national sovereignty to modern virtual space governance and to safeguard national sovereignty.

The purpose of data sovereignty is to address security issues of large-scale data sets. Data, as a basic element used to record the real physical world in cyberspace, contains huge amount of valuable information. Some network incidents and cybercrimes that endanger national interests are actually organized and planned in both virtual network space and real physical space. Internet technology is used for the sake of convenience in collecting and appropriating data, causing severe damage to the state and putting it at a disadvantage. Attaching high importance to data ownership and jurisdiction is an inevitable requirement for solving security problems of large-scale data sets, and is of great significance for combating data terrorism and cross-border data crimes.

Data sovereignty is practiced on the basis of the change of human activity space. Virtual network space is a new field of human activity space. Compared with the physical boundary of the physical world and the tangible nature of material resources, virtual network space and data resources are open, free and intangible. The *status quo* of excessive freedom and lack of order in virtual cyberspace requires regulation of sovereignty. Claim to data sovereignty is fundamentally equivalent to the claim to national sovereignty in international economic affairs. The subject of the data activity in the virtual cyberspace and the value of the data are objectively present, and the value of the data can be realized only through data use, transaction, etc., which are also traceable. The results of data use and transactions, etc., will reflect or affect national sovereignty, and each sovereign state has a practical basis

and realistic needs for sovereignty over the aforementioned subjects and interests. The claim to national sovereignty over virtual cyberspace is rooted in the fact that cyberspace is an integral part of today's human society and national affairs. Cyberspace sovereignty is the mapping of sovereignty on the Internet. Data sovereignty is the embodiment of sovereignty in data. Data sovereignty is an important part of cyberspace sovereignty (Li 2018).

c. The protection of data sovereignty

The protection of data sovereignty should be functionally oriented towards maintaining overall national security. The seamless global network connection brings unprecedented challenges to the countries which used to have clear and relatively closed borders and the national security thereof. From a global perspective, due to the disorderly and anarchic state of cyberspace governance, the absence of physical boundaries and the cross-border nature, a bit of breakthrough towards risk and threat of cyberspace will lead to rapid spread on the whole Internet. For example, the "Prism Gate" incident reveals that the United States exercises cyber hegemonic power to illegally steal and monitor global data, and carries out cyberattacks against other sovereign countries, seriously damaging the sovereignty of other countries. With data resources becoming increasingly important, the global competition focus is shifting from the competition of physical resources to the control of data resources. Compared with the security of traditional territories and territorial seas, data sovereignty concerns the emerging security types without boundaries in a more complex virtual space. With data being the basic element of virtual space, it is necessary to develop an institutional system of national data sovereignty for the sake of national sovereignty to safeguard the overall national security against new challenges and risks.

The free and disorderly data flow in cyberspace breaks the traditional concept of absolute sovereignty. The indivisibility of data as a whole makes the flow of data across borders in virtual network space involve a wide range, leading to overlapping of multiple jurisdictions and even conflicts of data sovereignty. At the same time, because the data protection regulations between countries are not the same, network service providers can seek to evade obligations under multiple jurisdictions, which adversely affects the data security of other countries. Different from the traditional approach of

sovereignty protection, data sovereignty protection may as well shift from absolute competition to international cooperation to some extent.

Data sovereignty protection should shift from adopting traditional absolute sovereignty theory to relative sovereignty theory. Under the background of the rapid development of digital technology, the cross-border data flow has become much more common and convenient. This flat and multi-centered network space has gradually awakened the awareness of social rights and undermined the control of data sovereign countries over their own data. Small countries lack the capability of ensuring the security of their data on their own, let alone establishing absolute data sovereignty, while powerful countries can effectively exercise data sovereignty with the help of advanced science and technology, and even endanger other countries' data sovereign security (Sun & Zhang 2015). In order to solve the multi-control conflicts and the predicament of national data security due to the absolute independence of data sovereignty, presently, it is more reasonable to establish a global cyberspace governance system under the UN framework with the principle of "relative sovereignty" in the current data field. Under the theory of relative sovereignty, the rule-of-law thinking plays an important role in the realization of "relative sovereignty." Domestically, the rule of law prohibits the "absolute authority" of sovereignty from overriding the whole nation; internationally, the consensus of "legal governance" and the international cooperation practice have compelled the states to give up part of their sovereignty through bilateral or multilateral treaties. In turn, the rule of law, as an effective governance model of a state and the world, can lodge "sovereignty" from the political sphere onto the regulation of law (Xiao 2017).

Data sovereignty should be exercised and data security protected under the legal framework. An authority system of data management should be internally established, which is the highest management authority for cross-border transmission, and collection, transmission, storage, processing, utilization, and transaction of data within the jurisdiction of the state. Efforts should be made, on the basis of the Network Security Law, to establish relevant legal systems so as to perfect the prohibition rules regarding the data endangering overall national security and human life safety, including the data concerning national defense, confidential information of political parties, human genes. The control over the actions, such as collection, storage,

processing, and use of data, comply with relevant national technical standards or other legal provisions. Internationally, an authority system of data control should be established. The right to data control means that sovereign state has the right to take protective measures against the national data to keep it from being monitored, tampered, forged, damaged, stolen, leaked, etc., and to ensure the security, authenticity, integrity and confidentiality of data.

Bibliography

Diamandis, Peter, and Stephen Kotler. 2014, *Abundance: The Future is Better Than You Think*. Hangzhou: Zhejiang People's Publishing House.

Duan Fan. 2016. *Power and Rights: Co-location and Construction*. Beijing: People's Publishing House.

The General Provisions of the Civil Law of the People's Republic of China.

He Zhe. 2017. "The Construction of Human Social Form and Order in the Era of Network Civilization." *Nanjing Journal of Social Sciences*, vol. 4.

Hu Weiping. 2011. "Legislative Confirmation of a New Personality Right." *Law Forum*, vol. 26.

Li Aijun. 2018. "Data Rights Attributes and Legal Characteristics." *Oriental Law*, vol. 3.

Li Xiaohui. 2013. "Information Property Rights: Extension and Supplement of Intellectual Property." *Electronic Intellectual Property*, vol. 11.

Ma Rui, and Li Jianhua. 2014. "Private Law Logic of the Concept of Private Rights." *Henan Social Sciences*, vol. 22.

Mei Xiaying. 2016. "The Legal Nature and Civil Law Position of Data." *China Social Sciences*, vol. 9.

Miao Wei. 2015. "Big Data: A Key Resource for Transforming the World." *People's Daily*, vol. 10–13.

Ruan Chuansheng. 2012. "The boundary between Public Power and Private Rights." *Learning Times*, vol. 11–12.

Sun Nanxiang, and Zhang Xiaojun. 2015. "On Data Sovereignty: Based on Virtual Space Game and Cooperation." *Pacific Journal*.

Sun Wei. 2016. "Correctly Distinguishing between Network Sovereignty and Data Sovereignty." *Chinese Journal of Social Sciences*, 5, July 2016.

The Supreme People's Court. 2014. *Provisions of the Supreme People's Court on Several Issues concerning the Application of Law in the Trial of Cases involving Civil Disputes over Infringements upon Personal Rights and Interests through Information Networks* [EB/OL]. (October 21), <http://www.court.gov.cn>.

Tao Peng. 2015. "The Conflict and Adjustment of Public Power and Private Rights in Virtual Social Governance." *Gansu Theory Journal*, vol. 3.

Wang Chunhui. 2018. "Comparison of GDPR Personal Data Rights and Personal Information Rights under the Cyber Security Law [EB/OL]." (August 11). <http://www.cbdio.com>.

Wang Jianmin. 2015. "Dialectical View of Public Power and Private Rights [EB/OL]." (April 7). <http://www.qstheory.cn>.

Wang Liming. 2012. "On the Status of Personal Information Right in the Law of Personality Rights." *Journal of Soochow University (Philosophy and Social Sciences Edition)*. 33.

Wang Liming. 2013. "On the Commercialization of Personality Rights." *Legal Science* (*Journal of Northwest University of Political Science and Law*), vol. 31.

Wang Liming. 2015. "My Complex and Ponderation of Personality Rights[N]." *Guangming Daily*, vol. 12–14.

Wu Tao. 2016/2018. "The Four Mainstream Views on 'Data Rights and Ownership' in the Legal Academia" [EB/OL]. October 24, 2016 and May 20, 2018, <http://www.aliresearch.com>.

Xi Xiaojuan. 2008. "On the Conflict and Coordination between Property Rights and Taxation Rights: From the Perspective of Legal Analysis of the Nature of Rights (Powers)," *Hebei Law*, vol. 12.

Xiao Dongmei, and Wen Yuheng. 2017. "Defending the Sovereign Security of National Data in the Global Data Torrent." *Hong Qi Wen Gao*, vol. 9.

Yu Zhigang. 2017. "The Rights Attribute of 'Personal Information' and the Idea of Criminal Law Protection." *Zhejiang Social Sciences*, vol. 10.

Zheng Chengsi, and Zhu Xiequn. 2006, "Information and Intellectual Property," *Journal of Southwest University of Science and Technology* (*Philosophy and Social Sciences Edition*).

Zhang Li'an, and Han Xuzhi. 2016, "Private Law Attribute of Personal Information Right under the Era of Big Data." *Law Forum*, vol. 31.

Zheng Yubo. 1988. *General Principles of Civil Law*. Taipei: Sanmin Bookstore.

Zhu Yanxin. 2017. "Network Sovereignty Issue under the International Law." *Journal of Xi'an Political College*, vol. 30.