WEP Warwick Evans Publishing

International Journal of Social Sciences and Public Administration

ISSN: 3005-9836 (Print), ISSN: 3005-9585 (Online) | Volume 10, Number 6, Year 2026
DOI: https://doi.org/10.62051/ijsspa.v10n6.15
Journal homepage: https://ijsspa.org

Exploring the Boundaries of the Necessity Principle in the Personal Information Protection Law of the People's Republic of China

Junqi Meng

Shanghai University of Political Science and Law, Shanghai 201701, China

ABSTRACT

This paper focuses on the necessity principle in the Personal Information Protection Law of the People's Republic of China (hereinafter referred to as the PIPL), conducting a detailed analysis of its connotation, applicable scenarios and boundaries. Through research on relevant domestic and foreign legislation and practices, combined with specific case studies, it discusses the key role of the necessity principle in balancing personal information protection and rational utilization. The paper clarifies the application standards of the necessity principle in different situations, provides more precise guidance for the legal practice of personal information protection, and promotes the healthy development of the digital economy and the effective protection of personal information rights and interests.

KEYWORDS

Personal Information Protection Law; Necessity Principle; GDPR.

1. INTRODUCTION

With the rapid development of digital technology, the collection, use and sharing of personal information have become increasingly frequent. The promulgation of the PIPL has provided a solid legal framework for personal information protection. Among them, the necessity principle, as one of the core principles[1], is of great significance for regulating the behaviors of information processors and protecting personal information rights and interests. However, in practice, there are still many ambiguities in the specific application boundaries of the necessity principle, which makes it difficult for information processors to accurately grasp during operation and also brings challenges to personal information protection. Therefore, in-depth exploration of the boundaries of the necessity principle has urgent practical needs for improving the legal system of personal information protection and balancing the relationship between information protection and utilization.

2. OVERVIEW OF THE NECESSITY PRINCIPLE IN THE PIPL

2.1. Connotation of the Necessity Principle

The necessity principle emphasizes that when collecting and using personal information, information processors shall limit it to the minimum scope necessary to achieve specific purposes, and there shall be a reasonable correlation between the means adopted and the purposes[1]. This means that information processors shall not excessively collect personal information, and the collected information shall be directly related and indispensable to the realization of their business functions. For example, for a weather application whose core function is to provide weather information, it is

reasonable and necessary for it to collect the user's geographic location information to obtain local weather conditions. However, if the application also collects the user's browsing history, consumption records and other information unrelated to the weather service, it may violate the necessity principle.

2.2. Legislative Purposes of the Necessity Principle

2.2.1. Protecting Personal Information Rights and Interests

As mentioned above, the necessity principle can prevent the excessive collection and abuse of personal information by restricting the scope of collection and use of personal information by information processors, thereby protecting legitimate rights and interests such as personal privacy and human dignity. Excessive collection of personal information may lead to the leakage of personal privacy, exposing individuals to various risks such as fraud and harassment. Therefore, the necessity principle reduces such risks from the source and guarantees individuals' right to control their own information.

2.2.2. Promoting the Healthy Development of the Digital Economy

On the premise of ensuring the security of personal information, the necessity principle provides a certain space for information processors to rationally utilize personal information. Clear boundaries of the necessity principle help information processors give full play to the value of personal information on the basis of compliance and promote the innovative development of the digital economy. For example, enterprises can use limited personal information for precise marketing to improve operational efficiency while complying with the necessity principle, and also avoid legal risks caused by excessive information collection, which helps create a healthy development environment for the digital economy.

3. DOMESTIC AND FOREIGN LEGISLATION AND PRACTICE ON THE NECESSITY PRINCIPLE

3.1. EU General Data Protection Regulation (GDPR)

Although the GDPR does not explicitly mention the term necessity principle, it emphasizes that data processing shall follow the data minimization principle, which has a similar connotation to the necessity principle in China's PIPL. According to the data minimization principle, data controllers shall only collect the minimum amount of data relevant to the processing purpose, and data processing shall be appropriate, relevant and necessary for the purpose. For example, in the case between Google and the Spanish Data Protection Agency, the court held that when processing user data, Google should ensure that the scope of data processing is strictly limited to what is necessary to achieve its service functions; otherwise, it may constitute an infringement of users' data rights.

Article 4(2) of the GDPR introduces the necessity principle, requiring data processors to further process data only after meeting conditions such as legality and necessity. This principle emphasizes that data processing must directly serve legitimate purposes, and when achieving the same purpose, the method that has the least impact on personal rights shall be selected. In addition, the GDPR also requires that data processing must comply with the proportionality principle, that is, measures shall not exceed the necessary scope. For example, the necessity test under the GDPR requires steps such as factual assessment, purpose determination, impact assessment and consideration of the initial processing environment[2].

The necessity standard under the GDPR is usually associated with strict necessity, especially in scenarios involving national security or public interests[2]. Meanwhile, the necessity principle of the GDPR is closely related to Article 52(1) of the Charter of Fundamental Rights of the European Union and Article 8(2) of the European Convention on Human Rights[2].

3.2. California Consumer Privacy Act (CCPA) of the United States

Although the CCPA does not explicitly mention the necessity principle, its proportionality

principle stipulates that measures taken by the government or enterprises shall be limited to authorized priority objectives and shall minimize the impact on personal privacy and freedom[3]. This is similar to the necessity principle of the GDPR in some aspects, but it focuses more on reviewing the legality of government actions. At the same time, the consent mechanism of the CCPA requires enterprises to obtain explicit consent from users before processing personal data. This is similar to the purpose limitation principle of the GDPR, but it highlights the protection of users' control rights[4].

3.3. China's Personal Information Protection Law

China's PIPL draws on the necessity principle of the GDPR, but its scope of application and interpretation standards are different. For example, the PIPL adopts the target subject standard in terms of extraterritorial effect, that is, if a data processing activity is directed at data subjects within the territory of China, the PIPL shall apply[5]. In addition, China also emphasizes the adequacy decision mechanism in cross-border data flow to ensure that data transmission meets international standards[6]. However, there are still some deficiencies in China's data protection legislation, such as the lack of a dedicated personal data protection authority and imperfect cross-border data flow rules[7].

In addition to the PIPL, laws and regulations such as the Cybersecurity Law of the People's Republic of China and the Civil Code of the People's Republic of China also contain provisions on personal information protection, some of which embody the spirit of the necessity principle. For example, the Cybersecurity Law stipulates that network operators shall follow the principles of legality, legitimacy and necessity when collecting and using personal information, publicly disclose the rules for collection and use, clearly state the purpose, method and scope of information collection and use, and obtain the consent of the collected persons[8]. These provisions provide a legal basis for the application of the necessity principle in different fields.

3.4. International Comparison and Trends

From an international comparison perspective, the necessity principle of the GDPR has a strong influence in the field of data protection, especially in cross-border data processing between EU member states and non-EU countries. For example, the extraterritorial effect of the GDPR applies not only to enterprises within the EU but also to non-EU enterprises, as long as their data processing activities affect individuals within the EU[9], they shall be subject to the jurisdiction of the GDPR. In contrast, U.S. privacy laws such as the CCPA mainly apply to consumers within the United States, with weaker extraterritorial effect[4].

While drawing on the experience of the GDPR, China is also exploring a data protection model suitable for its national conditions. For example, China is strengthening the supervision of cross-border data flow and promoting data protection cooperation with the EU and other countries and regions. In addition, China is also exploring the establishment of a class action mechanism for personal information protection to enhance individuals' ability to seek remedies in data protection[4].

Although relevant domestic and foreign laws have different definitions of the necessity principle, they all emphasize the need to balance personal rights and public interests in data processing. The necessity principle of the GDPR is relatively strict, emphasizing minimal intervention and proportionality review, while relevant laws in the United States and China differ in scope of application and interpretation standards.

4. APPLICATION ANALYSIS OF THE NECESSITY PRINCIPLE IN DIFFERENT SCENARIOS

4.1. Internet Application (APP) Scenario

4.1.1. Relationship between Function Realization and Information Collection

When designing applications, APP developers need to clarify their core functions and determine the scope of personal information to be collected based on the core functions. For example, for an online shopping APP, it is necessary to collect the user's name, delivery address, contact information and other information to complete commodity transactions. However, if the APP compulsorily requires access to the user's camera and microphone permissions during registration, and these permissions are not directly related to the shopping function, it may violate the necessity principle.

4.1.2. Personalized Recommendation and the Necessity Principle

Personalized recommendation is one of the common functions of APPs. When conducting personalized recommendations, information processors usually collect information such as users' browsing history and search records. However, such collection shall also follow the necessity principle. For example, when providing personalized commodity recommendations for users, e-commerce platforms shall only collect information related to commodity preferences and avoid excessive collection of other irrelevant information of users. At the same time, users shall be given sufficient control rights, such as allowing users to choose whether to accept personalized recommendations and requiring transparency of recommendation algorithms, so that users can understand the source and basis of recommended information.

4.2. Enterprise Data Processing Scenario

4.2.1. Necessity of Information Collection for Enterprise Operation

In the process of operation, enterprises need to collect and use certain personal information for the purposes of carrying out business and managing employees. For example, enterprises need to collect employees' bank account information to pay salaries; they need to collect employees' basic personal information, work experience and other information for human resource management. However, enterprises shall ensure that the collected information is necessary for carrying out business and avoid excessive collection. For example, in the recruitment process, enterprises shall not collect personal sensitive information unrelated to the job position, such as employees' constellations and emotional status.

4.2.2. Data Sharing and the Necessity Principle

Data sharing among enterprises is becoming increasingly common, and the necessity principle shall also be followed when conducting data sharing. For example, if Enterprise A shares user information with its partner Enterprise B, it shall ensure that the shared information is necessary for Enterprise B to achieve specific cooperation purposes. At the same time, Enterprise A shall clearly inform users of the purpose of data sharing, the recipient and the scope of shared information, and obtain the user's consent. If Enterprise A shares all user information with Enterprise B without restriction, while Enterprise B only needs part of the information to complete the cooperation, then Enterprise A's behavior may violate the necessity principle.

4.3. Government Department Data Processing Scenario

4.3.1. Limits of Information Collection for Public Administration

When performing public administration duties, government departments need to collect and use a large amount of personal information. For example, public security organs may collect citizens'

identity information, travel records and other information to maintain social order. However, information collection by government departments shall also be restricted by the necessity principle. Government departments shall clarify that the purpose of information collection is to achieve public administration objectives, and the collected information shall be limited to the minimum scope necessary to achieve such objectives. For example, during the COVID-19 pandemic, government departments collected residents' travel information to track the spread of the epidemic, but such information shall be deleted in a timely manner after the epidemic ends to avoid excessive retention of information.

4.3.2. Data Security and the Necessity Principle

Government departments hold a large amount of sensitive personal information, and data security is crucial. Following the necessity principle helps reduce the risk of data leakage. When storing and using personal information, government departments shall ensure that the security measures adopted are appropriate to the sensitivity of the information and the processing purpose. For example, for highly sensitive personal information involving national security, stricter security protection measures shall be taken, and the scope of access and use of information shall be strictly limited, only allowing specific personnel to access for necessary purposes.

5. CASE ANALYSIS IN THE APP FIELD: TAKING EXCESSIVE COLLECTION OF PERSONAL INFORMATION BY INPUT METHOD APPS AS AN EXAMPLE

Taking APPs such as iFlytek Input Method as examples, they were once notified by the Cyberspace Administration of China (CAC) for violating the necessity principle and collecting personal information unrelated to the services they provided. On May 1, 2021, the CAC notified the illegal collection and use of personal information by 33 APPs, among which iFlytek Input Method was prominently listed[10]. During the user's use of the APP, there was excessive collection of personal information, including a large amount of information unrelated to the basic business functions of the input method, such as the user's address book information, call records and SMS records. From the perspective of necessity, the core function of an input method is to provide text input services for users, and the collected information has no direct correlation with the text input function and is not necessary to realize the basic business functions of the input method. Collecting address book information cannot directly improve the input efficiency or accuracy of the input method, nor can it provide users with a better text input experience. Such behavior obviously exceeds the scope allowed by the necessity principle.

The PIPL clearly stipulates that personal information processors shall limit the collection of personal information to the minimum scope necessary to achieve the processing purpose and shall not excessively collect personal information. iFlytek Input Method's collection of personal information unrelated to its services obviously does not comply with this provision, and there is a lack of reasonable correlation between its processing purpose and the scope of information collection. From the perspective of processing purpose, the main purpose of the input method is to provide text input services, and collecting information such as address books cannot directly serve this purpose, nor can it bring practical benefits related to text input to users. From the perspective of information collection scope, iFlytek Input Method exceeded the minimum scope necessary to realize the text input function and excessively collected users' sensitive personal information, seriously infringing upon users' personal information rights and interests.

Such violations of the necessity principle have triggered a series of adverse consequences. At the legal level, according to the relevant provisions of the PIPL, APP operators who collect personal information in violation of the necessity principle may face administrative penalties such as ordering rectification, warning and fines. In the case of iFlytek Input Method, it was removed from major App

stores for rectification due to illegal collection of personal information. This not only brought direct economic losses to the APP operator, such as user loss and market share decline during the period of being removed from the shelves, but also damaged the enterprise's reputation and image and reduced users' trust in it. For users, excessive collection of personal information has greatly increased the risk of privacy leakage, and they may suffer from adverse consequences such as harassing calls, spam messages and fraud, posing a serious threat to users' life and property safety. After the user's address book information is leaked, it may be used by criminals for fraud activities, causing economic losses to users and their relatives and friends.

6. DETERMINANTS OF THE BOUNDARIES OF THE NECESSITY PRINCIPLE

6.1. Purpose of Information Processing

6.1.1. Clarity of Purpose

Information processors must clarify the purpose of collecting and using personal information, and such purpose shall be legal and legitimate. For example, enterprises shall not arbitrarily collect user information under the vague purpose of improving user experience. The clarity of purpose helps determine whether the scope and method of information collection are necessary. If the purpose is unclear, it is difficult to judge whether the collected information is relevant and indispensable to the purpose.

6.1.2. Stability of Purpose

The purpose of information processing shall be relatively stable and shall not be changed arbitrarily. Once an information processor has determined the purpose of information processing and collected personal information based on it, it shall not change the purpose without the user's consent to expand the scope of information collection and use. For example, if an APP developer informs users during registration that information is collected to provide a specific service, it shall not use such information for other commercial purposes without the user's consent afterwards.

6.2. Nature and Sensitivity of Information

6.2.1. Distinction between General Information and Sensitive Information

For general personal information such as name and gender, information processors can collect and use it relatively easily on the premise of meeting the necessity principle. However, for sensitive personal information such as biometric information and religious beliefs, since it involves the core rights and interests of individuals, information processors shall be subject to stricter restrictions when collecting and using it. For example, sensitive personal information can only be collected and used when there is a clear legal basis and for the purpose of achieving specific major public interests.

6.2.2. Protection Standards for Sensitive Information

For sensitive personal information, the application of the necessity principle requires higher protection standards. Information processors not only need to prove that the collection and use of sensitive information is necessary to achieve specific purposes, but also take stricter security protection measures, such as encrypted storage, access control and anonymized use, to prevent the leakage and abuse of sensitive information.

6.3. Industry Practice and Technical Feasibility

6.3.1. Reference Value of Industry Practice

Different industries have different characteristics and needs for the collection and use of personal information. Therefore, when determining the boundaries of the necessity principle, industry practices can be referred to. For example, the financial industry has strict norms and processes for the collection and use of customer personal information due to the involvement of capital security. When judging whether the information processing behavior of a financial institution complies with the necessity principle, the industry practices and regulatory requirements of the financial industry can be referred to. However, industry practice cannot be used as the sole criterion for judgment, and comprehensive analysis shall be conducted in combination with legal provisions and specific circumstances.

6.3.2. Consideration of Technical Feasibility

With the continuous development of technology, information processors can adopt more advanced technical means to achieve information processing purposes while reducing the collection and use of personal information. For example, in terms of identity verification, traditional methods may need to collect sensitive information such as users' ID numbers, but now biometric technologies such as face recognition and fingerprint recognition can achieve safer and more convenient identity verification, and to a certain extent, reduce the collection of other unnecessary information. Therefore, when determining the boundaries of the necessity principle, technical feasibility shall be considered, and information processors shall be encouraged to adopt advanced technical means to optimize information processing behaviors and reduce dependence on personal information.

7. CHALLENGES AND COUNTERMEASURES IN THE APPLICATION OF THE NECESSITY PRINCIPLE

7.1. Challenges in the Application of the Necessity Principle

7.1.1. Subjectivity of Purpose Interpretation

In practice, information processors may have subjective interpretations of the purpose of information processing. Different information processors may have different understandings of the purpose of the same business function, leading to differences in the judgment of the scope of necessary information collection. For example, for a social APP, developers may believe that collecting users' geographic location information is to provide a better social experience, such as finding people nearby, but users may think that this is not necessary information for social functions. This subjectivity of purpose interpretation brings difficulties to the accurate application of the necessity principle.

7.1.2. Uncertainty Brought by Technological Development

With the rapid development of emerging technologies such as artificial intelligence and big data analysis, the methods and scenarios of information processing have become more complex. New technologies may bring new demands for information collection and use, making the application of the necessity principle face uncertainty. For example, artificial intelligence algorithms may require a large amount of data to improve accuracy during training. This requires clarifying under what circumstances the collection and use of such data comply with the necessity principle and how to balance the relationship between algorithm performance and personal information protection.

7.1.3. Dilemma of User Cognition and Consent

In actual operation, users often cannot truly understand the purpose, scope and method of personal information collection and use by information processors, leading to the notice-and-consent mechanism being formalized to a certain extent. The privacy policies provided by information

processors are usually lengthy and complex, making it difficult for users to read and understand the meaning word by word. In addition, in order to use certain services, users often have to click to agree to the privacy policy even if they have doubts about the terms. This dilemma of user cognition and consent hinders the implementation of the necessity principle in practice.

7.2. Countermeasures

7.2.1. Clarifying Standards for Purpose Interpretation

Legislative and regulatory authorities shall formulate clear standards for purpose interpretation and standardize the expression and interpretation of information processing purposes by information processors. They can clarify the core purposes of different types of business functions and the corresponding scope of necessary information collection by formulating industry guidelines or judicial interpretations. At the same time, an approval mechanism for purpose changes shall be established, requiring information processors to file with the regulatory authorities and obtain explicit consent from users when changing the purpose of information processing.

7.2.2. Strengthening Technical Supervision and Guidance

Regulatory authorities shall strengthen the supervision of the application of new technologies in personal information processing and formulate corresponding technical specifications and standards. For example, for the data use of artificial intelligence algorithms, algorithm developers shall be required to disclose the basic principles of algorithms and data usage to ensure that the collection of training data for algorithms complies with the necessity principle. At the same time, scientific research institutions and enterprises shall be encouraged to carry out research and development of personal information protection technologies and promote technological innovation to better balance technological development and personal information protection.

7.2.3. Optimizing the User Notice-and-Consent Mechanism

Information processors shall optimize the presentation of privacy policies and explain the purpose, scope and method of information processing to users in concise, clear and easy-to-understand language. They can help users better understand through forms such as visual charts and animations. In addition, a layered consent mechanism shall be adopted to classify different types of information collection and use behaviors, allowing users to choose whether to agree separately and improving users' control over personal information processing. Meanwhile, regulatory authorities shall strengthen the review of the compliance of information processors' privacy policies to ensure that users can truly understand and make independent consent decisions.

8. CONCLUSION

The necessity principle in the PIPL is a key criterion for balancing personal information protection and rational utilization. Through in-depth analysis of its connotation, domestic and foreign legislation and practice, application in different scenarios and determinants of boundaries, we recognize the importance of the necessity principle in the field of personal information protection. However, in practice, the application of the necessity principle faces many challenges, which need to be addressed from aspects such as clarifying standards for purpose interpretation, strengthening technical supervision and guidance, and optimizing the user notice-and-consent mechanism. Only by accurately grasping the boundaries of the necessity principle can we promote the healthy development of the digital economy while protecting personal information rights and interests, and achieve a win-win situation between personal information protection and rational information utilization. In the future, with the continuous development of digital technology and changes in personal information protection needs, we need to continue to pay attention to the application of the necessity principle and

constantly improve relevant legal systems and practical operations to adapt to new challenges and opportunities.

REFERENCES

[1] Personal Information Protection Law of the People's Republic of China. (2021).

[2] Jasserand, C. (2018). Subsequent use of GDPR data for a law enforcement purpose: The forgotten principle of purpose limitation? *European Data Protection Law Review*, 4(2), 152–167. https://doi.org/10.21552/edpl/2018/2/6

[3] Dimović, Z. (n.d.). Analysing the EU data privacy implications resulting from Executive Order 14086: A legal perspective. *LeXonomica*.

[4] Wei, S. Y. (2019). A comparative study of CCPA and GDPR: Trends and paths of U.S. personal information protection legislation. *Cyberspace Security*, 10(4).

[5] Tian, X. P. (2023). Extraterritorial effect of the EU GDPR: Jurisdictional basis, implementation path, institutional effect and enlightenment. *Chinese Journal of International Economic Law*, (1).

[6] Chen, D. Z. (2021). The impact of the EU General Data Protection Regulation on international service trade rules. *China Business and Market*, 35(4).

[7] Han, J. M. (2019). The latest development of EU and UK personal data protection laws and its enlightenment to China's legislation [Master's thesis]. Beijing Foreign Studies University.

[8] Cybersecurity Law of the People's Republic of China. (2017).

[9] Chen, Y. M., & Wu, C. C. (2022). Deconstruction of the extraterritorial application conditions of the EU General Data Protection Regulation. *German Studies*, 39(1).

[10] Xinhua News Agency. (2021, May 1). These 33 apps illegally collect and use personal information! See if you are affected? Xinhuanet. http://www.xinhuanet.com/2021-05/01/c_1127400770.htm