The International Conference on Interdisciplinary Humanities and Communication Studies
DOI: 10.54254/2753-7048/4/2022827

The Dilemma and Outlet of Personal Data Rights Acquisition: Based on the Background of Digital Economy Partnership Agreement

Ruiheng Wang[1, a, *]

[1]*Office of Legal Affairs, Beihang University, No.37 Xueyuan Road, Beijing, China*
a. wrhdzb@buaa.edu.cn
**corresponding author*

Abstract: Constructing data security rules is an important prerequisite for participating in global data governance. China's application to join the "new" digital rules represented by the Digital Economic Partnership Agreement is also one of the ways to try to improve its own data rules, and the protection of personal data rights is the focus of all kinds of data rules. However, "informed and consent", "public interest authorization" and "information disclosure", as three ways of data rights of derivative acquisition, also face various transformations in their application. This paper analyzes the current rules dilemma through literature analysis and comparative research trying to find a way out of the current dilemma in data rights of derivative acquisition.

Keywords: personal data rights, informed and consent, public interest, information disclosure

1. Introduction

On November 1st, 2021, Ministry of Commerce of the People's Republic of China formally submitted an application to join the Digital Economy Partnership Agreement (DEPA) to New Zealand, the depository of DEPA. On August 18th, 2022, according to the decision of the DEPA Joint Committee, the working group on China's accession to DEPA was formally established, which comprehensively promoted the negotiations on China's accession to DEPA [1]. China's application to join DEPA is not only a reasonable reflection of the development trend of global digital trade, but also a concrete action to seek the right to make global digital trade rules. It also shows China's determination to try to participate in global governance by means of international economic law.

DEPA is an agreement aiming at the digital economy signed by Singapore, Chile and New Zealand in 2020. The whole agreement is exclusive to the digital economy. DEPA is different from Regional Trade Agreements (RTAs), and it is inclusive and forward-looking to build digital trade rules by setting up modules. And the issue of "Data Security" to promote cross-border data flow and protect related rights and interests is the core content of DEPA. Therefore, this paper starts from Article 4.2.3 of DEPA and based on the principle of perfecting the legal framework for protecting personal information, analyzes the ways and difficulties of obtaining personal data rights, and tries to find the balance point of acquisition personal data rights.

DOI: 10.54254/2753-7048/4/2022827

2. Personal Data Protection Rules and the Acquisition of Personal Data Rights

At present, there is no uniform standard for the definition of personal data. In the General Data Protection Regulation (GDPR), the concept is information that a data subject can be identified by such data. The process of class identification depends on the setting of data conditions, such as names, ID numbers, location information, and identification criteria, or by comparing one or more conditions of the natural person, one can judge individual conditions, such as genetic information, physiological condition, physical quality, psychological thinking, and cultural level. Literally, personal data can be understanding as the sum of electronic data and other data related to individuals that can be recorded.

Theoretically, it emphasizes the identifiability of personal data. For example, scholars such as Spiekermann S thinks that personal information refers to highly sensitive information that can identify individuals [2]. Morisawa Y divided the data into personal information and private information according to the degree of identification involved [3]. The information that can directly identify a certain person belongs to personal information, while the information that needs to be combined with other data information to indirectly identify a certain person belongs to private information.

2.1. Current Personal Data Protection Rules

From the perspective of global legislative trends, the current international legislation on personal data protection presents the legislative status of regional documents as the mainstay, supplemented by bilateral agreements, such as the Privacy Shield agreement signed by the European Union and the United States in 2016.

In the digital trade rules such as Regional Comprehensive Economic Partnership (RCEP), the United States-Mexico-Canada agreement (USMCA), and Comprehensive and Progressive Agreement for Trans-Pacific Partnership (CPTPP), there are specific rules governing the “protection of personal information”, namely Article 4.2 of DEPA, Article 14.8 of CPTPP, Article 19.18.1 of USMCA and Article 18 of RCEP.

From now on, there are a lot of advocacy clauses in the field of digital rules. Advocacy clauses are the rules that are standardized in soft language. There are two main reasons why a certain issue is classified as an advocacy clause. First, the rule respects a certain principle, but because countries have not yet reached a consensus on a certain issue, in order to ensure the acceptability of the whole rule, this kind of issue is put forward as a soft advocacy rule until the time is ripe to be converted into a mandatory clause. For example, most RATs generally show an approval attitude towards the importance of information. Article 4.2.1 of DEPA, Article 19.8.1 of USMCA and Article 14.8.1 of CPTPP require the recognition of the importance of personal information protection to economy and society in e-commerce, digital trade or digital economy. Compared with USMCA and CPTPP, which limit information to e-commerce or digital trade, DEPA conforms to the characteristics of its agreement covering digital economy, and extends the scope of personal information protection to “participants in the digital economy”. But this is a soft advocacy clause, and there is no substantive regulation.

Second, the solutions to some problems are not mature, and need to be constantly improved and confirmed in the practice of various countries. For example, DEPA stipulates that personal information protection rules should have certain elements, such as Article 4.2.3 of DEPA. This kind of clause has the guiding nature, but the standards of these elements have not been unified, so it is proposed as an advocacy clause and has no binding force.

The EU believes that protecting personal information is a manifestation of protecting basic human rights. GDPR sets high standards for personal data protection. In the Asia-Pacific region, APEC Privacy Framework is the first framework document for the cross-border flow of personal data in the region [4].

DOI: 10.54254/2753-7048/4/2022827

2.2. Acquisition of Personal Data Rights

As a right, personal data right can be acquired in two ways, one is original acquisition, the other is derivative acquisition.

The data subject is the owner of data rights, and the data acquisition method that naturally belongs to the data subject from the beginning of its production belongs to the original acquisition. However, for governments, data enterprises such as digital platforms and general traditional enterprises, their identities are generally data controllers, and there are few cases of obtaining data rights through the original acquisition, because most of the data volume depends on the individual as the data subject.

The data controller is not necessarily the subject that generates the data, and it is also possible to obtain data rights through derivative acquisition. For example, the digital platforms obtain the right to process user data by signing a user agreement with its users. According to the existing domestic and international legislative practices, data controllers who have obtained data control rights through derivative acquisition generally through three ways: one is “informed and consent”, the other is “public interest authorization” and the third is “open data access”.

3. Informed and Consent Mode

3.1. Application Scenarios of Informed and Consent

The Informed and consent model is a form of right submission, in which the data controller who obtains control of data. Personal data is closely related to the data subject itself and can restore the data subject completely, so the processing of personal data needs to be strictly controlled and regulated.

In the current domestic and foreign practices and related regulations, most countries have adopted this mode, clearly explaining to the original data subject why this type of data should be collected and what types of data will be collected. After the data subject has a substantial understanding and agrees to collect and use data, then the data controller gains the data control right.

3.2. The Dilemma of Informed and Consent

With the continuous development of Internet technology, there are some problems to be overcome in the Informed and consent mode. First, the difficulty of obtaining consent is increasing. Under the background of big data, because the purpose of data processing is uncertain and the content of consent is too professional and complex, it makes it more difficult for the data subject to really understand, which affects the psychological expectation of the data subject and then the possibility of consent. In addition, when the requirements of the rules tend to be strict, because the consent is only valid in a specific informing range, when the data processor uses personal information beyond the original range, the processor needs to inform again and obtain consent, which increases the number of times of obtaining consent.

Secondly, it is based on the legal logic behind this model and “autonomy of the will” in the theory of civil law. However, in many cases, the data subject’s consent to the data processing policy is not a true expression of will, but more often it is the consent of exchange conditions. Agree to be a prerequisite for data subjects, especially digital platform users, to obtain a certain product or service [5]. As the data collection pre-requirement requirement of using the program, refusal means that users can't get the right to use it, which also makes this kind of consent compulsory. For example, if users want to send a circle of friends or use a WeChat applet through WeChat, then they must agree to the data acquisition agreements of WeChat or the applet enterprise, otherwise they will not be available to use.

Third, the cost increases. High-volume and high-frequency data collection and processing make

DOI: 10.54254/2753-7048/4/2022827

the cost of consent constantly rise, including time cost and money cost. Reading the data policy will take a lot of time, and most users will choose to quickly skip to the end and click “Agree”. In 2008, a study in the United States showed that if all users in the United States read the online privacy policy word for word, the economic cost in one year would be as high as $781 billion [6]. However, in order to avoid responsibility, data processors are still increasing the length of the policy of formatting data. For most network users, they simply can’t fully understand how their personal information is collected and utilized.

3.3. The Outlet of Informed and Consent Mode

A large number of personal data infringement may lead to a wide range of collective data loss, so the supervision of personal information protection is also the supervision of collective data [7]. Most countries have improved their personal data protection structures and laws, and personal data protection is now regarded as a basic element of data-driven economy [8].

Personal data has the function of identification, but it also has the function of public, which means that there is impersonal decision on the protection of personal data. It is difficult for individuals to maintain their dignity and freedom with weak power. In order to meet the needs of real life, social cybernetics is expected to become the theoretical basis of personal information protection [9]. From “Self-Regarding action” to “Other-Regarding action”, from “individual decision” to “individual-group decision” [10]. The foundation of this change is the “group privacy right” put forward by Mitelstad [11]. Therefore, it can be considered that the data subject’s decision is no longer a personal decision, but will be transformed into a “personal-group decision”.

In addition, different data can be graded, and different grades of data require the consent of data subjects from weak to strong. Different importance and particularity of data are the basis of consent stratification, and identification is the essential feature of personal data, that is, only those data that can be traced back to the real identity of individuals should be protected, while data unrelated to personal identity is less restricted by the principle of Informed and consent.

4. Public Interest Authorization Mode

4.1. Application Scenarios of Public Interest Authorization Mode

Public interest can also be understood as social welfare. As for the non-public data, supplementing the “Informed and consent” model is essentially to protect personal data and privacy. At the same time, to protect social interests. The so-called “public interest” is not specifically explained. The GDPR stipulates that in order to realize the fundamental public order, to engage in scientific analysis and investigation, to investigate historical facts or some special reasons, such as public health or public health fields. Information security Technology-Personal information(PI) security specifications clearly points out that it includes important interests related to national security, such as military, political, national defense and other fields, hygiene and health, stable order, which can be determined, and can be directly collected and used without the authorization and consent of the original data subject.

The right to control data through the purpose of public interest, on this issue, the legitimacy comes from weighing the public interest and the characteristics of personal data. Based on the perspective of social public interests, to the extent that it is reasonable and necessary, the autonomy of personal data is weakened. For example, in the process of Internet operation, network operators intercept information about terrorism or national division from the perspective of national security and social security in information monitoring and report it to the national security department or other relevant departments, that is, through the automatic authorization of public interests, and then, for example, in the epidemic era, through scanning and displaying “health QR code” to obtain permission to pass.

DOI: 10.54254/2753-7048/4/2022827

4.2. The Dilemma of the Public Interest Authorization Model

The biggest problem in the mode of public interest authorization lies in the uncertainty and fuzziness of the concept itself. Some scholars have summarized it as "Essential Contestability" [12]. Mansbridge believes that public interest is a controversial concept in nature, and we can't know and determine the meaning of public interest, and people can't measure norms and make decisions accordingly [13]. The uncertainty of public interest makes it a powerful weapon for the group occupying the dominant position in society. It is easy to be controlled and defined by the elite groups of the society, which damages other social groups. Therefore, the public interest itself is controversial, which makes it difficult for legislation to formulate a specific application situation.

4.3. The Outlet of the Public Interest Authorization Mode

From the perspective of public law protection, more emphasis should be placed on limiting the excessive expansion of public power, and the regulation of relevant public power should also be incorporated into the legal rules of relevant public laws. Including how to judge that the purpose of regulation is really for national security, public welfare, national defense security, public environment and other social interests, and that the scope and degree of information collection and use should be limited, which needs to be justified. Promote the circulation of personal data from the perspective of public interest. As the object of public law protection, the digitized personal data should be aimed at improving the overall welfare of society and reflecting its characteristics of public interest.

In addition, pay attention to protecting citizens' spiritual and economic interests in personal information at the same time. In the past, China has always adhered to the unitary protection mode in legislation and judicature, that is, the protection of spiritual interests and economic interests can be realized simultaneously through the personality right system. For example, Article 1182 of the Civil Code stipulates that if personal information rights are infringed and property losses are caused, the infringer shall be required to make compensation according to the infringer's losses or the infringer's profits; Infringement of personal information rights and interests causes serious damage, and the infringed person has the right to claim compensation for mental damage.

In the process of case handling, three paths can be considered. First, weigh the interests. If it can be proved that the public interest in relevant cases is more important than the protection of personal data, it can be authorized. Second, analyze the interests. It is required to systematically analyze the specific benefits brought to the society and the public by authorizing relevant data. Third, reduce the damage. That is, when it is necessary to cause damage to citizens' interests, it should be minimized to the maximum extent.

5. Information Disclosure Mode

5.1. Application Scenarios of Information Disclosure Mode

The authorization modes of informed and consent mode and authorization of public interest mode are essentially aimed at non-public data. However, for public data, the right to obtain data and become the data controller is generally based on the government's initiative to disclose data, and the data subject will also actively disclose data. However, this is a kind of data processing behavior of the original data subject itself, which can be inferred to be the result predicted by the original data subject when it decides to disclose data, which actually belongs to another use of the informed and consent mode.

Disclosure data of the government. This kind of data can be divided into two types: the government's information related to the government that involves citizens and other reasons and can be made public, or other information obtained by the government through its administrative ability.

DOI: 10.54254/2753-7048/4/2022827

The disclosure of this kind of data is one of the ways for the government to perform its duties under the rule of law, and citizens can directly obtain the control right of the government's public data because of their right to obtain government information. According to Article 6 of the Regulations of the People's Republic of China on Disclosure of Government Information, the data information that the government should disclose is disclosed to the whole society, and the acquisition of such data control rights is also the increase and strengthening of the rights of data controllers.

5.2. The Dilemma of Information Disclosure Mode

The most obvious problem is that the related concepts are not clearly defined because most of the information disclosure models are based on the government's information disclosure. The legislative purpose of government information disclosure is to make use of publicity to ensure information transparency, strengthen the external supervision of administrative power, and protect the legitimate rights and interests of the public. Article 15 of the Regulations of the People's Republic of China on Disclosure of Government Information stipulates that "personal privacy" is an exception to the disclosure of government information, without specific scope and definition standards. Article 1032 and Article 1034 of the Civil Code respectively stipulate privacy and personal information, and explicitly put forward private information as an important part of privacy to protect. However, in China's practice, the recognition standards of privacy and information by administrative organs are not clear, and information disclosure review mechanisms are not complete.

5.3. The Outlet of the Information Disclosure Mode

In this process, pay attention to clarifying the exemption of government information disclosure, which means that when the internal information and process information in the information generated by the government during its administrative duties overlap with personal data, it should clarify the distinguishing rules. China can draw lessons from the rules of the definition of personal privacy and personal data in the United States and Japan, and make provisions on personal privacy information that should not be made public in the law and relevant judicial interpretations. Specifically, personal privacy information can be classified and enumerated in the law or regulation, which can be divided into the following four categories: citizen property, citizen health, citizenship and other information, so as to better safeguard citizens' personal privacy.

In judicial interpretation, the above four kinds of personal privacy are classified in detail. This way of summarizing, classifying and enumerating is based on identifiability, which comprehensively defines the specific scope of personal privacy information. Comprehensive coverage is conducive to clearly defining personal privacy, providing a clear legal basis, preventing the government and the courts from arbitrarily interpreting personal privacy, effectively avoiding the damage caused by improper disclosure of personal privacy by the government to the obligee, and preventing and alleviating the conflicts between citizens' right to know and personal privacy caused by unclear definition of personal privacy.

6. Conclusion

The conflict between personal data protection and international rule of law begins with the protection of personal information and ends with the dispute of national interests. The acquisition of personal data rights is even more important. As a production factor of rights, it directly leads to the dispute of regulation rights between countries and the dispute of personal information control rights between countries and enterprises. China should actively participate in the formulation of international rules. Therefore, the perfection of the domestic rule of law, the appropriate expansion of the extraterritorial effect of domestic laws and the Chinese voice in the formulation of international rules will all

DOI: 10.54254/2753-7048/4/2022827

contribute to the protection of digital sovereignty and the effective realization of national interests. As practice evolves, more ways of obtaining personal data rights may emerge, and this paper does not fully clarify all the dilemmas and solutions under the current model, but hopefully this paper will provide a bright perspective for the discussion.

References

[1] *Information Office of the Ministry of Commerce (2022) The working group on China's accession to the digital economic partnership agreement (DEPA) was formally established. Retrieved from http://www.mofcom.gov.cn/article/xwfb/xwrcxw/202208/20220803342152.shtml.*

[2] *Spiekermann, S., Acquisti, A., Boehme, R., Hui, Kai-Lung (2015) The challenges of personal data markets and privacy. Electronic markets, 2, 161-167.*

[3] *Morisawa, Y., Matsune, S. (2016) NESTGate - Realizing personal data protection with k-Anonymization technology. Fujitsu scientific & technical journal, 3, 37-42.*

[4] *OECD (2011), The Evolving Privacy Landscape: 30 Years After the OECD Privacy Guidelines. OECD Digital Economy Papers. Retrieved from https://read.oecd-ilibrary.org/science-and-technology/the-evolving-privacy-landscape-30-years-after-the-oecd-privacy-guidelines_5kgf09z90c31-en#page1.*

[5] *Zhang Xinbao (2019) Personal Information Collection: Limitations of Application of Informed and Consent Principle. Journal of Comparative Law, 6, 1-19.*

[6] *McDonald, Aleecia M., Cranor, Lorrie Faith (2008) The Cost of Reading Privacy Policies. A Journal of Law and Policy for the Information Society, 4, 543-568.*

[7] *AARONSON, S.A. (2021) Data is disruptive: How data sovereignty is challenging data governance. Retrieved from https://datagovhub.elliott.gwu.edu/2021/08/05/data-is-disruptive-how-data-sovereignty-is-challenging-data-governance/.*

[8] *AARONSON, S.A., Struett, T., Zable, A (2021) DataGovHub Paradigm for a Comprehensive approach to Data Governance. Retrieved from https://sites.tufts.edu/digitalplanet/files/2021/11/DataGovHub-Paradigm-for-a-Comprehensive-Approach-to-Data-Governance-Y1.pdf.*

[9] *Gao Fuping (2018) Personal Information Protection: From Personal Control to Social Control. Chinese Journal of Law, 3, 84-101.*

[10] *Huang Baiheng (2017) New "Personal Decision" and "Informed and Consent" in the Era of Big Data, Philosophical Analysis, 6, 101-111.*

[11] *Mittelstadt, Brent (2017) From Individual to Group Privacy in Big Data Analytics. Philosophy & Technology, 30, 475- 494.*

[12] *Stevens, Leslie Anne (2017) Public interest approach to data protection law: The meaning, value and utility of the public interest for research uses of data. Retrieved from https://era.ed.ac.uk/bitstream/handle/1842/25772/Stevens2017.pdf?sequence=2&isAllowed=y.*

[13] *Mansbridge, J., Macedo, S (2019) Populism and Democratic Theory. Annual Review of Law & Social Science, 15, 59-77.*