On the Constitutional Normative Logic of Data Rights Protection

ZHENG Xianjun[*]

Abstract: *Data rights refer to the ownership and the right of disposing of individuals over their own data and information. The subject is a natural person, and it is a constitutional fundamental right. Long before the European Union's General Data Protection Regulation (GDPR) was enacted, the constitutions of some states had stipulated the right to personal data and the principle of consent. Current research takes constitutional delegation and institutional guarantees as the constitutional normative basis for data rights so that data rights are only objective norms and national protection obligations. This view eliminates the defensive nature of a fundamental right against infringement by public power, ignores the public law protection of data rights, and confuses the difference between data rights and digital rights. The ethical nature of data rights is individual self-determination rather than the cyber democracy of digital rights. As a fundamental right, data rights are subject to the principle of legal reservation. Restrictions on data rights shall be limited and the principle of proportionality protects the essence of data rights from infringement by the legislature. Individual dignity is the basis for judging whether the core of data rights is violated. It is necessary to eliminate the theoretical blind spot that data rights are merely private law rights and to overcome the "Idols of the Marketplace" and "Idols of the Theater" created by objective norms.*

Keywords: fundamental rights ♦ right to defense ♦ objective norms ♦ data rights ♦ principle of proportionality

Introduction to the Issue

"Data rights are the rights of data subjects and are a fundamental right of

[*] ZHENG Xianjun (郑贤君), Professor and Ph.D. Supervisor at the School of Political Science and Law, Capital Normal University. His research interests include constitutional theory, fundamental rights, intra-party regulations, the Basic Law of Hong Kong, and constitutional review. This paper is a phased result of the National Social Science Fund Key Project "Research on the Localization and Systematization of Standards for Constitutional Review" (Project Approval Number 19AFX005).

natural persons."[1] Data includes personal information, materials, and files, and data rights refer to the ownership and disposal rights individuals have over their own data. Both China's laws and the EU *General Data Protection Regulation* (hereinafter referred to as GDPR) have made provisions for the nature of data rights, indicating that data rights have constitutional attributes. Without this basic understanding, any discussion on data rights will deviate from common sense and may go astray, affecting the comprehensive protection of data rights, including protection by public and private laws.

Constitutional normative logic refers to the constitutional normative basis, attributes, scope, and protection measures for data rights. At present, there are certain biases in the domestic academic community's definition of the concept, nature, and connotations of data rights. These biases primarily focus on the following five aspects. First, in defining the attributes of data rights, some studies only identify data rights as private law rights or civil rights,[2] and not as constitutional rights, public law rights, or fundamental rights. Second, in terms of the identification of data rights holders, some studies believe that data rights holders include not only natural persons but also legal persons, data controllers, and data processors.[3] This is incorrect. Third, in identifying the value attributes of data rights, some studies are keen on arguing whether data rights are personal rights, property rights, or privacy rights,[4] ignoring the characteristics of data

[1] Article 1(3) of Chapter 1 of the GDPR stipulates that "The free movement of personal data within the Union shall be neither restricted nor prohibited for reasons connected with the protection of natural persons with regard to the processing of personal data." Article 2 of China's Personal Information Protection Law stipulates that "The personal information of natural persons shall be protected by law. No organization or individual may infringe upon natural persons' rights and interests on their personal information." Article 3 stipulates that "This Law shall apply to the processing of personal information of natural persons within the territory of the People's Republic of China."

[2] Cheng Xiao, "Personal Data Rights in the Big Data Era," website of China Sociology, accessed November 29, 2022, http://ltirue.edu.cn/sy/xwdt/d3ab5a8ae08e4f58937511df7398fbc8.htm.

[3] He Yuan, *Data Law* (Beijing: Peking University Press, 2021), 50-51.

[4] Ding Xiaodong, "What Are Data Rights? — On the Protection of Data Privacy From the Perspective of the EU's GDPR," *Journal of East China University of Political Science and Law* 4 (2018): 39-53. Some scholars believe that digital rights are the fourth generation of human rights. Yang Xueke, "The Fourth Generation of Human Rights Theory: Outline of Digital Rights in the Digital Age," *Journal of Shandong University of Science and Technology (Social Sciences Edition)* 2 (2022): 10-22. For example, some scholars directly equate data rights with digital rights. Ding Xiaodong, "On the New Rights Characteristics of 'Digital Human Rights'," *Science of Law (Journal of Northwest University of Political Science and Law)* 6 (2022): 52-66. Liu Zhiqiang, "On the Fact That 'Digital Human Rights' Do Not Constitute the Fourth Generation of Human Rights," *Chinese Journal of Law* 1 (2021): 20-34. Li Quntao: "A Literature Review on the Legal Attributes and Ownership of Data," dataprotection.cn, Source: Internet Rule of Law Research, accessed November 29, 2022, http://www.dataprotection.cn/news/34.html. Zheng Xianjun, "Conceptual Analysis

rights as composite constitutional value attributes. In other words, data rights integrate personal, spiritual, and property rights. For example, the right to correction has personal attributes, the right to be forgotten embodies personal values, and the right to portability has property qualities.[5] Fourth, some studies have largely confused the differences between data rights and digital rights, equating the two.[6] Fifth, some studies ignore the normative basis of data rights in China's Constitution, which is manifested in taking a single constitutional norm as the constitutional basis for data rights, or misinterpreting constitutional provisions,[7] or taking foreign data laws as the legal basis. All of the above, in general, lack the analytical dimension or perspective of constitutional relations (legal relations), [8] which is not conducive to China's promotion of comprehensive protection of data rights. The Constitution guarantees data rights as fundamental rights, which we can only comprehend through the general principles of fundamental rights. On the occasion of national institutional reform and the establishment of the National Data Administration, it is necessary to base ourselves on China's Constitution and legal norms, apply the principles of fundamental rights, draw on the results of comparative law, and explore the constitutional normative logic of data rights protection from the perspective of constitutional relations.

I. Constitutional Rights, Not Just Private Law Rights

Although the terms "constitutional rights" and "fundamental rights" are different, the term "fundamental rights" not only indicates the constitutional nature of data rights but also indicates the constitutional status of this right in a country, indicating that although data rights may not be stipulated or granted by the Constitution, they must be protected by the Constitution.

Data rights are both a natural constitutional right and a self-evident fundamental right. First, data rights are subject to personal self-determination and are a fundamental right of human beings. Being human means that each

of Data Rights and Digital Rights," *The Democracy and Law Times*, December 16, 2022.

[5] Zheng Xianjun, "Is the Right to Be Forgotten a Constitutional Right?" *Journal of Capital Normal University* 2 (2022): 178-188.

[6] Ding Xiaodong, "Rethinking China's Personal Information Protection Law from the Comparative Law Perspective: China's Path and Interpretation Principles," *Journal of East China University of Political Science and Law* 2 (2022): 73-86.

[7] For example, using "social security clauses" as the basis for regulating data rights. See Zhou Weidong, "The Constitutional Systematization of Personal Data Rights," *Law Science* 1 (2023): 32-48.

[8] In 2023, at a seminar in Shandong, Professor Ding Xiaodong proposed a public-private law protection model for personal information and data rights, and reviewed the shortcomings of private law protection, namely, infringement law protection. See Law School of Shandong University, "Professor Ding Xiaodong Teaches the Public-Private Law Integration Characteristics and Legal Significance of Personal Information Protection," accessed on November 29, 2022, https://law.sdu.edu.cn/info/1050/11807.htm.

person is born with qualities that are different from others. Data, such as date of birth, parents, genes, blood type, and even gender, appearance, and preferences, express these qualities. Second, many constitutions around the world have long stipulated data rights as personal data and privacy. Third, data rights are implied in many constitutional provisions in China. For instance, human rights, personal rights, property rights, personal dignity, residence, freedom of communication, and confidentiality of communications. As early as 1993, Article 24 (1) of the *Constitution* of the Russian Federation stipulated that "Material about a person's private life shall not be collected, stored, used or disseminated without his or her consent." This constitution not only stipulates the right to personal data but also defines the principle for protecting this right, namely the principle of consent. This shows that the right to personal data has long been recognized by the *Constitution*, and it is an indisputable constitutional fact that it is a fundamental right of individuals. The same is true for the *Charter of Fundamental Rights of the European Union*, which was drafted in 2000 and 2007 as part of the *Lisbon Treaty*. Article 8 of the *Charter* stipulates that the protection of personal data is the protection of personal information and clearly stipulates the right to erasure (right to be forgotten) and the principle of consent. The first paragraph of this article stipulates that "Everyone has the right to the protection of personal data concerning him or her." And the second paragraph stipulates that "Such data must be processed fairly for specified purposes and on the basis of the consent of the person concerned or some other legitimate basis laid down by law. Everyone has the right of access to data that has been collected concerning him or her and the right to have it rectified." Article 1(2) of the GDPR promulgated in 2018 stipulates that "This Regulation protects fundamental rights and freedoms of natural persons and in particular their right to the protection of personal data." Some scholars believe that "the GDPR stipulated in the Constitution elevates data rights to fundamental rights, which stems from the Constitution's legal principle of protecting the personal dignity of citizens, and sets high standards for personal data security, information and privacy protection."[9] This is true. As a modernized version of the data protection law in the 21st century,[10] GDPR simply unifies the data protection standards of European countries and is the strictest personal data protection rule in the history of the European Union. This shows that data rights protection cannot be carried out independently of the constitution, although current research on data rights is mostly found in departmental laws, especially in the field of private law.

[9] Ding Xiaodong, "Rethinking China's Personal Information Protection Law from the Comparative Law Perspective: China's Path and Interpretation Principles," *Journal of East China University of Political Science and Law* 2 (2022): 75.

[10] IT Government Privacy Group, *EU General Data Protection: GDPR's Compliance Practice*, translated by Liu Hexiang (Beijing: Tsinghua University Press, 2021), 191.

In China, there has been discussion about whether data rights are a fundamental right or a constitutional right, but the relevant theories are still unclear. For example, some people only take constitutional delegation, institutional guarantee, and social security theories as the basis for constitutional norms or believe that data rights are merely personal rights or property rights. While existing research has started advocating for public law protection of data rights, related discussions are still in their infancy, with no consensus or conclusion on the relevant concepts, nature, and connotations.[11] What is certain is that data rights are not a concept explicitly stated in China's Constitution but are implicit in the corresponding constitutional norms. At the same time, data rights are a fundamental right. It is not just about whether the right is an explicit constitutional right or an unlisted implied constitutional right. Instead, the focus should be on the constitutional relations. By exploring the legal relationship between the state and the individual in a vertical sense, it reveals that data rights must be used as a right to defense to resist infringement by public power and must also be used through objective normative analysis to prevent infringement between individuals in a horizontal sense, thereby achieving dual protection of data rights, namely public law protection and private law protection.

The GDPR calls data right the "right of the data subject" or the "right to the protection of personal data," which refers to the rights enjoyed by the data subject regarding his or her personal data. The National Committee for the Examination of Scientific and Technological Terminology approved and released this concept as a new big data term in China in July 2020. On July 25, 2022, the Supreme People's Court issued the *Opinions of the Supreme People's Court on Providing Judicial Services and Guarantees for Accelerating the Construction of a National Unified Market* (hereinafter referred to as the "*Opinions*"). The *Opinions* clearly put forward the concept of "data rights" and points out that the legitimate rights and interests of data rights holders in data control, processing, and income must be protected in accordance with the law. On December 19, 2022, the Central Committee of the Communist Party of China and the State Council issued the *Opinions of the Central Committee of the Communist Party of China and the State Council on Building a Data Infrastructure System to Better Play the Role of Data Elements*. In addition to the implicit constitutional norms, the *Data Security Law*, the *Cybersecurity Law* and the *Personal Information Protection Law* provide a normative basis for data rights. Article 7 of the *Data Security Law* promulgated in 2021 stipulates that "The state shall protect the data-related rights and interests of individuals and organizations, encourage the lawful, reasonable, and effective use of data, ensure the free flow of data in an orderly manner and in accordance with the

[11] Dai Jitao, "The Right to Protection of Personal Data as a Constitutional Right," *Human Rights* 5 (2021): 110-130.

law, and promote the development of a digital economy with data as the key factor." Chapter 4: "Network Information Security" of the *Cybersecurity Law* stipulates the protection of personal information, namely data.[12] In reality, the concepts of data rights and personal information rights are identical. The difference lies in the fact that data is objective, whereas personal information is specific and identifiable. Data associated with a specific personal identity constitutes personal information. For example, blood type is data, which becomes personal information when it is linked to a specific individual. This explains why the information protection principles outlined in the *Personal Information Protection Law* also apply to data rights. As far as theoretical research is concerned, as early as 2018, Chinese scholars put forward the concept of data rights,[13] and other scholars have successively published papers on data rights. These studies have initially formed the basic theoretical framework of data rights. By reviewing the normative attributes of data rights, we can draw the following conclusion: Data rights are a basic constitutional right and a fundamental right of natural persons. At present, some scholars believe that "data rights are generally considered to be the property rights of data controllers to possess, process and dispose of data… The subject of data rights is the data controller, not limited to natural persons; the object of data rights must exclude personal information and can only be electronic data that cannot identify specific individuals; the nature of data rights is property rights rather than personality rights; the content of data rights is reflected in the power of possession, use, making income, and disposal of property rights and does not have the power of the right to know, the right to correction, the right to deletion, the right to blockage, etc. of personal information rights."[14] This definition is inaccurate in almost every respect.

First, it is inappropriate to clearly separate data rights from personal information rights and exclude data rights that include the right to know, the right to correction, and the right to deletion. Both the GDPR and China's relevant data laws recognize that data rights and personal information are roughly the same, and both include the right to correction and the right to deletion. For example, Kai-Fu Lee, a famous AI expert, translates GDPR as ″

[12] Article 40 of the *Cybersecurity Law* stipulates that "Network operators shall strictly maintain the confidentiality of any user information collected, and establish a comprehensive system for protecting user information." Article 41 stipulates that "Network operators who collect and use personal information shall abide by the principles of legality, propriety, and necessity; they shall disclose the rules for collecting and using such information, explicitly stating the purposes, means, and scope for collecting or using information, and obtain the consent of the users whose data is being collected."

[13] Cheng Xiao, "Personal Data Rights in the Big Data Era," website of China Sociology, accessed November 29, 2022, http://ltirue.edu.cn/sy/xwdt/d3ab5a8ae08e4f58937511df7398fbc8.htm..

[14] He Yuan, *Data Law* (Beijing: Peking University Press, 2021), 50-51.

一般资料保护规则〞in Chinese and calls it the strictest regulation for protecting personal privacy. He said that "The GDPR is a new set of rules to protect personal privacy and data, designed to help people take back control of their personal data."[15] This shows that "data" is nothing more than personal data, information, and files.

Second, it is incorrect to think that the subject of data rights is the data controller. This view holds that "any subject that possesses and uses other people's information and data is the subject of data rights."[16] Both the GDPR and relevant laws of China recognize that the subject of data rights is a natural person. Data "controllers" and "processors" are "organizations" and "institutions" that accept data and information provided by data subjects. They are subject to regulation by data laws. The use, processing, collection, dissemination, and management of data must comply with regulations and not infringe on the rights of data subjects. The purpose of data legislation is to protect the data, information, and privacy security of natural persons and to balance the relationship between personal data security and public use, namely the free flow of information. Article 1(3) of Chapter 1 of the GDPR stipulates that "This Regulation lays down rules relating to the protection of natural persons with regard to the processing of personal data and rules relating to the free movement of personal data." On the one hand, personal data is personal information and must be protected from infringement by public power and others without reasonable grounds. On the other hand, personal data can be disclosed for the public interest, such as public health, judicial trials, archives protection, historical research, etc., and the state must regulate and protect it. Therefore, it is necessary to strike a balance between preventing infringement, public use, and free movement. Defining the subject of data rights as data "controllers" or "processors" violates the purpose of these rights as a fundamental right and is inconsistent with the basic understanding that the subject of data rights is a natural person.

Third, it is incorrect to assume that the object of data rights must not include personal information but rather can only encompass electronic data belonging to unidentifiable individuals. This is the result of treating data only as an object of property rights protection. It is also a misunderstanding of data legislation. The original intention of data legislation is to protect the security of personal information and to ensure its free use by the public. If personal information is not included in data rights, the relevant legislation will lose its meaning, and data rights will merely become property rights, losing their characteristics of personal rights and privacy rights. Furthermore, it is wrong to think that data rights refer only to electronic data. Both the GDPR and Chinese law recognize

[15] Kai-Fu Lee and Chen Qiufan, *AI 2041: Ten Visions for Our Future* (Taipei: Global Views Commonwealth Publishing Co., Ltd. 2021), 438.
[16] He Yuan, *Data Law*, 50-51.

that the object of data rights can be automatically processed electronic data, non-automatically processed data stored in archives, or semi-automatically processed data, and must be specific personal information. This is also why the GDPR is an upgraded version of the *Data Protection Directive* of 1995, as the GDPR is not limited to regulating electronic data. The Preamble of the *European Declaration on Digital Rights and Principles* of 2022 stipulates that "taking necessary measures to ensure that the values of the EU and the rights of individuals as recognized by EU law are respected online as well as offline." This is exactly the intention.

Fourth, the notion that data rights are property rights rather than personal rights is incomplete. Data rights are rights with complex value. They have both personal attributes and property value. They are also the carriers of personal dignity and privacy and contain the quality of pursuing happiness. In fact, legal provisions in the GDPR and China's *Personal Information Protection Law* can put an end to these debates. The right to correction and the right to be forgotten are manifestations of personality, dignity, and privacy, while the right to portability has the attributes of property rights. Personal data shall not be disclosed but can be sold and transferred to obtain economic value and economic benefits. This is also the basis for the Supreme People's Court to clarify "data property rights"[17] and the basic meaning of the norms. Whether insisting that data rights are property rights or merely considering data rights as personal rights, the drawbacks of the norms themselves are more or less ignored. In short, if the legal norms themselves are carefully studied, the dispute over data rights, personality rights, and property rights can be settled. This once again confirms what US constitutional scholar Akhil Amar said: "Is it even possible to deduce the spirit of a law without looking at its letter"?[18]

Fifth, data rights have dual attributes. These rights encompass both constitutional and private law aspects. According to the principle of fundamental rights, individual rights may be violated from two aspects: one is the state or public power, and the other is individuals.[19] The former is a constitutional right, which refers to the infringement of personal data rights by the state or public power without reasonable basis; the latter is a private law

[17] The Opinions point out that "It is necessary to protect the legitimate rights and interests of data rights holders in data control, processing, and income, as well as the property rights of data products developed by data factor market entities based on legally collected and self-generated data. It is necessary to properly adjudicate all types of cases arising from data transactions, unfair competition in the data market, etc., to provide judicial guarantees for cultivating a data factor market that is data-driven, interdisciplinary, co-created and shared, and fairly competitive."

[18] "It is even possible to deduce the spirit of a law without looking at its letter"? Akhil Reed Amar, *The Bill of Right* (New Haven: Yale University Press, 1998), 296.

[19] Volker Epping, Sebastian Lenz and Philipp Leydecker, *Fundamental Rights*, translated by Zhang Dongyang (Beijing: Peking University Press, 2023), 59.

right, which refers to the infringement of personal data rights by equal subjects. Some scholars believe that "from the perspective that the essence of personal information rights is to protect natural persons and their personal interests, the obligations of the subject of personal information rights processing, and the provisions on personal information protection in the Civil Code, Cheng Xiao believes that personal information rights should be civil rights."[20]

The nature of data law determines the dual attributes of data rights. The *Data Security Law*, *Cybersecurity Law* and *Personal Information Protection Law* are not just private laws or special laws of civil law,[21] but comprehensive laws that regulate both public law relations and private law relations. Together with the *Constitution*, they build a normative framework that protects personal data from infringement by public power. The digital and intelligent era has intensified the complexity of the legal relationship of data rights. The internet makes it possible for personal data rights to be violated by multiple entities. In addition to individuals, controllers and processors of network platforms, companies, various public power organizations, and the state may infringe on personal data. Data rights must not only resist private infringement, but also resist abuse and infringement by data controllers, processors, legal persons, public institutions, and governments. Data rights are not only against natural persons and legal persons who are equal subjects but also include entities, organizations, and state organs with public power. Therefore, data rights are not only a civil right and a private law right but also a constitutional right and a public law right. Data rights require not only protection by private law but also that by public law, especially by the Constitution.

Data rights, as a fundamental constitutional right of individuals, serve several functions in regulating public power. First, the defensive function, resisting the illegal infringement of personal data rights by public power. This function requires that public authorities shall not collect, use, disseminate, disclose, publish, or excessively collect personal data without legitimate reasons. When state organs process personal information, they must have the necessary legal basis and authorization and must follow legal procedures and be within the scope prescribed by law. These constitute the boundaries of state

[20] Zhang Chen, "People's Courts Say No to Excessive Collection of Personal Information, Tailor-made Judicial Interpretations to Regulate the Trial of Face Recognition Cases," Tencent, accessed November 29, 2022, https://new.qq.com/rain/a/20221117A01U5500.

[21] Chen Feng, "Comparison between the Personal Information Protection Law and the GDPR: Analysis of Article 1, Article by Article," Sohu.com, accessed November 29, 2022, http://new.sohu.com/a/518763570 120677543. China's Personal Information Protection Law is a comprehensive law in the field of personal information protection. It regulates both private law subjects and public law subjects' behaviors of personal information processing. In the field of public law regulation, it also includes the regulation of personal information processing activities for the purpose of stopping criminal offenses and maintaining public security. Its coverage of regulation is greater than GDPR.

power and are constitutional protections for data rights. Second, the benefit function refers to the state's legal protection of personal data rights, such as the right to review and the right to correction, through legislation. The state needs to improve data rights laws. Third, the right to request function. When personal data rights are violated, you have the right to require the state to take certain measures and means to remedy the situation. The state must open channels for complaints and reconsideration to discipline, punish, and compensate for violations of other people's data and remedy violated data rights. Fourth, the functions of organization and procedural guarantee. The state needs to improve the organization and procedures of data rights through legislation, establish corresponding institutions such as the "Data Security Bureau" and "Cybersecurity Agency," and have specialized courts accept data disputes. Fifth, the function of institutional guarantees. The state should be required to establish a data infrastructure system, strengthen data legislation, and improve the data rights protection system. It is generally believed that the first three are the functions of fundamental rights as subjective rights, and the last two are the requirements of fundamental rights as objective values for departmental laws. In addition, the state's obligation protect, to prohibit private infringement of data rights, originates from the objective legal attributes of fundamental rights.

As a constitutional right, data rights are also objective norms and principles. Their value must be permeated into life relationships through ordinary laws to prevent mutual infringement between equal subjects. Therefore, the protection of data rights by public law or private law alone is insufficient. Providing dual protection for data rights is the legal quality and connotation that data rights should have.

II. The Dual Attributes of Data Rights

Objective norms mean that fundamental rights, as objective values,[22] must be implemented by lower-level laws. Data rights are a value that constrains all branches of law. Ordinary laws must implement this supreme legal value, improve the comprehensive protection of data rights through private law and other laws, and implement the state's protection obligations. The German Federal Constitutional Court believes that "fundamental rights form an 'objective value order,' and therefore require the state to effectively implement this value order in all areas of life. This is the doctrinal basis of the state's obligation to protect."[23] Individuals, organizations, institutions, enterprises, and

[22] Zheng Xianjun, "fundamental rights as an Objective Value Order: The Obligation to Protect fundamental rights from the Perspective of German Law," *Science of Law (Journal of Northwest University of Political Science and Law)* 2 (2006): 35-45; Yang Dengjie, "Constitutional Rights as Values-A Clarification and Defense of the Doctrine of an Objective Order of Values," *The Jurist* 3 (2024): 30-45 and 191.

[23] Volker Epping, Sebastian Lenz and Philipp Leydecker, *Fundamental Rights*, translated by Zhang Dongyang (Beijing: Peking University Press, 2023), 60.

public institutions must abide by the value of data rights and must not infringe on personal data rights. The *Civil Code*, *Personal Information Protection Law*, *Data Security Law*, *Cybersecurity Law*, etc. stipulate that individuals, institutions, internet platforms, and data processors must respect personal data rights. These laws jointly provide comprehensive legal protection for personal data.

Fundamental rights and objective norms are different. Fundamental rights are the demands of individuals on the state and are also the subjective rights of individuals against the state. In countries that practice constitutional litigation, fundamental rights are also the ones that individuals can claim from the state. Objective norms are a constitutional principle. They are the requirements of the highest-level constitution for the country's overall legal order. They enable constitutional values to radiate to ordinary laws through legislation, forming a unified "body of meaning." Although objective norms are a concept in German constitutional law, China's constitutional tradition also recognizes that the constitution is the highest law, and its principle attributes give the constitutional principles at the top of the pyramid a radiating effect on lower laws. Research currently in existence suffers from two shortcomings: firstly, it fails to provide a comprehensive constitutional interpretation of data rights; secondly, it views data rights solely as objective norms, disregarding the inherent constitutional quality of their fundamental rights.

From an interpretative perspective, the *Constitution* of China implicitly provides the normative basis for data rights. In the field of data rights, domestic researchers tend to narrow the constitutional normative basis of this right, either taking only the "human rights clause" and "dignity clause" as its normative basis[24] or resorting to theories such as constitutional delegation and institutional guarantees,[25] without paying attention to the interpretative aspects of other constitutional norms. This tendency leads to two problems: first, it does not pay attention to the relationship between "fundamental rights" and data rights; second, it objectively regards data rights as objective norms, thereby erasing their constitutional quality as fundamental rights. Analytical models such as constitutional delegation and institutional guarantee reduce the constitutional status of data rights, directing the nature of data rights to objective norms and a state's protection obligations, making data rights fall only within the scope of protection by ordinary laws and departmental laws, and eliminating the constitutional nature of data rights to resist infringement by public power. Data rights must be protected by private law through general laws such as civil law, and departmental laws also have the protection obligation of the state to

[24] Some scholars have summarized the constitutional basis for data rights as "personal dignity," "human rights" and "social security system." See Zhou Weidong, "Expansion on Constitutional Systematization of Rights in Personal Data," *Law Science* 1 (2023): 32-48.
[25] Dai Jitao, "The Right to Protection of Personal Data as a Constitutional Right," 110-130.

implement constitutional values through legislation to stop infringements by individuals. However, objective norms cannot replace the constitutional quality of fundamental rights, which serve as defensive rights against infringements by the state and public power. Furthermore, both the constitutional delegation theory and the institutional guarantee theory analyze from the perspective of the constitution's tasks in the legal order, rather than analyzing the constitutional relationship between individuals and the state. This is the reason why data rights are only regarded as objective norms, and it is also the theoretical blind spot that makes departmental laws dominate the research on data rights. In essence, it can be attributed to the weakness of constitutional interpretation theory. It has not examined the fundamental rights clauses of our constitution from the perspective of hermeneutics and has taken the long way around, relying on constitutional delegation and institutional guarantee to give data rights an objective normative status, thus ignoring the fundamental rights attributes of data rights. In addition to the provision in Article 33(3) of the *Constitution* that "the state respects and protects human rights," the following fundamental rights clauses are the constitutional normative sources of data rights, indicating that data rights are not only objective norms, but also fundamental rights and constitutional rights.

A. "Human dignity": respect for data

Dignity is one of the constitutional norms of data rights. Article 38 of China's *Constitution* stipulates the personal dignity clause, which encompasses both personal integrity and respect for individuals. This article is an independent constitutional norm[26] and one of the normative bases for data rights.

Personal data has unique attributes and is the embodiment of what makes a person a person; different from other individuals. Personal data is neither replicable nor imitable and belongs to the inherent dignity of humans. Theoretically, Kant's famous assertion that "each person is an end and not a means" connotes dignity, signifying that individuals can only function as subjects, not objects or means. The theory of dignity has developed into the "object formula" in Germany's Constitution, which points out that people can only be their own masters in order to be in line with their own dignity, that is, "the individual as a person himself is at the center and is respected and recognized for his humanity."[27] Man is himself. Man is the future of man. The individual is the master of his own destiny and must develop himself according to his own regulations. Otherwise, he will be reduced to a mere means and object, a violation of his dignity. The state cannot deviate from the purpose of

[26] Zheng Xianjun, "On the Normative Status of the *Constitution*'s 'Personal Dignity' Clause," *China Legal Science* 2 (2012): 79-89.

[27] Clemens Mentzer, "Introduction to The Role of the State," in Wilhelm von Humboldt, *The Sphere and Duties of Government*, translated by Lin Rongyuan and Feng Xingyuan (Beijing: China Social Sciences Press, 1998), 2.

developing human personality; otherwise, the individual "will remain a mere object, a potential force for change that has not been developed or a mass of exchangeable goods that are controlled by others."[28] Dignity as a fundamental right was confirmed in international documents after World War II, which is completely different from the natural human rights of the classical period. The "nature" in the natural human rights refers to the Creator and the transcendental power independent of human will. Dignity is not independent of the individual but exists within the individual himself. It is based on the autonomous characteristics of independent individuals in secular society. Therefore, it is neither innate nor assumed, but inherent in human nature. Dignity in the Japanese Constitution is both a victory over collectivism and a transcendence of egoism, and its ideology is based on individualism. Japanese constitutional scholar Toshiyoshi Miyazawa points out that being respected as an individual demonstrates the principle of individualism.[29] Whether it is the right to correction, the right to be forgotten, or the right to objection, it indicates that individuals have the right to maintain the confidentiality, integrity, and availability of personal data through their own will, and individuals have the right to be respected by others by eliminating erroneous data, false data, and outdated data.

B. Data integrity of "personality self-discipline"

The protection of personality is the normative basis for data rights, and its core is "personality self-discipline." Personality self-discipline refers to the self-setting of personality, which includes self-restraint and self-improvement of personality. Data rights have natural personality attributes and are the objective existence that distinguishes an individual from others. Individuals have the right to maintain their own existence and image by keeping their personal data intact, confidential, and authentic. Kant points out that "Personality is the subject whose actions can be imputed to it."[30] Personality is a process of continuous shaping and completion.[31] He believes that "personality is subject to no other laws except those which it itself (either alone or in conjunction with others) promulgates for itself."[32] A moral character is one to whom one can attribute past actions. The Supreme Court of Japan pointed out in a 1986 ruling that "In terms of protecting personal reputation as a personality right, it is judged that 'when the value of a person's character, morality, reputation, credit, etc., as

[28] Ibid.

[29] Miyazawa Toshiyoshi, *The Spirit of the Constitution of Japan*, translated by Dong Ruiyu (Beijing: China Democracy and Law Publishing House, 1990), 170.

[30] Gary B. Herbert, *A Philosophical History of Rights*, translated by Huang Tao and Wang Tao (Shanghai: East China Normal University Press, 2020), 214.

[31] Teruya Abe et al., *The Constitution: Basic Human Rights (vol. 2)*, translated by Zhou Xianzong (Beijing: China University of Political Science and Law Press, 2006), 98.

[32] Gary B. Herbert, *A Philosophical History of Rights*, translated by Huang Tao and Wang Tao (Shanghai: East China Normal University Press, 2020), 214.

evaluated by society, is unlawfully infringed upon,' in addition to seeking damages and restoring reputation, one may also request to prohibit future infringements."[33] This attribute of personality rights gives data rights a self-discipline feature. Individuals have the right to know whether their data is used, under what circumstances, and whether it is used against their will through the right to know, the right to fair treatment, and the right to review, so as to maintain the integrity of their personal data.

It is important to note that dignity and personality are distinct concepts, each having its own nature and normative implications. The nature of dignity lies in the respect of the state and others; personality is the spiritual cognition of the self, which is subject to personal freedom. Its nature lies in self-discipline and self-determination under the premise of excluding interference from others. Kant points out that personality is different from things. "Personality is subject to no other laws except those which it itself (either alone or in conjunction with others) promulgates for itself, but for animals there is no responsibility."[34] In a democratic country ruled by law, respect for individuals is a universal requirement. Every person is unique, and there is no universal, unified personality. Different individuals have different personalities. Filling in specific data shapes each individual's personality. Its self-determined attribute creates the self-determined nature of data rights and is also the profound philosophical motivation for data integrity. "Personality self-discipline" and the resulting "personality self-determination" indicate that the content of data rights refers to personal information, materials, and files, which involve the disclosure of information related to oneself, and individuals have the right to make their own decisions.

C. Data reshaping of the pursuit of happiness in "human rights"

The pursuit of happiness is one of the connotations of data rights. Its normative basis is Article 33 of the Constitution of the People's Republic of China, which stipulates that "the state respects and protects human rights." "Human rights" contain the content of the right to pursue happiness. Furthermore, the "dignity clause" and "personal freedom" also imply the right to pursue happiness.

The pursuit of happiness means that everyone has the right to pursue happiness and shape themselves. According to Japanese constitutional theory, the pursuit of happiness stems from individualism, closely aligns with the legal principle of dignity, and possesses a legal essence. Dignity is the normative basis of this right.[35] The central feature of Japan's right to pursue happiness is

[33] Teruya Abe et al., *The Constitution: Basic Human Rights (vol. 2)*, translaged by Zhou Xianzong (Beijing: China University of Political Science and Law Press, 2006), 100.
[34] Immanuel Kant, *Fundamental Principles of the Metaphysic of Morals*, translated by Wang Rong and Li Qiuling (Beijing: China Renmin University Press, 2013), 50.
[35] Zhang Weiwei, "On the 'Right to Pursue Happiness' As a General Right in the Japanese

that it emphasizes its right attributes in positive law. It is not just a general clause but has specific constitutional connotations and is a specific right. As a general constitutional right, the right to pursue happiness is the basis for fundamental rights not listed in the Constitution and plays a unique role when other fundamental rights, such as privacy, cannot be guaranteed. In recent years, Japan has protected personal self-discipline as a right, calling it the "fundamental right to personal self-discipline," the basis of which is the "right to pursue happiness." All unlisted fundamental rights can be derived from this and are supplemented by the right to pursue happiness in Article 13 of the Japanese Constitution. Japan's right to pursue happiness is an independent norm, and its status has become synonymous with human rights and dignity. It is a "right of rights" and a "norm of norms." In the digital and information age, the right to pursue happiness has become synonymous with personality self-discipline because it is associated with respect for the individual and personal values, providing the basis for all names, reputations, honors, right of personality of copyright and privacy rights.[36]

In addition to the current Constitution, the Preamble of China's Constitution of 1954 stipulates that "The people's democratic system of the People's Republic of China... aims to ensure that China can eliminate exploitation and poverty through peaceful means and build a prosperous and happy socialist society." "People's yearning and pursuit of a better life," as mentioned by Xi Jinping, general secretary of the Communist Party of China (CPC) Central Committee, constitutes the legal basis for the right to pursue happiness. The meaning of happiness refers to shaping and realizing oneself and improving the quality of life, including spiritual and material living standards and abilities. The self-discipline inherent in personal dignity significantly contributes to enhancing self-quality and personal integrity. It can be used to forge a sound personality and cultivate a spirit of personal responsibility through self-restraint. The "right to correction" is an individual's reshaping of his or her own personality. Forgetting is the beginning of a new life and the pursuit of happiness.

D. Data privacy concerning "residence" and "freedom of communication"

Privacy is the inherent connotation of data rights. Article 39 of the *Constitution* of the People's Republic of China, which states that "the residence shall be inviolable," and Article 40, which states that "freedom of communication and confidentiality of communication shall be protected by law," provide a normative basis for privacy. Personal data is a private matter and is not intended to be known to others. Its privacy is necessary to maintain the uniqueness of the individual and is what distinguishes an individual from others.

Constitution," *Hebei Law Science* 10 (2010): 171-178.

[36] Teruya Abe et al., *The Constitution: Basic Human Rights (vol. 2)*, translated by Zhou Xianzong (Beijing: China University of Political Science and Law Press, 2006), 96 and 98.

Data rights and privacy rights overlap yet differ. The former pertains to an individual's freedom to manage and exercise self-determination over all their personal data, whereas the latter solely pertains to the individual's right to manage information that is not part of the public domain and that they wish to remain anonymous. As long as it does not affect the public interest and the freedom of others, others and public authorities have no right to interfere without legitimate reasons; otherwise, it will violate personal privacy. The constitutions of almost all countries in the world recognize that privacy is included in residence, family, and freedom and confidentiality of communication. Residence and family are personal, private spaces that have nothing to do with public life and are personal privacy. No one may enter another person's home or interfere with another person's family without permission. Correspondence is a form of communication between individuals to express feelings, opinions and insights, and is a form of personal privacy. Article 22 of the 1992 *Lithuanian Constitution* states, "The private life of a human being shall be inviolable. Personal correspondence, telephone conversations, telegraph messages, and other communications shall be inviolable." Article 24 provides that "The home of a human being shall be inviolable. Without the consent of the resident, entrance into his home shall not be permitted." Article 17 of the 1966 *International Covenant on Civil and Political Rights* stipulates that "No one shall be subjected to arbitrary or unlawful interference with his privacy, family, home or correspondence, nor to unlawful attacks on his honor and reputation." Japan calls the right to privacy the right to information privacy, believing that "individuals are morally self-disciplined entities pursuing purposes deemed good for themselves through judgment, communicating with others, and having a selective range and nature of information privacy rights regarding the disclosure of information related to themselves."[37] In practice, in the Gonźalez v.Google Spain SL case,[38] the European Court of Justice held that, according to the *Charter of Fundamental Rights of the European Union,* data subjects have the right to privacy and the right to protection of personal data. Generally speaking, these two rights outweigh the economic interests of search engine operators and the interests of the public in obtaining data from search engines by entering the name of the data subject, indicating that personal data privacy information outweighs the economic interests of search engine operators and the public.

[37] Teruya Abe et al., *The Constitution: Basic Human Rights (vol. 2),* translated by Zhou Xianzong (Beijing: China University of Political Science and Law Press, 2006), 101.

[38] González v. Google Spain SL is a case involving the "right to be forgotten." On May 13, 2014, the European Court of Justice (ECJ) ruled that the *Directive 95/46/EC of 1995* applies to Internet search service providers, and that data controllers are responsible for web page information containing personal data published by third parties that they process and are obliged to delete it.

E. Ownership of data concerning "property rights"

Data is a thing and has the attributes of property rights. As a new type of property rights, data property rights refer to an individual's autonomy and control over his or her own information, materials, and files. Autonomy and control are the characteristics of ownership. Its property rights attributes do not have economic value and economic benefits like intellectual property and copyright, but individuals lose control over their own data.[39] The reasons why data rights become property rights are as follows. First, property rights are a sovereign right. Individuals have the right to control their own property. Its inherent characteristics are that no one else may possess, use, benefit from, or dispose of it without the consent of the owner or the need for public interest.[40] As a property right, data rights mean that without the individual's consent or the need for public interest, public power and others may not steal, disclose, destroy, copy, paste or capture their personal data. Second, data rights have economic benefits. As personal property, data can be sold, transferred and generate economic benefits and economic value, expressed in money. This feature of data rights is consistent with the content of property rights in Article 13 of the *Constitution* of China, which stipulates that "Citizens' lawful private property is inviolable. The state shall protect the right of citizens to own and inherit private property in accordance with the provisions of law. The state may, in order to meet the demands of the public interest and in accordance with the provisions of law, expropriate or requisition citizens' private property and furnish compensation."

To sum up, the constitutional norms of data rights indicate the following four aspects. First, although China's *Constitution* does not explicitly stipulate data rights, data rights are not derived from the constitutional delegation and institutional guarantee in the general principles, but are directly derived from the fundamental rights stipulated in the *Constitution*. Therefore, data rights are fundamental rights rather than just objective norms. Second, the multiple normative bases of data rights indicate overlapping constitutional values and co-petiion of norms, indicating that data rights have multiple constitutional value attributes. The constitutional qualities of data rights are pluralistic yet unified. They are not limited to the three categories of personal rights, property rights, and privacy rights, but rather integrate the three into one, with the attributes of dignity and pursuit of happiness. The *Data Regulations of Shenzhen Special Economic Zone* implemented on January 1, 2022 is the first basic and comprehensive local regulation in China on data rights. The

[39] James Grimmelmann and Christina Mulligan, "Data Property," *Law-Based Society* 1 (2024): 61-80.

[40] Zhang Xinbao, "On Data Property Rights as a New Type of Property Right," cssn.cn accessed November 29, 2022, https://www.cssn.cn/dkzgxp/zgxp_zgshkx/2023nd4q/202305/t20230531_5641709.shtml.

Regulations stipulate that "Natural persons enjoy personal rights and interests in personal data; natural persons, legal persons and unincorporated organizations enjoy property rights and interests in data products and services formed by their legal processing of data." This is equivalent to confirming data rights at the regulation level, distinguishing them from personal rights and property rights.[41] This means that any tendency to single out the constitutional value of data rights is inappropriate. Whether denying its personality rights attributes or denying its property rights attributes,[42] the complex value attributes of this right are ignored, which will undermine the multiple protection of data rights in practice. Third, the simple constitutional norms of data rights and the theory of constitutional delegation and system support to some extent reflect that the "fundamental rights" in China's *Constitution* have not been correctly interpreted. Fourth, the normative basis of China's data rights reveals their difference from digital rights. Irrespective of the general human rights provisions, such as dignity, personal freedom, family, residence, freedom and privacy of communication, and property rights, all of these imply the moral self-discipline of personal reputation and credit. These are fundamentally distinct from the digital human rights of free participation that are manifested in the internet and virtual space. It is important to note that these two types of rights cannot be equated or compared with each other.

III. Data Rights as the Right of Individual Self-Determination

Individuals are the owners and sovereigns of their own data. Unless it is for the public interest, data controllers, processors, operators, legal persons, institutions, or countries and government organizations must use the data in accordance with the individual's will. This is what distinguishes data rights from digital rights, and is also the legal philosophical basis of data rights.

A. Differences between data rights and digital rights

Data rights and digital rights are significantly different in concepts, philosophical foundations, and normative bases. Data rights refer to the data subject's ownership of his or her own information, files, materials, and data. Its philosophical basis is personal information autonomy, and its normative basis is human rights, personal rights, personal dignity, freedom of residence, freedom of communication and confidentiality of communication, and property rights as stipulated in China's *Constitution*. Digital rights are an extension of basic constitutional rights in cyberspace and the virtual world. They refer to the

[41] Wang Zipei, "Shenzhen's Legislation to Regulate Data Rights Is of Great Significance," czly.jsjc.gov.cn, accessed November 11, 2022, http://czly.jsjc.gov.cn/xf/202107/l20210713_1247211.shtml.

[42] Zhou Sijia, "Constitutional Analysis of Personal Data Rights," *Journal of Chongqing University (Social Science Edition)* 1 (2021): 133-140. Although the article emphasizes that data rights are a constitutional right, it denies that it is a property right. This goes to another extreme and ignores the fact that data rights have complex value attributes.

right of individuals to express opinions, communicate, create and publish works, consume, play games, and receive education on the Internet. Its philosophical basis is cyberspace democracy, and its core and essence are to promote participation and expression. Its normative basis is the fundamental rights stipulated in China's *Constitution*. In 2022, the Preamble of the *European Declaration on Digital Rights and Digital Principles* jointly issued by the European Parliament, the European Council, and the European Commission stipulates that "(we commit to) strengthening the democratic framework for a digital transformation that benefits everyone and improves the lives of all people living in the EU." In 2022, the European Council adopted the *Lisbon Declaration — Digital Democracy with a Purpose*, calling for a digital transformation model that is centered on a digital single market and enriches the digital ecosystem. In May 2023, UN Secretary-General António Guterres released the Global Digital Compact. The Compact takes the *UN Charter* and the *Universal Declaration of Human Rights* as its agenda, recognizes that human dignity is at its core and universal human rights are the basis for promoting a digital future of open, free, secure, and people-centered internet access, and it ensures that cyberspace is non-discriminatory and safe for women, expands women's digital participation, and eliminates the digital gender divide.

These illustrate that the value foundation of digital rights is cyber democracy, ensuring participation, inclusion, and equality for everyone and opposing discrimination, violence, terror, false information, and misinformation. At the same time, digital rights are not a new type of rights, nor are they the fourth generation of human rights, but rather an extension of the values of traditional fundamental rights in the cyber world. We can refer to cyberspace as virtual, online, electronic, and digital. As the *European Declaration on Digital Rights and Digital Principles* states in its Preamble, "With the acceleration of the digital transformation, the time has come for the EU to spell out how its values and fundamental rights applicable offline should be applied in the digital environment." The Declaration states that European values and the rights and freedoms enshrined in the EU legal framework must be respected in cyberspace.

B. Individual self-determination is determined by the attributes of data rights

The GDPR clearly stipulates a series of data rights, including the right to fair processing, the right to access, the right to correction, the right to be forgotten, the right to objection, the right to portability, the right to restrict processing, and rights related to automated decision-making. Chapter IV: Individuals' Rights in Personal Information Processing Activities of China's *Personal Information Protection Law* stipulates the types of data rights. Referring to the *Data Security Law* and the *Cybersecurity Law*, China's laws

~~stipulate that~~ individuals enjoy the following data rights. First, the right of individuals to process their information, including the right to know, the right to decide, and the right to restrict or refuse others from processing their personal information.[43] Second, the right to review and copy.[44] Third, the right to correction.[45] Fourth, the right to delete.[46] Fifth, the right to request an explanation.[47] Sixth, the right to information of the deceased.[48] Seventh, the right to relief.[49] In addition to these provisions of the *Personal Information Protection Law*, the *Data Security Law* and the *Cybersecurity Law* also stipulate some data rights. These rights overlap with the rights stipulated in the *Personal Information Protection Law* in most cases, but there are also other data rights,

[43] This article stipulates that "Individuals shall have the right to be informed, the right to make decisions on the processing of their personal information, and the right to restrict or refuse the processing of their personal information by others, except as otherwise provided by laws or administrative regulations."

[44] The normative basis is Article 45(3) of the *Personal Information Protection Law*: "Where an individual requests the transfer of his personal information to a designated personal information processor, which meets the requirements of national cyberspace department for transferring personal information, the requested personal information processor shall provide means for the transfer."

[45] The normative basis is Article 46(1) of the *Personal Information Protection Law*: "Where an individual discovers that his personal information is incorrect or incomplete, he shall have the right to request the personal information processors to rectify or supplement relevant information."

[46] Article 47 of the *Personal Information Protection Law* provides that "In any of the following circumstances, a personal information processor shall take the initiative to erase personal information, and an individual has the right to request the deletion of his personal information if the personal information processor fails to erase the information: (1) the purposes of processing have been achieved or cannot be achieved, or such information is no longer necessary for achieving the purposes of processing; (2) the personal information processor ceases to provide products or services, or the storage period has expired; (3) the individual withdraws his consent; (4) the personal information processor processes personal information in violation of laws, administrative regulations, or agreements; or (5) other circumstances as provided by laws and administrative regulations. Where the storage period provided by any law or administrative regulation has not expired, or it is difficult to erase personal information technically, the personal information processor shall cease the processing of personal information other than storing and taking necessary security protection measures for such information."

[47] This article stipulates that "An individual has the right to request a personal information processor to interpret the personal information processing rules developed by the latter."

[48] This article stipulates that "The close relatives of a deceased natural person may, for their own legal and legitimate interests, exercise the rights to handle the personal information of the deceased, such as consultation, duplication, rectification, and deletion, as provided in this Chapter, except as otherwise arranged by the deceased before death."

[49] This article stipulates that "A personal information processor shall establish the mechanism for receiving and handling individuals' requests for exercising their rights. Where an individual's request is rejected, the reasons therefor shall be given."

such as the right to cybersecurity, the right to privacy in cyberspace, the right to cyber data security, etc. These rights themselves indicate that data belongs to individuals and must be subject to individual will and autonomous decision-making. They are the normative basis for determining the quality of autonomous data rights.

Some scholars further divide data rights into categories such as data personality rights, data identity rights, data credit rights, data equality rights, data privacy rights, and data property rights, which can confuse the distinction between data rights and digital rights. Data rights certainly include data privacy and data property rights, but it may not be appropriate to call them "data personality rights" or "data identity rights." Instead, they should be called "digital personality" or "digital identity" rights[50] Cyberspace encompasses digital personality, digital credit, and digital identity, all of which represent an individual's image and identity on the internet and in the virtual world, commonly referred to as their "virtual image." Whether an individual is honest and trustworthy, whether he honors his promises and keeps his word, whether he abides by rules and contracts, whether he fulfills his legal obligations, whether he does not publish false information, does not slander or insult others, does not launch cyber violence, and does not engage in cyber-bullying, all involve personal image, identity, and status in the digital world and are therefore inherent in digital human rights, but they do not belong to data rights. Individuals have a "virtual image" in the digital world, also known as virtual reality, where they can experience "digital immortality" or "digital reincarnation."[51] It is not allowed to forcibly construct a virtual image of another person and use this image to do bad things; otherwise, it may constitute defamation or fraud. Moreover, if the words and deeds of this virtual character mislead people in the real world, it involves accountability issues and may even constitute criminal liability.[52] Some papers consider the right of access as a data right, which is deemed inappropriate. The right of access means that individuals have the right to freely access the internet and browse websites to obtain information. This is a digital right, but not a data right. The so-called access in data rights refers to the right to fair processing and the right to review, which means that individuals have the right to obtain information about how their

[50] On 29 June 2023, the Council of the European Union announced that it had reached a provisional political agreement with the European Parliament on the core elements of a new European Digital Identity (eID) framework, which will amend Regulation (EU) 910/2014 (eIDAS Regulation), accessed November 29, 2022, https://www.sohu.com/a/694358919_120076174.

[51] In Taiwan Province of China, digital is translated as "数位" while in Hong Kong SAR it is translated as "数码".

[52] Kai-Fu Lee and Chen Qiufan, *AI 2041: Ten Visions for Our Future* (Taipei: Global Views Commonwealth Publishing Co., Ltd. 2021), 243.

information is used, by whom, and under what circumstances it is used. The content of data rights has been stipulated by laws such as the *Personal Information Protection Law*, and the GDPR has also clearly defined the specific connotations of data rights. These so-called bundles of data rights are the result of confusing data rights and digital rights. They also represent the "illusions" that data rights have created during the process of digitalization. They are what Bacon called "Idols of the Marketplace" and "Idols of the Theater."

C. Self-determination is determined by the principle of informed consent

As mentioned earlier, the principle of consent has been confirmed in the *Constitution* of the Russian Federation and the *Charter of Fundamental Rights of the European Union*. The latter stipulates freedom of personal information and consent in Title II: Freedoms, which not only shows that this right is a natural constitutional right but also explains the constitutional quality of "self-determination" and the difference between data rights and digital rights.

The principle of informed consent means that data controllers and processors should obtain the consent of the data subject when using personal data. "Processing" here includes collection, storage, dissemination, recording, organization, construction, adjustment, retrieval, change, use, consultation, disclosure, etc. The reason why informed consent becomes a protection principle for data rights is determined by the philosophical quality of data rights. Individuals are the owners of their own data and information and are subject to their own will. The nature of their autonomy determines that public power, including other people and institutions, may not process personal data without their prior consent. Chapter 2 of the GDPR specifies the principle of informed consent in detail and uses Articles 5, 6, 7, 8, 9, and 10 to define the connotation of this principle, including consent, informed consent, voluntariness, withdrawal of consent, and consent substitution, and also stipulates child's consent, consent of special categories of subjects, consent to the personal data relating to criminal convictions and offences, and consent to already public data. China's *Personal Information Protection Law* stipulates the principle of informed consent. In addition to Article 13, Articles 14, 15, and 16 of the Law make specific provisions for this.[53] Article 41 of the *Cybersecurity Law* also

[53] Article 13 of the *Personal Information Protection Law* stipulates that "A personal information processor can process personal information of an individual only if one of the following circumstances exists: (1) the individual's consent has been obtained"; Article 14 provides that "Where personal information processing is based on individual consent, the individual consent shall be voluntary, explicit, and fully informed. Where any other law or administrative regulation provides that an individual's separate consent or written consent must be obtained for processing personal information, such provisions shall apply. In the case of any change of the purposes or means of personal information processing, or the category of processed personal information, a new consent shall be obtained from the individual." Article 15 provides that "Where personal information processing is based on individual consent, an individual shall have the right to withdraw his consent. Personal

stipulates the principle of consent.[54] It can be seen from this that the philosophical quality of data rights is personal information autonomy, that is, the data subject has the right to self-determination over personal data. Personal information autonomy is also known as personal information self-determination, and personal information self-discipline, and is subject to personal will and self-determination. Individuals are the owners, sovereigns, managers, and disposers of their own data. In addition to complying with the public interest, individuals have the right to decide how their data is used. Personal information autonomy is a manifestation of personal self-determination or self-discipline in the private sphere. Individuals have the right to independently process all information about themselves as long as it does not conflict with the public interest or those of others. In this sense, data rights are equivalent to personal information rights, and individuals have the right to process their personal data independently. This means that individuals have the right to independently decide on the use, collection, storage, and publication of their own information (data) as long as it does not infringe on the public interest or the rights and freedoms of others. Whether it is the right to fair processing, the right to review, the right to correction, the right to be forgotten, or the right to objection, the right to portability or the right to restrict processing, all must be processed based on the individual's self-determination.

D. The ethical quality of self-determination determines its difference from

information processors shall provide convenient ways for individuals to withdraw their consent. The withdrawal of consent shall not affect the validity of the processing activities conducted based on consent before it is withdrawn." Article 16 stipulates that "A personal information processor shall not refuse to provide products or services for an individual on the grounds that the individual withholds his consent for the processing of his personal information or has withdrawn his consent for the processing of personal information, except where the processing of personal information is necessary for the provision of products or services."

[54] The specific connotations of the principle of informed consent in China's laws are as follows: First, personal consent. Consent refers to the data subject's freely given, fully informed, unambiguous consent to the processing of his or her personal data through a statement or a clear and convincing action. Second, consent is given voluntarily and clearly by the individual on the premise of being fully informed. Third, the individual's separate consent or written consent is given in accordance with the law. Fourth, if the purpose, method, or type of personal information processed changes, the individual's consent must be obtained again. Fifth, if personal information is processed based on the individual's consent, the individual has the right to withdraw his or her consent, and the processor should provide a convenient way to withdraw consent. Sixth, an individual's withdrawal of consent does not affect the effectiveness of personal information processing activities that have been conducted based on the individual's consent before the withdrawal. Seventh, personal information processors may not refuse to provide products or services on the grounds that the individual does not agree to the processing of his or her personal information or withdraws consent.

digital rights

The ethical quality of digital rights is not individual self-determination but cyber democracy. Digital rights are not a new type of rights but an extension of fundamental rights in cyberspace and virtual space, manifested in automated processing. The normative features of digital rights are access, participation, and free expression in cyberspace and virtual spaces, in addition to some cyber data such as privacy. Due to the particularity of the cyberspace, such extension mainly lies in the fact that digital rights, while promoting communication, oppose discrimination and bullying and improve the online protection of personal data and privacy. China's *Cybersecurity Law* stipulates the digital rights of individuals but does not list them in a separate chapter. Instead, they are scattered in various chapters, mainly summarizing these rights from the perspective of internet users, including the right of access, the right to freedom of speech on the internet, the right to privacy on the internet, the right to exit, opposition to cyber-bullying and cyber violence, as well as online education, online consumption, entertainment, games, etc. Indeed, digital rights and data rights overlap, manifested in the storage of personal data, including personal birth, experiences, residence, communication methods, medical records, political inclinations, religious beliefs, ethnicity, race, and sensitive personal information, which all become electronic data that can be processed automatically. It is true that the electronic transformation or the internet application of personal data means digitization, but the two do not completely overlap, because "data' is not equivalent to "digital."[55] For example, freedom of speech on the internet, online education, online consumption, online games, and entertainment are all typical digital rights, not data rights.

The key to distinguishing between the two is the difference in philosophical foundations. Individual self-determination means that individuals are the owners and sovereigns of their own data. Based on their own will, individuals have the right to decide whether to make their data public; cyber democracy determines the freedom of individuals in cyberspace. Digital rights are exercised in cyberspace and the virtual world,[56] which provides individuals

[55] Viktor Mayer-Schönberger and Kenneth Cukier, *Big Data: A Revolution That Will Transform How We Live, Work, and Think*, translated by Sheng Yangyan and Zhou Tao (Hangzhou: Zhejiang People's Publishing House, 2013), 102. Zheng Xianjun, "Conceptual Analysis of Data Rights and Digital Rights," *The Democracy and Law Times*, December 16, 2022.

[56] If VR (virtual reality) creates a sense of the "spiritual realm" as Qian Xuesen says; AR (augmented reality) can also be called "expanded reality," which is a feeling of superposition of virtual world and real world, that is, the combination of virtual and real. The latest MR (mixed reality) technology creates a feeling of interactive feedback between virtual reality and the real world. It is not a simple superposition between the virtual and the real, but requires understanding of the scene, including interaction and feedback, which needs to be strengthened. VR, AR and MR are collectively referred to as XR. Their

with freedom of action in the digital age. These rights cannot be equated with data rights. Their salient feature is the freedom of individual action in virtual space, the combination of the virtual world and reality, and the interaction between the virtual world and reality. This combination and interaction determine the democratic and participatory quality of digital rights, which is incomparable to data rights, including personal information, materials, and files. Currently, many studies in academia confuse the two, which is something that must be noticed.

Generally speaking, individuals are the owners of their own data, which is clearly different from the inviolability of caber terrorism terrorism democracy. Although there is value overlap and normative co-petition between digital rights and data rights, the two not only have significant differences in normative connotations but also have distinct philosophical qualities and constitutional purposes. Therefore, achieving a balance between protecting personal data self-determination and promoting the free flow of data is the main purpose of data rights, while resisting discrimination, bullying, violence, and cyber terrorism, protecting expression, privacy and opposing false information are the focus of digital rights protection. This highlights the substantial distinction between the two.

IV. Restriction of Restrictions: Substantive Protection of Data Rights

A. The connotation of the principle of proportionality

The principle of proportionality plays an important role in protecting the essence of fundamental rights. Its mechanism is to prevent fundamental rights from exceeding necessary limits and infringing upon the core or essence of the fundamental rights when they are restricted by legislative power. Therefore, the principle of proportionality is an important device reserved by the constitution, which is reflected in "restrictions must be subject to restrictions." As the "imperial principle" of fundamental rights protection, the principle of proportionality ensures that the core of fundamental rights is not violated by the legislature and is an important tool for the constitutional restriction of legislative power. This device is fully reflected in the use and restriction of data rights. However, due to the absence of a fundamental rights perspective in existing research, data rights studies have not fully developed the important principle that fundamental rights must be subject to restrictions.

The principle of proportionality is a constitutional principle, which can be called "prohibition of excessiveness." This principle examines the relationship

prominent feature is "immersive," making it difficult to distinguish between the real and the virtual. This technology covers the human sixth sense in all directions and is achieved by fooling human senses, with vision being the sense most fooled. Kai-Fu Lee and Chen Qiufan, *AI 2041: Ten Visions for Our Future* (Taipei: Global Views Commonwealth Publishing Co., Ltd. 2021), 231.

between purpose and means to determine whether the restriction of fundamental rights by law is reasonable, and prevents the restriction of fundamental rights from exceeding the necessary limit.[57] The principle of proportionality includes three sub-principles, namely necessity, appropriateness and rationality (narrow sense of proportionality, equality and balance). China's data laws clearly stipulate the principle of proportionality. Article 41(2) of the *Cybersecurity Law* stipulates that "Network operators shall not collect personal information which is unrelated to the services they provide." Article 1035(1) of the *Civil Code* stipulates that the processing of personal information shall be in compliance with the principles of lawfulness, justification, and within a necessary limit, and shall not be excessively processed. Article 6 of the *Personal Information Protection Law* states that "Personal information processing shall be based on explicit and reasonable purposes and directly related to those purposes, and shall exert the minimum impacts on the rights and interests of individuals. The collection of personal information shall be limited to the minimum scope required by the purpose of processing, and personal information may not be collected excessively." These provisions contain the content of the principle of proportionality, clarifying that there must be a relevance between the purpose and the means, and that the means must be appropriate and prohibit excessiveness.

B. The reflection of the principle of proportionality in data rights protection

Necessity refers to the relevance between the means taken and the purpose. If too much personal information is collected, or the data and information are irrelevant to the purpose, or the purpose of disclosing the data no longer exists, it constitutes excessive collection and excessive disclosure. The "minimum impacts" principle of necessity is being violated. The principle of necessity, commonly referred to as the principle of minimum impacts, mandates the restriction of fundamental rights using the mildest, least intrusive, and irreplaceable methods. Reasonableness means that the means and purpose of infringement must be moderate, balanced, and proportionate and must be within the legal scope and reasonable proportion. It must not exceed the necessary limits or infringe upon the core of fundamental rights. Otherwise, the core of fundamental rights will be hollowed out, and the protection of fundamental

[57] German constitutional scholar Dieter Grimm believes that the current German Constitution has a declining ability to protect fundamental rights. He points out that "Even the principle of proportionality, which is responsible for providing substantive protection for fundamental rights, requires the rule of law and democracy to pay a price. The reason is that as a standard of appropriateness and rationality, the principle of proportionality has largely lost the possibility of being universal." See Dieter Grimm, *Constitutionalism: Past, Present, and Future*, translated by Liu Gang (Beijing: Law Press·China, 2010), 125.

rights will lose its meaning. Items 5 and 6, Article 13(1) of the *Personal Information Protection Law* stipulate the principle of rationality, which is the normative basis for the restriction of data rights. Item 5 of this article stipulates that "personal information is reasonably processed for news reporting, media supervision, and other activities conducted in the public interest"; Item 6 stipulates that "the personal information disclosed by the individual himself or other legally disclosed personal information of the individual is reasonably processed in accordance with this Law." That is to say, although personal consent may not be obtained for the sake of public interest or public opinion supervision, or personal information may be disclosed for other legitimate purposes, it must be kept within certain reasonable limits. As to what is "reasonable," it is necessary to balance various interests in specific disputes and judge whether the restriction of personal data exceeds the necessary limits, constituting "unreasonable" or disproportionate. It is generally believed that excessive infringement means that it touches the core of fundamental rights. As to what is the core, the general view is that human dignity constitutes the core of fundamental rights. German academia believes that human dignity is the core of both fundamental rights and the constitution. It is not only the essence and core of fundamental rights but can even counter the right to amend the constitution, that is, constitutional amendments must not touch upon human dignity.[58] Here, human dignity is the substantive requirement, and prohibition of excessiveness is the formal requirement. Together, these two elements form the core of the principle of proportionality, which aims to limit restrictions in the protection of fundamental rights. If the means of restricting fundamental rights infringe upon human dignity, it is equivalent to infringing upon its essence, which is not tolerated by the principle of proportionality and is "unreasonable." In addition, the importance of the public interest and the means of restriction are also criteria to help determine whether a particular measure is "unreasonable."

C. Restrictions on data rights protection must be restricted

China's data legislation has imposed restrictions on fundamental rights, stipulating that data rights can be restricted in the public interest. For example, the exception to the principle of informed consent is a manifestation of limiting data rights, which means that for the public interest and the freedom and interests of others, and as provided by law, the processing of specific personal data may not require individual consent. Article 23 of the GDPR specifically stipulates restrictions on data rights, which include ten items, including national security, defence, public security, criminal investigations, compliance with the laws of other EU countries, judicial proceedings, protection of the data subject or the rights and freedoms of others, and enforcement of civil law claims. Here

[58] Chen Ciyang, *The Empirical Approach to the Core Theory of fundamental rights and Its Difficulties* (Beijing: Hanlu Publishing Co., Ltd., 1997), 183-185.

we can see the difference between data rights and digital rights protection principles.

This exception is both a need for data rights to be subject to the public interest and a concrete manifestation of Article 51 of the *Constitution* of the People's Republic of China in restricting data rights.[59] It shows that Article 51 of the *Constitution* is a constitutional norm for restricting fundamental rights and is also the constitutional basis for the exception to the principle of informed consent. [60] Article 13 of China's *Personal Information Protection Law* is a legal norm that restricts data rights and is also the embodiment of the principle of legal reservation in protecting data rights. The six items following the second item of Article 13(1) of the *Personal Information Protection Law* stipulate the specific circumstances in which data rights may be restricted: first, the processing is necessary for the conclusion or performance of a contract in which the individual is a party; second, is necessary for the performance of statutory duties or obligations; third, is necessary for the response to public health emergencies, or for the protection of life, health, and property safety of natural persons in emergencies; fourth, is reasonably processed for news reporting, media supervision, and other activities conducted in the public interest; fifth, the personal information disclosed by the individual himself or other legally disclosed personal information of the individual is reasonably processed in accordance with this Law; and sixth, other circumstances as provided by laws or administrative regulations. This also means that personal data rights can be

[59] Article 51 of the *Constitution* of the People's Republic of China stipulates that "When exercising their freedoms and rights, citizens of the People's Republic of China shall not undermine the interests of the state, society or collectives, or infringe upon the lawful freedoms and rights of other citizens."

[60] This provision is somewhat different from the provisions of GDPR. Article 23 of the GDPR specifically stipulates data rights restrictions, which states that "Personal information processors may process personal information only if any of the following circumstances is met: (a) obtaining the individual's consent; (b) necessary for the conclusion or performance of a contract to which the individual is a party, or necessary for the implementation of human resources management in accordance with labor rules and regulations formulated in accordance with the law and collective contracts signed in accordance with the law; (c) necessary for the performance of statutory duties or statutory obligations; (d) necessary for response to public health emergencies or to protect the life, health, and property safety of natural persons in emergency situations; (e) to process personal information within a reasonable scope for news reporting, public opinion supervision, and other activities in the public interest; (f) to process personal information that an individual has disclosed on his or her own initiative or that has been lawfully disclosed within a reasonable scope in accordance with the provisions of this Law; and (g) other circumstances prescribed by laws and administrative regulations. In accordance with other relevant provisions of this Law, the processing of personal information shall obtain the consent of the individual; however, except for the circumstances specified in the second to seventh items of the preceding paragraph, the consent of the individual is not required."

restricted if these six conditions are met.

Exceptions to the principle of informed consent are certainly restrictions on data rights, but such restrictions must also be restricted and must comply with the principle of proportionality. According to China's *Constitution*, if restrictions on data rights infringe upon the personal dignity of individuals, it constitutes a violation of the essence of data rights. Excessive collection of personal information is an example of this. Collecting personal information without the consent of the person concerned, disclosing or making public other people's information without the consent of the person concerned, and collecting personal information unrelated to the purposes prescribed by law—all of these infringe upon personal dignity to varying degrees and touch upon the core and essence of data rights.

The above-mentioned legislation of China stipulates the principle of proportionality while stipulating the principle of legal reservation. The restrictions in data rights must be subject to restrictions, which means that the principles of appropriateness, necessity and reasonableness should be observed, that is, personal information must be processed within the necessary and reasonable scope. Neither state agencies nor individuals may collect personal information excessively. The *Civil Code*, the *Personal Information Protection Law* and the *Cybersecurity Law* all prohibit excessive collection of personal information. In practice, certain courts have determined that certain applications have unlawfully collected or utilized individuals' personal information. This includes: not clearly specifying the purpose, method, and extent of collecting and utilizing personal information; collecting and utilizing personal information without the user's consent, thereby breaching the principle of necessity; gathering personal information unrelated to the services offered, leading to excessive collection of personal information and violating the "minimum impacts" principle. The data in question qualifies as personal data, thus the principle of proportionality is applicable.

Conclusion

Data rights are the fundamental rights of natural persons. Without them, it is impossible to clarify their constitutional nature, and their protection in practice cannot be complete. Whether it is the subject and nature of data rights, the constitutional basis, value attributes, or even the principles of consent and proportionality, they all reveal its fundamental rights attributes, indicating that it is not only an individual's constitutional right but also has objective normative qualities. Simply entrusting data rights to various departmental laws for protection as objective norms is insufficient and will inevitably lead to the following drawbacks. First, ignoring the fundamental rights status of data rights will split their constitutional value, leading to extremes, either ignoring their attributes of dignity, personality, privacy, and pursuit of happiness or ignoring

their property attributes. Second, treating them as an objective norm will not only make data rights fall into the theoretical misunderstanding that they are only protected by private law but also confuse the differences between data rights and digital rights by ignoring the philosophical qualities of the two. Third, ignoring the constitutional status of data rights will make it impossible to introduce the principle of proportionality in the protection of data rights, making it difficult to ensure that the essence of data rights is not violated and unable to provide comprehensive constitutional protection for data rights.

Neglecting the fundamental rights status of data rights will not only strip them of their attributes as a right to defense, but also undermine vigilance against public power and weaken public law protection of data rights. It is important to remember that when it comes to fundamental rights, resisting infringement by public power is an inherent constitutional duty, and data rights without constitutional protection are destined to remain inadequately safeguarded. Straying from the characterization of data rights as "a fundamental right of natural persons," studies on data rights will inevitably lose its way and struggle to reach full fruition.

(Translated by *CHEN Feng*)