ISSN: 2688-8653

Research on Personal Information Protection in the Field of Biometrics

Ye Ju[1, a], Wanrong Liu [2] and Meiling Lan[1]

[1]Faculty of Law, College of Applied Arts and Science, Beijing Union University, Beijing, China

[2]School of Law, University of International Business and Economics, Beijing, China

[a]juye@buu.edu.cn

Abstract

The legal protection of biometric information is taken as the research object, and by drawing on the achievements of foreign legislation, based on the current situation of biometric information protection in China, analyzes the existing problems of biometric information protection in China, and puts forward suggestions for perfection. This paper briefly introduces the basic concept of biometric information protection, analyzes the development process by studying the extraterritorial biometric information protection legislation, and refines the experience that our country's legislation is worth learning from. The current situation of the legal protection of biometric information in China and the existing problems are also analyzed. On the basis of analyzing the existing problems in our country, the proposals of the legal protection of personal biometric information in our country are put forward.

Keywords

Biometric data , Personal information, Legal protection.

1. Question Raised: The Application and Development of Biometrics

The identification technology derived from biometric information, known as biometrics, is simply the identification of an individual's unique biometric information which is collected and processed by computer algorithms to achieve the purpose of identifying an individual's identity. With people's continuous exploration in this field, a variety of information collection sensors have been developed that can identify biological information including but not limited to fingerprints, facial features, irises, sounds, etc, and such technology has been widely promoted and used in life.

Biometric technology, such as the well-known attendance record system, is introduced into people's lives by means of "fingerprint punch card". Likewise, facial recognition technology is increasingly used in our daily life, whether it's for bank transactions, transportation, or other occasions where passwords are normally required..In addition, iris recognition systems are widely used in key security areas. By granting different privileges to authenticated persons, iris recognition technology prevents unauthorized persons from entering restricted areas and performing any operation. While voice recognition technology, taking advantage of the properties of waves, can be used for identification without the need for direct observation of an individual or human organ. It is quite advantageous in the field of public security. For example, after the establishment of a voice sample database, it is possible to use communication information extraction to target suspects, which is of tremendous help to such cases which are inherently difficult to solve like telecommunication fraud.

Thus, biometrics have brought a lot of convenience to our lives. Such a booming new field brings not only new experiences, but also higher demands and expectations. Biometrics are

ISSN: 2688-8653

increasingly involved in important areas of life, involving safety of life and property. Security has replaced convenience as a new important consideration for people. From convenient and efficient to information security, this is also the development direction of biometric technology.

2. Analysis of Basic Problems of Personal Information Protection in the Field of Biometrics

2.1. Relationship between Biometric Information and General Personal Information

Biometric information is defined as a type of information used to identify the innate physical characteristics of a particular individual, such as fingerprints, iris or facial features, etc, which has the ability to uniquely identify a specific individual. "Biometric identifier" is used to identify a specific individual, including but not limited to fingerprint, iris, voice or face. "Biometric information" means any information that is generated based on an individual's biometric identification. The process of “biometrics” can be understood simply as comparing an individual’s biometric identifier to a specific individual in a database compiled from multiple individuals' biometric identifiers, then granting access to the individual or permission to perform certain operations if the input data matches the specific data in the database. As the biometric identifier is usually part of the human body, a biometrically authenticated user will always "carry" their identifier with them. In addition, biometrics enable users to interact with data in a much faster and more efficient way than traditional passwords, which maks it a much more efficient way to access data than ever before. A convenient alternative to traditional identification methods. However, in contrast to other personal information in the traditional sense, biometric information is unique and its irreplaceable nature makes such information has specific sensitivities. If a malicious third party succeeds in stealing an individual's biometric information, any information related to that particular individual may be threatened. Moreover, unlike other passwords that can be changed once compromised, individuals whose biometric information has been stolen can never securely use the stolen biometrics again for authentication.

As can be seen, biometric information, as a type of personal information, has the same identification function as other personal information. But differing from the general personal information whose carrier is often an external object, biometric information is directly associated with the human physiological organism and has a unique direction and it lasts a lifetime.

2.2. Particularity of Biometric Information

With regard to the protection of personal information, China does not yet have a unified law specifically regulating such protection. There is also no clear legal definition of the ownership of personal biometric information, and the latest Civil Code has not yet established an independent right to personal information. As a result, the issue of ownership of "personal information" remains vague, and there is also controversy over the legal nature of personal information in Chinese academic circles. For example, Prof. Wang Liming believes that the right to personal information should be legally recognized, while Prof. Wang Zejian believes that personal information protection laws should be incorporated into the Privacy Law. There are also many criteria for classifying personal information, the most common being the degree of sensitivity of the information. Under China's current legal system, the classification of various types of personal information is already vague and confusing. Article 76(5) of the Cybersecurity Law of the People's Republic of China lists the extensions of personal information, and in the definition of the scope of personal information in the Civil Code, “personal biometric information” is specially listed, which belongs to sensitive personal information. However,

ISSN: 2688-8653

there is still no clear legal boundary between personal biometric information and general personal information, and no special protective measures have been taken. Chinese academics also have different views on this issue. Professor Zhang Xinbao has proposed the theory of "two-sided reinforcement, three-sided balancing", in which one of the "two-sided" is personal sensitive private information. At one end of the spectrum is general personal information, the commercial use of which should be enhanced and the use of which for national public administration purposes should be strengthened. The use of "sensitive personal information". Dissenting scholars such as Professor Zhou Hanhua point out that it is currently inappropriate to include provisions on "sensitive personal information" in Chinese law.

In essence, personal biometric information is more special than general personal information. Biometric information confers an extremely high personality attribute due to its direct connection with the human physiological organism. It is this unchangeable quality that accompanies life-long that makes biometric information need special protection. For most general personal information, there are still many ways to readily replace almost any form of personal information when it is compromised. However, when the biometric information is stolen, it is impossible to replace the personal biometrics at will. For example, in terms of face recognition, there is no face replacement technology that does not have the risk of biorejection and has a short recovery time. The risk posed by the theft of biometric information is likely to be persistent and will almost permanently limit the ability of the individual whose information was stolen to securely reappear. The biometric identifier is needed to carry out various activities. In summary, based on the above characteristics, biometric information is unique compared to general personal information, and in the face of the severe social and personal challenges. Information security situation, it is all the more important for China to distinguish biometric information from general personal information and to protect it differently.

2.3. Necessity and Urgency of Protection of Personal Information in the Field of Biometrics

At present, biometric identification technology has a wide range of applications in mobile payment, mobile phone unlocking, smart securityand other fields. However, in the growing innovation and application of biometric technology, there is no complete legal protection system to match it to regulate these new and evolving segments. As a result, there are serious hidden troubles existing in the security of personal biometric information.

For example, many apps collect mobile phone face information, and recently, a face-changing app called ZAO has aroused widespread public discussion. ZAO applies artificial intelligence technology to use the frontal face photos uploaded by users to make popular facial expression packages in various well-known movies. Acting as the protagonist and acting as a star idol has caused users to worry about the misuse of their biometric information.[1] In fact, ZAO's problem is not alone. Checking the 2018 "Personal Information Collection and Privacy Policy Evaluation Report" shows that 10 applications out of a total of 100 applications with 10 types of query samples did not clearly inform users that the act of collecting user personally identifiable biometric information by himself is suspected of excessively collecting personal biometric information. What's more, an investigation by a journalist has revealed that facial photos without the authorization of the photo owner are being openly touted on Internet platforms. When this facial data information is used to apply for credit or register a company, it can cause a huge loss to the user whose information has been compromised.[2] Likewise, the misuse of fingerprint identification information has also resulted in a number of negative incidents. The famous hacker Jan Krissler introduced at the 31st Chaos Computer Club Conference that he only collected close-up photos of the fingers of the German Defense Minister at a public press conference in October and used a commercial software called VeriFinger, which made him succeed in extracting the fingerprint of the Minister of Defense. It's hard to

ISSN: 2688-8653

imagine that a set of photos of a meeting would thus provide a conduit for biometric information to be leaked.

In recent years, in view of the rising trend of biometric information leakage and cybercrime cases, people have gradually realized the risks that biometric technology may bring. Once the biometric technology is out of control, such as theft, misuse or even illegal disclosure of biometric information, it will bring significant network security risks. If a hacker successfully steals a person's biometric information, any information related to the biometric information will be at risk. At present, the collection of personal biometric information does not require excessively advanced technology. Many ordinary institutions such as artificial intelligence companies, biological companies, and medical institutions can master this technology. However, the data protection level and security protection level of technology developers and users are not high, and there is a lack of unified and standardized technical standards. There are security risks in many application links. Due to the relatively new biometrics technology, China's legislation in this area is still slightly behind. Consequently, legislation should be carried out as soon as possible for the protection of biometric information, and a legal protection system of biometric information should be established in line with China's reality, so as to avoid the obstruction and adverse impact of this legislative gap on the development of science and technology and the life of citizens, as well as to protect the relevant rights and interests of citizens from infringement.

3. The Extraterritorial Legislative Model and Development Trend of Personal Information Protection in the Field of Biometrics

3.1. Overview of Extraterritorial Legislative Models for the Protection of Personal Information in the Field of Biometrics

The collection of biometric information and the loss of its anonymity is widely recognized in Europe and the United States as a threat to the exercise of citizens' fundamental rights, including but not limited to the right to equality, freedom of expression, freedom of communication and assembly, and the right to privacy. In 2012, the French Constitutional Court explicitly addressed this issue, stating that databases containing biometric information violate the fundamental right to privacy. In the United States, the impact of biometrics has attracted more attention, and scholars have conducted detailed discussions on the legal issues. After four consumer protection organizations, led by the Electronic Privacy Information Center, complained about excessive use of facial recognition technology, the US Federal Trade Commission began investigating the risks of using facial recognition technology ten years ago. Another report from the Georgetown Privacy and Technology Law Center in 2016 showed how U.S. law enforcement officials can compare photos of suspects with photos stored in driver's licenses and other databases from unsuspected individuals, or just pedestrians walking on the road captured from surveillance cameras. European and American countries generally believe that in order to keep up with the rapid development of biometric technology, clear legal provisions help to provide clear guidance to government officials and the private sector who wants to use biometric information in their projects. In addition, foreign scholars have begun to discuss the strengthening of legislation on biometric information in specific areas (such as the protection of consumer rights and the protection of the rights of persons with disabilities) to minimize any negative effects that biometric technology may have. In summary, as the most private part of personal privacy, biometric information has become a key protection category of relevant laws in European and American countries.

Looking at foreign legislation in the field of biometrics, it can usually be distinguished between two different models: the model of specific legislative protection and the model of comprehensive legislative protection model. The specific legislative protection model is

ISSN: 2688-8653

represented by the United States and is characterized by specific legislation on the protection of relevant biometric information. The comprehensive legislative protection model is common in the European Union and is characterized by the inclusion of different types of personal information in a unified law, as well as the incorporation of civil, criminal and administrative protection measures relating to this legal issue.

3.2. The US Model of Special Legislative Protection

The specialized legislative model is represented by the United States, which currently does not have a federal law specifically addressing the collection, use or release of biometric information. All states except Illinois, Texas and Washington allow employers or businesses to collect and analyze biological identifying information without disclosure or notice to employees or consumers.

In 2008, Illinois passed the Biometric Information Privacy Act (BIPA), becoming the first state to pass biometric information regulations. In 2009, Texas followed suit by adopting the Access to Biometric Identifiers or Use Act (hereinafter CUBI), and after the passage of BIPA and CUBI, states tried to start creating their own legislation on biometric information security. However, it wasn't until 2017 that Washington became the third state to create such a law, the Washington Biometric Privacy Act (hereafter referred to as WBPA). All three of these bills regulate the acquisition and use of biometric information in different ways, and make different provisions for the manner of law enforcement.

In the bills of the above three states, the "biological identifier" is generally used as the main body of the regulated information type. However, each bill has its own unique definition of biological identifiers. BIPA defines "biological identifiers" as scans of the retina or iris, fingerprints, voiceprints, or the geometry of the hand or face. Biological identifiers do not include written samples, written signatures, photographs, human biological samples, demographic data, tattoo descriptions, or physical descriptions (such as height, weight, hair color, or eye color). CUBI defines biological identifiers as "retina or iris scans, fingerprints, voice prints or records of head or face geometry" to distinguish them from BIPA. Unlike BIPA, the definition of CUBI does not provide specific exemptions for items or information that are not considered as biological identifiers by BIPA, such as photos and demographic data. Similarly, WBPA also gives a general definition of biological identifiers, and then exemplifies what is included or not included in the definition to distinguish it from the previous bill.

Among them, the Illinois "Biometric Information Privacy Act" is considered to be the most effective bill among the many biometric information bills in the United States due to its stipulated private litigation rights and its strong stance on selling biometric information, and has become a typical model of special legislative protection.

The Illinois Biometric Information Privacy Act was first submitted to the Illinois Senate in February 2008 when a company called “Pay by Touch” in San Francisco went bankrupt. This company provided merchants with biometric authentication methods that consumers can pay for the goods by binding their financial information with fingerprint information. After the company went bankrupt and disbanded, consumers did not get any information about how their biometric information provided by fingerprint payment in advance would be dealt with. This incident promoted the drafting and final adoption of BIPA. Probably because the drafting of BIPA was caused by the actual situation, it detailed the legislative purpose of the bill. It believes that the use of biometric technology in the commercial field and security inspection departments is increasing. Although it helps simplify the financial transaction process and improve the security inspection efficiency. However, because biometric information is a unique biometric identifier that is different from other general personal information, once biometric information is leaked, it will bring a huge threat to the safety of personal life and property, and may even prevent individuals from permanently participating in transactions involving this

ISSN: 2688-8653

information. Illinois legislators mentioned in this statement of purpose that the risks of using biometric information are not limited to what is seen today, and the characteristics of this information are destined to be at risk of being leaked or even more likely to be leaked. The legislator believes that by regulating the collection, use, protection, processing, storage, retention and destruction of biological identifiers and biometric information will help ensure public safety.

In terms of biometric information protection standards, BIPA has two main features: First, for the protection of biometric information, reasonable protection measures in the industry to which the private entity belongs should be adopted. This requirement takes the market practices in the industry as objective standards. Second, it requires biometric information to be treated in a manner similar to the private entity's treatment of other confidential and sensitive information. This requires private entities to store, transmit, and protect all biometric information in the same or more protective manner as other confidential sensitive information, preventing it from being disclosed.In terms of the sale and distribution of biometric information, BIPA absolutely prohibits the sale of biometric information, stating that "Any entity that possesses biometric identification or biometric information shall not sell, rent, trade or otherwise profit from the biometric identification or biometric information of individuals or customers."

In terms of rights relief, according to BIPA regulations, individuals can file civil suits to seek judicial relief. By granting private litigation rights, anyone can file a damages lawsuit in the State Circuit Court or the Federal District Court. If a private entity violates BIPA due to negligence, the winning party may receive $1000 or actual damages (whichever is greater amount), and if the violation of BIPA was willfully or recklessly caused, the prevailing party may be awarded $5,000 or actual damages (whichever is the greater amount), and the costs of litigation are borne by the offending party. In addition, BIPA also stipulates other forms of relief that the state or federal courts may deem appropriate, including injunctions.

In terms of regulatory agencies and their functions, the "Biometric Information Privacy Investigation Committee" as a special regulatory agency established by BIPA oversees and manages participants in all aspects of biometric information. Including the review of its practices, principles, procedures, the legitimacy and legality of the disclosure, and the management of procedures and methods of storage and destruction, etc.

In summary, the special legislative protection model has a specific legislative purpose, an exclusive legal concept, clear protection rules, and strong pertinence and operability.

3.3. The EU Model of Comprehensive Legislative Protection

The comprehensive legislative protection model is represented by the European Union, which has always provided strict protection of personal information at the legislative level and its level of legislation on personal information is also among the highest in the world. However, at the legislative level, the EU does not have a special biometric information department law, and the main basis for dispute resolution is the relevant provisions of the General Data Protection Regulation. In 2018, the European Union began implementing the General Data Protection Regulation (GDPR). The types of data protected by GDPR are mainly divided into two categories: personal data and sensitive personal data. Personal data is defined as "any data related to an identified or identifiable natural person; an identifiable person is a person who can be directly or indirectly identified".

Personal data includes names and addresses, ID numbers, location data, and even network data, such as IP addresses. According to the GDPR, sensitive personal data is a "special category of personal data", so it must be more strictly protected than general personal information. GDPR adds a new data category to "specially sensitive" data, namely "biometric data processed as a unique identification of natural persons". Special sensitive data usually includes data such as

ISSN: 2688-8653

an individual's race or ethnicity, political opinions, religion or philosophical beliefs. Due to the special sensitivity of such data, the GDPR stipulates that it is generally prohibited to process biometric information "only for the purpose of identifying natural persons", as well as to process all other special categories of personal data. This means that all entities that fall within the scope of GDPR regulation, including public agencies, governments, and private organizations, in principle, do not allow biometric information to be processed “only for the purpose of identifying natural persons”. However, the GDPR also stipulates ten kinds of exceptions that can handle special sensitive data in Article 9, paragraph 2. Five of them need to be clarified by the laws of the European Union or member states to protect the basic rights and interests of the individuals concerned. In legal practice, companies that develop biometric software and companies that use biometric software for employee management must abide by the GDPR. It is worth noting that in western countries’ privacy protection theories and privacy protection legal systems, sensitivity has long become a reference factor for the classification of personal information, such as the EU “108 Agreement”, 95/46/EC, and the Personal Date Protection Act of Iceland, Bulgaria, Hungary and German, all of which clearly prohibit the handling of special sensitive data.

One of the most revolutionary aspects of the GDPR is that it regulates biometric data as a type of independent data, rather than attempting to incorporate it into a privacy law that does not consider the sensitivity of biological data. The GDPR pays special attention to biometrics and clearly recognizes the potential of biometrics to develop a balance between the free flow of data and the protection of citizens’ rights.

Although the GDPR has made regulations prohibiting the processing of biometric information in principle, this does not mean that the processing of biometric information is completely prohibited. For example, one of the exceptions is "explicit consent", and the other exception is that it is necessary and appropriate to use biometric information for the sake of significant public interest under certain circumstances. This shows that the GDPR does not prohibit the commercial use of biometric information, but GDPR emphasizes that care must be taken before processing biometric information. Of course, GDPR has no special regulations or additional regulations on biometric information, and the protection requirements and measures for biometric information are not different from other special sensitive information. According to the regulations made by the GDPR, personal information about physical, physiological or behavioral characteristics can be divided into several categories according to different methods, and EU member states can formulate more specific laws accordingly. At present, EU member states have not reached a clear consensus on the use of biometric information, and there is still no agreement on the legal requirements for the processing and use of biometric information.

3.4. Comparison and Relevance of the Two Models of Legislative Protection

3.4.1. Comparison of the Two Models of Legislative Protection

The two legislative protection models for biometric information have certain common points in legislative value orientation, legislative background, protection principles, and specific regulations. The legislative purpose orientation of these two legislative protection models stems from the rapid development of biometric technology and the consideration of the importance of individual rights, freedom and information security. The two legislative protection models both have made a clear interpretation of the biometric information and information processing process. It goes without saying that no matter which model is adopted, it upholds the value orientation of protecting individual rights and information security, recognizes the unique status of biometric information, and has some similarities in protection principles and methods.

Although the two legislative protection models have certain common points, the relevant protection methods, protection measures, protection mechanisms and other contents are still

ISSN: 2688-8653

different. Compared with the EU's comprehensive legislative protection model, the biggest feature of the US special legislative protection model is that it does not have a centralized or specialized data protection law, but regulates data protection by enacting relevant legislation in specific fields. As we all know, the legal systems of the United States and the states are not completely consistent. At the federal level, the regulation of specific areas depends on the type of law involved. For example, for the healthcare sector, the Department of Health and Human Services will be responsible for implementing the Health Insurance Portability and Accountability Act. In the field of privacy protection, FTC is mainly responsible. States in the United States usually take enforcement actions against any violation of state privacy laws, and definitions of personal information and sensitive personal information vary across the United States. Taken together, the special legislative protection model mainly solves the rights and obligations between information subjects and private entities, as well as the scope of rights protected by the law, and explains in detail the specific legal concepts and connotations for biometric information, and specific provisions are made for specific subjects and specific protection principles, and specific protective measures are specified, but the comprehensive legislative protection model does not make specific provisions for the above content.

3.4.2. Analysis of the Development of the Two Models of Legislative Protection

Take the United States as an example. Since this year, some lawmakers have questioned and opposed the government's use of facial recognition technology. Jeff Merkley and Corey Booker expressed their request to suspend the use of this technology in government agencies. The reason is that there are currently no guidelines and restrictions on the use of this technology, and the hasty use may violate the privacy and freedom of citizens stipulated in the First Amendment. Merkley said: "Technology is developing and advancing every day, and these advancements usually bring improvements in our quality of life, economy, and even public safety." "But Congress has an important responsibility to ensure that the government does not abuse emerging technologies to infringe on the American people's right to privacy, or wrongly targeting people of color." In recent years, biometrics has caused huge controversy in the United States. A federally released study in December 2019 found that Asians and African Americans are 100 times more likely to be misidentified by facial recognition than white men. [3] This raises a serious warning about the impact of using this technology in law enforcement. From California to Massachusetts, many cities in the United States have banned facial recognition technology from municipalities. But Congress has not passed any federal regulations or guidelines to regulate the use of facial recognition technology. The "Face Recognition Ethical Use Act" embodies the high degree of congressional attention to the danger of this technology, and also reflects the attention of the American society to the use of this technology.

In Europe, the GDPR contains detailed regulations on the exercise of public power and the exercise of the rights of natural persons, but there is no specific regulation on biometric information. Currently, the European Union is considering the introduction of new regulations on the protection and use of facial recognition information. The European Fundamental Rights Protection Agency (FRA) released in 2019 "Facial Recognition Technology: Consideration of Basic Rights in Law Enforcement". The report outlines and analyzes the challenges posed by the use of facial recognition technology in public administration to the fundamental rights of citizens, and proposes implementation methods to prevent human rights violations when government agencies deploy facial recognition systems for law enforcement purposes.

By examining the legislation on biometric information protection in Europe and the United States in recent years, it can be found that, like the United States, the use of facial recognition information for public purposes may expose the public to concerns about "surveillance of society", and the EU has the same legislative considerations.

ISSN: 2688-8653

From the perspective of social development, the opportunities and challenges brought about by biometrics coexist. Convenience and efficiency are undoubtedly in line with development tendency and trends, which allows biometric technology to quickly occupy the market and be accepted by a wide audience. But the need for personal information protection makes biometrics technology must be limited to a safe range. Only when these two conditions are met at the same time can we achieve a balance between the rights of personal information and the exchange of data, and achieve long-term and stable development in the field of biometrics and our lives.

3.4.3. Implications of the Two Models of Legislative Protection

Based on the above analysis, the model of special legislation in the United States is more targeted on this issue, and the protection of relevant persons in litigation is also more practical. The EU comprehensive legislation protection model has more advantages in the protection level and the protection effect of the system. The specific legislative model adopted to protect personal biometric information is a problem that needs comprehensive consideration, and in particular, it is necessary to pay attention to the relationship with the laws related to the protection of personal information. If the personal information protection legal system is complete, it is a lower cost and better choice to incorporate biometric information into the legal system for the legal protection of personal information; If the legal system for the protection of personal information is not perfect, then it is appropriate to adopt a special legislative protection model, which is more conducive to the protection of individual legal rights.

4. Current Situation and Problems of Legal Protection of Personal Information in China's Biometric Field

4.1. Overview of the Current Status of Legal Protection of Personal Information in the Field of Biometrics in China

In recent years, all walks of life in China have more or less "co-operated" with biometrics, which has brought tremendous convenience to the development of the industry, production and life. There are faster and more practical ways of authenticating individuals, but at the same time, it has also raised public concerns about the protection of personal information in the field of biometrics. Although China has adopted some laws and regulations to protect personal information, and "biometric information" is included in the scope of "personal information", such as the "Network Security Law of the People's Republic of China", "Information Security Technology Personal Information Security Code" and so on. However, the protection of biometric information by these laws and regulations is still incomplete. For example, there is no clear law to clearly define the attributes and functions of biometric information; the legal principles, rights and obligations are not clear; the lack of a corresponding legal protection system to remedy the rights of the information subject. At present, people are widely using biometric information such as fingerprints and faces to make mobile payments. It is precisely because of the above-mentioned protection flaws in related fields that behind the popularity of the face-changing app "ZAO", it has also aroused the concern and thinking of the society to this problem. Therefore, a comparative analysis should be carried out on the foreign protection model of personal biometric information, and then combined with China's legal tradition and specific national conditions, clarify China's due legislative model on this issue, and improve China's legal protection system for biometric information.

ISSN: 2688-8653

4.2. Problems in the Legal Protection of Personal Information in China's Biometrics Sector

4.2.1. Lack of Specific Provisions for Biometric Information

At present, China's legislative system has no special regulations on the protection and use of biometric information. The legal attributes, functions, and effects of biometric information have not been clearly defined. The lack of legislation on the one hand will lead to more rampant disclosure, theft or misuse of biometric information, threatening the safety of citizens' biometric information; on the other hand, it is also not conducive to the development of the biometric information industry norms. Although it provides a certain legal basis for the protection of biometric information, the existing laws still lack completeness and relativity.

Although the Chinese Civil Code provides relevant protection for biometric information, the protection intensity in the biometric information processing behavior regulations is slightly weaker. The current law is limited to information collection, storage and disclosure. The rights and obligations of information controllers and information processors are not clearly stated.

4.2.2. Lack of Redress Mechanisms for the Rights of Information Subjects

In recent years, infringement cases of biometric information in China have occurred frequently. In addition to the lack of special regulations, the reason is that it is difficult for the infringed person to find an effective way to protect their rights, which makes the infringer "unjustified" and difficult to receive punishment. This dilemma is mainly manifested in the following aspects:

First, it is difficult to identify the responsible party. At present, information sharing has become a trend in the era of big data, but because the process of "notification-agreement" is not clear during the use of network services, many information controllers will obtain and process the information of the subjects without the knowledge of them. At the same time, due to the concealment of information acquisition, information subjects are often unable to determine the source of information leakage or abuse, and it is difficult to determine the subject of litigation in actual litigation.

Second, the proof is difficult. As mentioned earlier, in the wave of the Internet connecting thousands of households in the era of big data, more and more personal information has been transferred from physical and paper records to electronic information records. Correspondingly, a highly specialized field has been formed in the areas of information processing and information transmission. Because users of information subject technology often do not have more professional knowledge and technical support, it is difficult to find favorable evidence when they are infringed, so that they are in a passive position.

In addition, due to the particularity of the Internet, information controllers and information subjects are often separated from each other, which also increases the complexity and cost of protecting the rights of information subjects after being infringed. Therefore, many information subjects have actively or passively waived their rights and remedies after being infringed, and the relevant approaches have become empty talk.

4.2.3. Lack of a Statutory Body to Regulate the Processing of Biometric Information

Among the institutions currently set up in China, there are different management institutions for different aspects of personal information such as online personal information and personal credit information. However, there is no special agency to manage personal biometric information. On the one hand, this kind of institution management model will cause repeated management and unnecessary use of administrative and judicial resources. On the other hand, some areas have not been included in the supervision of existing institutions. If problems are encountered in new fields, it is difficult for the law to play its due role. From this, it can be seen that establishing an institution that centrally supervises personal information is more in line with the development trend of personal information application. Similarly, the establishment

ISSN: 2688-8653

of more detailed specifications for the collection, processing, use, and storage of personal information by the same agency is also conducive to the unification and specific implementation of the standards.

5. The Path and Countermeasures for the Legal Protection of Personal Biometric Information in China

5.1. Legislative Level: Clarifying Special Protection for Biometric Information

First, Comprehensive reference to the European and American legislative model. In terms of legislative technology, the experience of the United States and the European Union in the specific legislative and comprehensive legislative models can be fully learned, so that the defects and deficiencies inherent in the two models can be compensated accordingly, so as to achieve the effect of gaining strengths and avoiding shortcomings and refining the essence. Based on the current situation in China, many theoretical issues in the protection of personal information, such as information ownership, rights model, infringement relief, and conflicts of interest of various parties, have not been fully clarified. The prematurely introduction of a special “Biometric Information Privacy Protection Act” is of no sufficient theoretical basis, which only increases the cost of legislation. The provision of biometric information in the unified legislation can fill the relevant gaps in a short time, which helps to solve the actual needs at the same time, and also avoids the problems of single measures and incomplete mechanisms in the special legislative model. The protection of biometric information in China’s current legislation tends to be included in the category of personal information, but considering that biometric information also has some characteristics that other personal information does not have, it is recommended to consider this problem in future legislation and revision processes, and protect it as sensitive personal information.

Second, adding special provisions on biometric information in general laws. For example, add corporate responsibility for biometric information to the Consumer Protection Law and the E-commerce Law that companies are required to obtain special authorization to obtain the information, and after obtaining the information need to fulfill the obligation to protect information security. At the same time, industry standards and related evaluation mechanisms can be added, and even administrative licensing can be added to regulate the bioinformatics technology industry to promote the orderly and healthy development of the industry.

Third, adding special chapter provisions in special laws. Judging from the legislative plan of the 13th NPC Standing Committee, it is imperative for China to enact special legislation in the field of personal information protection. At the same time, considering what has been mentioned above, the legislative protection of biometric information in most countries is usually unified in the Personal Information Protection Law, so in light of China's national conditions, it is recommended to set up an independent chapter in the upcoming "Personal Information Protection Law" and “Data Security Law”, which stipulates special protection rules for the acquisition, use, disclosure, storage, and cross-border transmission of biometric information.

5.2. Judicial Level: Reducing the Judicial Litigation Requirements for Biometric Information

The infringement of personal biometric information occurs in the data processing activities of the data controller. Because the consequences of substantial damage are usually not tangible or very obvious, and there are problems such as the difficulty of obtaining evidence for the information subject, which leads to the possibility of the realization of civil rights litigation relief being insufficient. In view of this, foreign laws on the protection of personal information usually impose a "reversed burden of proof" along with the principle of "burden of fault", that is, information processing parties can prove that they have no fault before they can bear civil

ISSN: 2688-8653

liability. At the same time, Germany adopts the principle of "no-fault liability" in terms of the principle of liability, that is, in the process of large-scale processing of personal information, public authorities, even if there is no fault, but actually shall be liable for material or non-material damage to the information subject. At present, the problem exposed in the processing of personal biometric information in China is that various legal persons, unincorporated organizations, and natural persons process personal biometric information arbitrarily and disclose, trade, and steal without legal authorization or consent of the information subject, etc. The information subject is usually unaware of the infringement it has suffered, and even if it is known that it has been infringed, it usually cannot fully prove the substantial damage caused by the illegal processing by the processing party. It should be noted that from the reference of extraterritorial legislation, we cannot directly define what constitutes "damage" in the civil damage compensation for personal information protection, that is, the determination of the specific amount caused by infringement is difficult to determine. This aspect is due to the different circumstances of different countries, but the more important reason is the complexity of personal information infringement, which makes it difficult to generalize the consequences of damage with a unified standard.

Therefore, in Chinese judicial practice, this feature should also be fully taken into account. I suggest that the rule of judicial protection of biometric information be established as follows: Even if the citizen's biometric information has not been materially harmed, data subjects still have the right to seek judicial remedies. Compared to general personal information infringement, the standard of judicial protection of biometric information is obviously higher. The reason for lowering the judicial litigation requirements for biometric information is to ensure that biometric information subjects can claim their rights in a timely manner so as to take precautions against possible future losses. After all, once real damage has been done, the consequences of that damage will be difficult to repair.

5.3. Enforcement Level: Establishing an Information Protection Regulator

Personal information covers many different aspects, each of which shows different aspects of the individual as a person in social life. It goes without saying that biometric information is also an important part of it. The protection of biometric information not only depends on a complete legal framework, but also needs to be supplemented with measures that match it. Only when the two complement each other and implement the legal provisions into practice can the protection effect be truly effective.

It is not an unfounded fantasy to advocate the establishment of a special supervisory authority for personal information protection in China. Personal information protection agencies have been established in many countries and regions, such as the UK Data Protection Commissioner's Office, the Icelandic Individuals' Data Protection Agency, Japan Information Disclosure and Personal Information Protection Review Board, etc. These institutions mainly start from the guidance of the establishment of personal information protection mechanisms and the supervision of the processing of personal information data, comply with the rationality and legitimacy and exercise the powers conferred by the law. In Hong Kong, China and Macao, China, there are also organizations with similar functions that carry out work related to the protection of personal information. Generally speaking, such institutions have the following main responsibilities: First, it provides guidance for the establishment and maintenance of protection mechanisms. Second, it provides supervision for the collection, use, and processing of data. Third, it provides feedback to the public’s complaints (including investigation after accepting comments, and the processing results will be summarized and fed back to the maintenance mechanism again to provide guidance). Fourth, it plays a role in propagating popular science of relevant knowledge.

ISSN: 2688-8653

It should be noted that the significant differences between the institutions such as the "Internet Information Office", "National Information Center" and even the "Big Data Bureau" owned by China at the current stage are that they do not have legal regulatory authority. This leaves no legitimate source of power and no coercive force in the process of agency management. Therefore, China needs to legislate to establish a national-level information protection regulatory agency and set up subordinate organizations at the local level. The supervisory authority should have the right to review, permit, investigate, inspect, order, and intervene in the processing of various entity data, as well as the right to mediate disputes, and to accept complaints and appeals. Regulators should go even further and design a “opt-in” mechanism similar to GDPR, rather than the “opt-out” mechanism adopted by the United States for the use of biometrics, which protects both the legitimate rights and interests of citizens and the operating interests of enterprises.

5.4. Summary

Establishing and improving the legal system and supporting measures related to personal biometric information is an indispensable important link in the protection of personal biometric information not only because some of the problems we face at this stage need to be further improved by the law, but the development trend of biometric technology is also destined that these measures are necessary. An effective legal framework and supporting measures should not only focus on improving relevant legislation at the legislative level, and to improve the rights remedy mechanism for information subjects at the judicial level, but also to establish an information protection regulatory agency at the level of law enforcement. In the long run, biometric information can be fully and effectively protected, the superiority of biometric technology can be fully reflected and applied to production and life, and all industries involved in biometric information can develop healthily and orderly.

6. Conclusion

Today, as the process of globalization continues to accelerate, the construction of a community of human destiny directly determines that no problem exists in isolation. The same is true of the legal protection of personal biometric information, which is not only a problem in China, but also a worldwide problem. In the legislative exploration of the protection of personal biometric information, some countries in the world have accumulated some valuable experience in the pace of the forerunners. Both the legislative and judicial levels have extremely important reference significance for our country to solve this problem.

Nowadays, biometrics technology has spread throughout every corner of our lives, changing our lifestyles, habits and even living conditions in all directions. It is no exaggeration to say that biometric technology has promoted a huge social governance change. It is not difficult to see that it is necessary to establish a comprehensive biometric information protection system. Only in this way can we protect the interests of individuals and society in this reform, at the same time balance the relationship between data circulation and protection of rights and interests, and maximize the application of the advantages of biometrics, thereby promoting the healthy development of industry and benefiting society.

For China at the present stage, it should take the actual situation as the basis and starting point, fully implement the rule of law thinking in the three aspects of legislation, justice, and law enforcement, innovate to establish and improve relevant legal systems on the basis of drawing on foreign experience, and improve the supporting protection system, so as to effectively protect personal biometric information.

ISSN: 2688-8653

Acknowledgements

This article is a research result of the National Social Science Fund of China, Research on Financial Supervising Regulations Based on Big Data (Fund No., 18BFX137), and a teaching-type research result of Premium Funding Project for Academic Human Resources Development in Beijing Union University, Study on Cohesive Mechanism between Civil Redress and Administrative Protection for Online Consumer (Project No., BPHR2017DS03).

References

[1] Zhang Xinbao. Collection of Personal Information: Restrictions Applicable to the Principle of Informed Consent [J]. Comparative Law Research, 2019(06): 1-20.

[2] Fu Weiming. Legal protection model of personal biometric information and China's choice [J]. Journal of East China University of Political Science and Law, 2019, 22(06): 78-88.

[3] Zhao Shuyu. International experience and enlightenment of biometric information legal regulation [J]. China Information Security, 2019(11): 37-39+43.

[4] Pi Yong, Wu Bo. Challenges and countermeasures of the application of artificial intelligence to the protection of personal information [J]. Confidentiality, 2019(10): 52-54.

[5] Shi Jiayou. Advancement and Limitation of Personality Rights Legislation——Comment on "Draft of Personality Rights in Civil Code (Three Review)"[J]. Tsinghua Law, 2019, 13(05): 93-110.

[6] Fu Weiming. The significance of the legal protection of personal biometric information in the era of big data [J]. Graduate Law, 2019, 34(04): 134-140.

[7] Cheng Xiao. Personal Information Protection from the Perspective of Civil Code Compilation [J]. Chinese Law, 2019(04): 26-43.

[8] Tian Ye, Zhang Chenhui. On the Legal Protection of Sensitive Personal Information [J]. Henan Social Sciences, 2019, 27(07): 43-49.

[9] Wang Liming. Highlights and improvement of the draft of the personality code of the Civil Code[J]. Chinese Law Review, 2019(01): 96-108.

[10] Masmon. Analysis of the legal protection path of personal biometric information in the United States[J]. Legal Expo, 2019(04):258.

[11] Hu Haiming, Zhai Xiaomei. On the privacy protection of the application of biometric technology[J]. Chinese Medical Ethics, 2018, 31(01): 60-64.

[12] Long Weiqiu. Research on the construction and system of new data property rights[J]. Forum on Political Science and Law, 2017, 35(04): 63-77.

[13] Liu Yue. On the protection of the property rights of biometric information [J]. Legal Business Research, 2016, 33(06): 73-82.

[14] Zhu Gongyu. The legal conflict and coordination of biometrics and privacy protection [J]. Science and Technology, 2009 (06): 25-28.