Proceedings of the International Conference on Social Psychology and Humanity Studies
DOI: 10.54254/2753-7048/10/20230195

Legislative Conception for the Special Protection of Biometric Information: A Study Based on Extraterritorial Experience

Ruoxue Ma[1,a,*]

[1]*Beijing Normal University, No.19, Xinjiekouwai Street, Beitaipingzhuang Street, Haidian District, Beijing, 100875, China*
a. maruoxue20011225@163.com
**corresponding author*

Abstract: In present society, where digital technology is widely used, biometric information is extensively applied to public security, social governance, finance and etc. Considering that biometric information, one of the most identifiable identifiers, has the characteristics of irreplaceability, immutability, and uniqueness, special legislative protection of biometric information is required. This paper uses case study, comparative research and regulatory research methods. It selects the definition, collection rules and processing rules of biometric information, which are mainly analysed in the United States, as studying points. Compared with Illinois Biometric Information Privacy Act, provisions of China Personal Information Protection Law on the processing rules of biometric information are more detailed and specific, but lack of a clear definition of biometric information and a clear exposition for informed consent, partial exemptions, and the principles of legality, legitimacy and necessity. There is still room for improvement in the refinement of the system and the practical implementation.

Keywords: biometric information, extraterritorial experience, comprehensive legislation, normative system

1. Introduction

Since the beginning of the Aadhaar Case in 2012, discussions on the privacy protection of biometric information began among scholars from various countries. The Aadhaar Project in India established the Unique Identification Authority of India (UIDAI) and the world's largest biometric information database was founded to provide universal identity to every Indian resident. However, since the implementation of UIDAI, there has been many controversies, such as some scholars considering the possibility of identification anxiety and the threat to national security which may cause by this project [1,2].

In China, the "First Case of Face Recognition" has gradually brought the protection of biometric information represented by face recognition into the public view. In recent years, this issue has also been widely discussed in the academic community. On October 28, 2019, Guo Bing, a professor at Zhejiang Sci-Tech University, filed a lawsuit with the Hangzhou Fuyang District People's Court on the grounds that Hangzhou Wildlife World had collected his biometric information such as facial features without prior consultation or consent. As soon as the case was accepted for processing, it was widely reported by media, and the issue about the rules for the collection and processing of facial

DOI: 10.54254/2753-7048/10/20230195

recognition information involved in the case also aroused continuous social concern. The case was finally heard by two trials, and both courts affirmed that the information subject have the right to erasure. However, it is regrettable that the courts of both instances considered and positioned the focus of the dispute in this case based on the framework of a breach of contract, but did not affirm the right attribute of the right to personal biometric information, or even personal information, of information subjects [3]. In addition, the second instance judgment of this case was pronounced when the Personal Information Protection Law was about to be promulgated, this means that the judgment of this case has considerable influence on the judicial process of personal information protection. Although the court affirmed the special characteristics of biometric information compared with other personal information, and explicitly required special protection for biometric information such as facial information and fingerprint information, at the same time it affirmed the necessity of the defendant's information collection of facial information itself, which was considered to be an overly broad interpretation of the principles of legality, legitimacy and necessity [4].

On August 20, 2021, China's first special legislation on personal information protection, the Personal Information Protection Law (PIPL), was officially promulgated. This law includes biometric information within the framework of sensitive personal information to implement special protection, but outside of this law, only a small number of rules deal with special protection of biometric information. Compared with the protection of biometric information of European Union and the United States, there are still great potentials for improvement in China's legislation. In addition, the PIPL does not clarify the definition of biometric information, and the boundary of the right to biometric information is not clear. Therefore, this article will mainly discuss the collection and processing of information which are the two most critical links to avoid information leakage through a comparative study of biometric information privacy legislation in the United States and try to clarify the scope of protection by clarifying the definition of biometric information.

2. The Definition of Biometric Information

2.1. The Essentiality of Defining Biometric Information

Compared to other sensitive personal information, biometric information is particularly special. It can reflect the unique and irreplaceable physical, physiological or behavioural characteristics of a natural person, such as appearance, fingerprints, gait, etc. Except in rare cases, such as identical twins with the same genes, with the help of related technologies, others can directly and accurately identify a natural person. Therefore, compared with other sensitive information, the leakage of biometric information will bring greater security risks to the information subject, which requires stricter legal protection.

In order to clarify the scope of protection of biometric information, the definition of biometric information should first be clarified to distinguish it from other personal information, especially information that is prone to confusion such as medical and health information. China's PIPL includes biometric information in the framework of sensitive information for special protection, but unfortunately does not clarify the definition of biometric information. At present, there is no unified definition of biometric information in Chinese legislation, and the relevant concepts are mainly scattered in judicial interpretations, local regulations and national standards, which makes the judicial authorities have great limitations in the application of law [5]. All in all, a clear definition of biometric information in the PIPL is essential.

2.2. Examination of the Definition of EU and US Legislation

Article 4 of the General Data Protection Regulation (GDPR) sets up a special provision to define biometric information, uses the term biometric data, and adopts the definition model of "summary +

DOI: 10.54254/2753-7048/10/20230195

enumeration". The definition emphasizes the purpose of identification (allow or confirm the unique identification of that natural person), the content of identification (physical, physiological or behavioural characteristics), and the technical theory (specific technical processing). Recital 51 points out that through the purpose of identification and technical theory, biometric information can be effectively distinguished from medical data, health data and captured raw data such as images and audio. Like the PIPL, Article IX of the GDPR places biometric information in a special category of personal data. However, it is notable that unlike most of the definitions in China, the GDPR separates biometric information and genetic information, reflecting the GDPR's strict legislative attitude.

Table 1: Category of the legislative model of the definitions of biometric information in the United States.

	National Biometric Information Privacy Act NBIPA	**Biometric Information Privacy Act (Illinois) BIPA**	**Capture or Use of Biometric Identifiers (Texas) CUBI**	**Biometric Privacy Act (Washington); Consumer Data Protection Act (Virginia) WBPA, CDPA**	**California Consumer Privacy Act; California Privacy Rights Act CCPA, CPRA**	**Consumer Online Privacy Rights Act COPRA**	**Consumer Data Privacy and Security Act of 2020 CDPSA**
Patterns of the Definition	Enumeration + exclusion	Summary + Enumeration + exclusion	Enumeration	Summary + Enumeration + exclusion	Summary + Enumeration	Summary + Enumeration + exclusion	Summary
Methods of the Definition	—	Technical theory + identification content + identification purpose	—	Technical theory + identification content + identification purpose	Identification content + identification method (alone or in combination) + identification purpose	Identification content + technical theory (Not require identification of a specific individual)	Technical theory + identification content + identification purpose
The way to enumerate	Exhaustive enumeration	Exhaustive enumeration	Exhaustive enumeration	Incomplete enumeration	Incomplete enumeration	Incomplete enumeration	—
Whether specific information is explicitly enumerated	NO	NO	NO	NO	YES (DNA, vein patterns, keystroke habits, gait, and sleep, health, and exercise data with identifying information)	YES (DNA and gait)	NO

DOI: 10.54254/2753-7048/10/20230195

Table 1: (continued).

Excluded information	**Original samples, body descriptions, organ donation transplants, healthcare data, and anatomical images**	**Original samples, body descriptions, organ donation transplants, biomaterials, healthcare data, and anatomical images**	—	**Raw data and healthcare data**	—	**Raw samples that are not used to identify the unique characteristics of an individual**	—

There are three main names for biometric information in U.S. legislation, biometric identifier, biometric information and biometric data. Among them, the connotation of biometric identifier was specifically explained in the case of Rivera v. Google Inc. Unlike the latter two, a biometric identifier is "a set of measurements" used to identify a person's prescribed physical components, while the latter "is a conversion of those measurements into a different, useable form". As shown in the figure above, the United State federal and state governments mainly use enumeration to define biometric information, and distinguish biometric information from other information such as raw data, medical and health information, etc. by summary or exclusion. Similar to China legislation, the legislation of the United State also does not agree on what exactly biometric information contains.

Combined with the above, the legislation of the European Union and the United States both believe that the identification content of biometric information is the physiological, physical or behavioural characteristics of the human body, and most of them recognize individual identification methods and require the identification of specific individuals. However, there are certain differences in the method of the definition, the summary and the types of enumeration. The EU adopts a pattern of "summary + enumeration" to defining biometric information, while the US prefers to adopt a pattern of "summary + enumeration + exclusion". For the technical theory in the summary, the European Union adopts the expression "specific technical processing" to emphasize the non-originality of the data, while the US adopts the expression "measurement" or "scanning" to emphasize the acquisition of data; For identification content, the EU excludes genetic information, but some US legislation also lists human characteristics such as DNA and genes. In addition, the EU lists only two common and widely used biometric information, while the US prefers to include all types of biometric information as much as possible.

2.3. Choice of China's Legislative Model

At present, most of the few legislation examples in China that define biometric information adopt the pattern of "summary + enumeration". Summary can illustrate the abstract definition of biometric information and indicate the elements that constitute something, but it is too abstract and not conducive to judicial application. Enumeration can directly enumerate the types of biometric information one by one, but this approach lacks interpretative flexibility. Exclusionary enumeration can clearly distinguish biometric information from other confusing categories of information, but there is also the possibility of vulnerabilities in this pattern. Considering all above, it is best to define biometric information by listing common types of biometric information and excluding the types of confusing information. Among them, the summary definition of biometric information shall include

DOI: 10.54254/2753-7048/10/20230195

four elements: identification purpose, identification content, identification method and technical theory. In summary, the definition of biometric information should be expressed like: information obtained by processing the unique biological characteristics of a natural person, such as physiology, body or behaviour, through a specific technology, and can confirm the identity of a specific natural person alone or in combination with other identifiable information.

3. Rules for the Collection of Biometric Information

The collection rules of personal information, especially biometric information, mainly contains informed consent, exemption, express terms and principle of minimum necessary restriction. Among those rules, the first two are the most important, and the others are also slightly reflected in the first two rules. Hence, this article will discuss informed consent and exemptions in the collection of biometric information in detail.

3.1. Informed Consent

During the process of collecting the biometric information, the information right framework is constructed with informed consent as the core, and thus constitutes the legal basis for the information processor or controller to collect the biometric information. Informed consent includes the right to know and the right to consent, and knowing is the basis of consent. The right to know in the collection of biometric information is often only reflected in the knowing of the content and purpose of collection, but consent is often the most visible provision of legal protection for information collection. To understand the "consent" under personal information protection, clarifying the attribute of the information right is the most important task.

The right to personal information was initially negatively understood as "leave my right alone", then transformed into "self-control of personal information" and further transformed into "self-determined autonomy" in modern times [6]. In the network information society, the negative defence mode of the original traditional personality rights theory has long been unable to meet the requirements of the protection and use of personal information, and it is difficult for individuals as information subjects to fully control all their information, but in most cases, personal information fragments are controlled by various institutions and organizations. Therefore, under the framework of modern privacy, the essence of "consent" under personal information protection should be understood as the right of informational self-determination, that is, the information subject independently decides whether his information can be collected and processed as the essential connotation of consent.

Taking the special nature of biometric information into account, there should be stricter standards and procedures for informed consent of biometric information compared to other categories of personal information. The principle of informed consent established by PIPL for sensitive information is separate and written when necessary. However, in practice, it often occurs the condition that users consent to the collection of their biometric information by clicking a button to agree a general Privacy Shield Agreement. Despite the specific provisions of the privacy policy for biometric information in the agreement, few users would like to open the link and read the entire content of the agreement, and the informed consent for biometric information collection is effectively lost. In order to ensure the materiality of the information subject's right to know and right to consent, according to Article 15(b), BIPA in the United States adopts a "mutual-expressed written consent" mechanism: on the one hand, private entities need to inform the information subject or their statutory agent in writing of the content, specific purpose and duration of information collected or stored; On the other hand, private entities are also required to receive a written disclaimer signed by the information subject oregal authorized representative. In addition, from the perspective of terminology, BIPA's description of consent

DOI: 10.54254/2753-7048/10/20230195

emphasizes the notification of the dynamic operation of "scanning", so that the information subject can more intuitively feel how the information is collected, what it will be used for after collection, and how long it will be used. Combining the two aspects above, BIPA strictly regulates the collection mechanism of biometric information by private entities in terms of content and form. However, in China, due to the widespread application of facial recognition, face payment and other technologies, although this strict "mutual express written consent" mechanism has certain reference significance, direct application will inevitably lead to increased costs for enterprises, user loss and other problems. Excessive protection of the right to personal information should not be an obstacle to data utilization and industrial development [7].

In order to seek a more protective consent mechanism, many scholars have begun to discuss dynamic consent mechanisms under the topic of face recognition in recent years. The advantage of this mechanism is that it can solve the current problem of excessive formality of rights protection, but at the same time this mechanism requires repeated consent or withdrawal by users, and faces problems such as low efficiency and poor user experience. In addition, the industry has also begun to explore technical application specifications. For example, Alipay took the lead in formulating the "General Rules for Biometric Technology" separately in an attempt to achieve better rights protection. Although the content of this general rule is still crude and its protective role is debatable, this kind of strengthening the protection of rights through industry norms is a good way to generalize.

3.2. Exemptions

Generally, the processing of personal biometric information requires the consent of the information subject, and only in rare cases can the information be collected without the consent of the information subject. The PIPL mainly provides for six exceptions in its general provisions, including a miscellaneous provision. Other five situations are: it is necessary to conclude a contract, perform statutory duties or legal obligations, respond to public-health emergency or other emergencies for the purpose of protecting life, health and property safety, news reporting or public opinion supervision for the purpose of public interest, and personal information that has been disclosed. Compared to the PIPL, BIPA article 15(d) is more conservative and provides only three situations: disclosure for the purpose of fulfilling a financial transaction, legal requirements, and court search warrants or subpoenas requests. In contrast, it can be seen that BIPA has a stricter attitude towards the application of biometric information, especially in the context of public health events and public opinion surveillance. Moreover, the terms of BIPA are more direct and specific, and there is no legal concept that needs to be further defined. For example, how to define the purpose of public interest has not only been one of the concepts that need to be discussed in detail in court judgments, but also been a problem in domestic academic circles which has never been agreed, and the definition of this concept is slightly different in different legislative contexts. This distinction in legislative attitudes is influenced by the scope and frequency of application of biometric information, as depicted in BIPA article 5 (d), when biometric information is closely linked to other personal information and finances, people have a negative attitude towards its use. However, in China, biometric information is widely used in common fields such as payment, identification, information verification, and financial accounts. Especially during the epidemic, biometric information is widely used in the government's epidemic prevention behaviour.

In addition to the above provisions, China's restrictions on the rules for the collection of biometric information are also found in the Information Security Technology: Personal Information Security Specification (GB/T 35273-2020). This guideline prohibits the storage of biometric information in principle, and further clarifies that PIPL specifies the minimum necessary and strict protective measures for the collection of biometric information (e.g., minimum standards of confidentiality technology required during the collection and storage process). However, as a normative document

DOI: 10.54254/2753-7048/10/20230195

regulating the processing behaviour of information processors, the guideline provides a weak protection for biometric information. It has no remedy measures, and its effectiveness level is low. Hence, it requires the cooperation of other government departments and regulatory authorities to improve its implementation effectiveness.

4. Rules for the Processing of Biometric Information

The term "processing" as used herein differs from the meaning of "processing" in PIPL, so that a special explanation is necessary here. According to Article 4, "processing" in PIPL includes the collection, storage, use, processing, transmission, provision, disclosure, deletion, etc. of personal information, but the processing rules discussed here refer to the application of personal information, including use, transmission, processing, storage, etc., and do not include collection.

BIPA and PIPL take a particularly different legislative approach to the processing of biometric information. BIPA does not directly prescribe the processing principles of biometric information, but it achieves protection purposes by strictly restricting the storage and use of biometric information by private entities. The processing rules of biometric information include the rights and obligations of information processors and the rights and obligations of information subjects, but this article mainly focuses on the legal protection of biometric information, so the three most important rules are selected: the principles of legality, legitimacy and necessity, security responsibility and transparency.

4.1. The Principles of Legality, Legitimacy and Necessity

Article 4 of the PIPL sets out the principles of legality, legitimacy and necessity. This clause is general, i.e. this processing principle applies to all processing of personal information. BIPA does not directly stipulate the legal principles that private entities need to comply with when processing biometric information, and this provision of PIPL is more similar to the three principles of legality, fairness and transparency, purpose limitation and data minimization in the GDPR.

Similar to the legality of the GDPR, PIPL requires that the processing of personal information has a legal basis, but the specific legality situations are slightly different. Both provide for the consent of the information subject, the performance of the contract, the performance of legal obligations, and the protection of public and important interests. The GDPR provides data controllers with a defence in this situation which is that the processing has overriding legitimate grounds, but unlike the GDPR, the PIPL does not affirm the priority interests of the controller, even if such interests need to be analysed on a case-by-case basis under the GDPR to determine whether they have sufficient priority [8].

The PIPL's legitimacy principle mainly but not exclusively corresponds to the purpose limitation principle of the GDPR. The purpose limitations of the GDPR include that personal information is processed only for specific purposes and must not be processed beyond the purposes originally agreed with the data subject, unless consent has been obtained from the information subject [9]. However, the PIPL principle of legitimacy not only requires that the purpose of personal information processing is specific and clear, but also requires that the purpose of processing is reasonable, that is, it should be in the public interest and legitimate private interests [10]. The purpose of processing cannot only comply with the provisions of the law. If there is a lack of certain reasonableness, in the society of informationization where the scope and frequency of personal information processing are expanding, the effect of information application and the protection of personal information cannot be well realized.

The word "necessary" is common in the rules for the processing of personal information. As specified in Article 5 of the GDPR, the data shall be limited to the extent necessary for the purposes for which it is processed. There is no consensus on the meaning of the necessary principles of PIPL,

DOI: 10.54254/2753-7048/10/20230195

but most agree that the use of data and the impact on individual rights and interests should be minimized.

4.2. Security Responsibility of Private Entities

Article 7 of the PIPL makes transparency a principle for the processing of personal information and stipulates the purpose, method and scope of the processing that needs to be specified. Article 17 further stipulates this principle, that the information processor needs to inform the information subject truthfully, accurately and completely of its basic information, the purpose of processing, the processing method, the type of information processed and the retention period, as well as the methods and procedures for the information subject to exercise its rights, in a conspicuous manner and clear and easy-to-understand language. In contrast, BIPA does not explicitly require the information subject to be informed of the manner and procedure for exercising his rights, but Article 15(a) stipulates that the relevant private entity needs to establish a plan and guidelines for data retention and destruction, and the private entity must strictly comply with this plan and guidance. Unfortunately, although the GB/T 35273-2020 clearly stipulates that when the retention period for biometric information has expired, the information processor needs to take procedures and safeguards to deal with the information, it does not include any procedures or measures within the scope of disclosure. This provision is too specific to be included in the PIPL, but it could be considered as an industry norm. Information processors do not need to explain to the information subject in a professional and detailed manner all the contents of the specific destruction procedures or measures they have taken, but only inform them of what procedures and measures they will take and what effects the procedures and measures will achieve, which can not only enhance the supervision of the information controller, but also enhance the trust of the information subject.

4.3. Transparency

According to the provisions of the Article 51 and 57 of the PIPL, personal information processors have the obligation to ensure the security of the biometric information they process and to take security remedial measures when damage occurs or may occur. However, due to the particularity of biometric information, it is difficult to say that the security remedial measures that the information processor can take are truly effective unless timely measures are taken to stop the damage before it occurs. From this point of view, about the security liability rules of biometric information processors, the norms of their security obligations need to be paid more attention, and higher security protection standards should be adopted. For example, Article 15(e) of BIPA stipulates that private entities should protect biometric information with standards equivalent to the protection of other confidential and sensitive information, and encourages the adoption of higher standards of protection. Similarly, PIPL includes biometric information in the category of sensitive personal information, stipulates higher protection standards for sensitive information, and specifies the protection measures that can be taken in stages in the national standard *Information security technology - General requirements for Biometric Information Protection* (GB/T 40660-2021). In addition, to reduce the processing risk of biometric information, Article 55 of the PIPL and Article 11 of GB/T 40660-2021 stipulate that security risk assessment shall be continuously carried out for the processing of biometric information, including pre-assessment and post-assessment. Article 60 of PIPL has also established a supervisory department for personal information processors, which is responsible for the protection and supervision of personal information. However, the problem is that there is not only one regulatory department with relevant responsibilities, including the national internet information department, relevant government departments, and even relevant public security departments and industry associations. In the national standards, it is not specified what technical standards information

DOI: 10.54254/2753-7048/10/20230195

processors need to adopt to protect biometric information, and the regulatory authorities do not fully communicate and coordinate, and sometimes hold different review standards, resulting in information processors will consume unnecessary costs and lose some benefits when responding to regulatory review. Therefore, it is recommended that various regulatory authorities strengthen the interoperability of standards to promote industrial development while ensuring information security.

5. Conclusion

As one of the most special type of personal information among sensitive personal information, biometric information lacks special protection in current Chinese legislation. As far as the current legislative approach of PIPL is concerned, it is not suitable to formulate a special law for its special protection, but it is more appropriate to carry out comprehensive legislation, and combine relevant legislative interpretations and judicial interpretations to further clarify the definition, collection rules and processing rules of biometric information. Compared with BIPA and GDPR, PIPL lacks a clear enumeration and connotation explanation of biometric information. Besides, on the one hand, some provisions such as the principles of legality, legitimacy and necessity and the collection exemption are vaguely worded, and lack necessary legislative and judicial interpretations; On the other hand, norms such as informed consent, transparency, and security responsibility for biometric information can be further improved by formulating or improving industry norms and strengthening cooperation between relevant departments, so as to strengthen the protection of biometric information on the premise of promoting the development of the industry and realize the multi-dimensional value of biometric information.

References

[1] *Singh, P. (2021). Aadhaar and data privacy: Biometric identification and anxieties of recognition in India. Information, Communication & Society, 24(7), 978-993. https://doi.org/10.1080/1369118X.2019.1668459*

[2] *Chandrasekhar, R. (2017, Jun 04). Time to Fix Aadhaar: In spite of high-decibel promotion, Aadhaar has several loopholes that can impact national security and invade people's privacy. Business Today, https://www.proquest.com/magazines/time-fix-aadhaar/docview/1899748091/se-2*

[3] *Dongya , L. (2022, Jan 28). Legal Analysis of the First Case of Facial Recognition in China. Global Law Review, 44(01), 146-161.*

[4] *Yanan, M. (2019). The first case of face recognition: what is sued. Fangyuan Magazine, 2019(24), 14-17.*

[5] *Qi, Z., & Dongmei, X. (2022). Judicial Application of Biometric Information Definition in China: Dilemma and Strategy. Library Tribune, 42(7), 43-54.*

[6] *Xuxuan, H. (2013). The right to self-determination of personal data information in comparative law. Comparative Law Research, 2013(02), 61-76.*

[7] *Cate, F. H., & Mayer-Schönberger, V. (2013). Notice and consent in a world of Big Data. International Data Privacy Law, 3(2), 67-73. https://doi.org/10.1093/idpl/ipt005*

[8] *Simmons, C. L. (2018). Privacy Law Compliance in Bankruptcy: The EU's New GDPR. American Bankruptcy Institute Journal, 37(10), 18-19,69-70. https://www.proquest.com/scholarly-journals/privacy-law-compliance-bankruptcy-eus-new-gdpr/docview/2136000107/se-2*

[9] *Henriksen-Bulmer, J., Yucel, C., Faily, S., & Chalkias, I. (2022). Privacy Goals for the Data Lifecycle. Future Internet, 14(11), 315. https://doi.org/10.3390/fi14110315*

[10] *Quan, L. (2021, Sep 15). On the Principle of Legality, Legitimacy and Necessity of Personal Information Processing. The Jurist, 188(05), 1-15+191. DOI:10.16094/j.cnki.1005-0221.2021.05.001.*