World Journal of Sociology and Law
ISSN: 2960-0308
DOI: 10.61784/wjslv2n188

COMPARISON OF THE PROTECTION OF PERSONAL HEALTH DATA UNDER DIFFERENT NATIONAL LEGISLATIONS

BinXian Wu*, JingWen Zu, QiLi Chen

School of English for International Business, Guangdong University of Foreign Studies, Guangzhou 510420, Guangdong Province, China.

Corresponding author: Binxian Wu, Email: 2408073482@qq.com

Abstract: This paper uses literature research, case study and comparative analysis to compare and analyze the legal protection status and problems of personal health data under different national legislations, and puts forward relevant legislative measures. The results show that countries outside the region still face challenges of innovation and supervision in the legal protection of personal information, especially personal health data. By exploring the international soft law frameworks of data protection such as GDPR and APEC Privacy Framework, as well as the legal norms, problems and opportunities of some representative countries in Europe, America and Asia in the protection of personal health data, this paper aims to improve the theoretical depth of data jurisprudence research and provides guidelines for the scientific legislation in the relevant fields in China.
Keywords: Personal health data; Privacy protection; International standards; Comparative analysis

1 INTRODUCTION

Personal health data is personal data relating to the physical or mental health of natural persons. Personal health data belongs to the scope of "personal information", and because it is mainly generated by natural persons in the process of disease prevention and health management, it has great medical value and the necessity and urgency of legal protection. Existing studies have mostly discussed the legal protection of personal data from a domestic perspective or compared it with countries such as the nations in the European Union and the United States, presenting a fragmented state, and have yet to conduct a systematic study from an international comparative perspective, ignoring the advanced experiences of Asian countries such as Japan, South Korea, and Singapore and the relevant provisions of regional treaties such as the APEC Privacy Framework.

Focusing on the legal protection of personal health data, this paper conducts an international comparative study based on the international soft law framework of data protection such as GDPR and the relevant legal norms of representative countries in Europe, the Americas, and Asia, with the aim of exploring the domestic legislation of other countries on the protection of personal health data and its operational effects and thus proposing countermeasures to improve the legal protection of personal health data in China.

Comparative analysis of the relevant experience of overseas countries can help improve the regulation and governance of personal health data in China, and provide partial guidance for the national legislation on data security in related fields. It can also help enhance the utilization value of personal health data, promote the development of the medical research field, and further promote the law system in China.

2 PERSONAL HEALTH DATA PROTECTION UNDER THE EU JURISDICTIONS AND NON-EU COUNTRIES

2.1 The EU Legal System

2.1.1 France

The Data Protection Act, enacted in 1978, covers personal information held by government agencies and private entities[1]. The law states that anyone wishing to process personal data must register to obtain permission in cases related to processing by public bodies and medical research. The individual must be informed of the reasons for the collection of the data and have the right to obtain their personal data, request its correction and object to the processing of the data.

2.1.2 Germany

The court's decision can be based directly on the "right to information self-determination" enshrined in Article 2 of the German Constitution [2].

The Federal Data Protection Act features that in addition to itself as a comprehensive law, there are several sector-specific provisions. The law applies to the collection, processing and use of personal data by federal and state public bodies in the absence of provisions of state regulations, as well as to the processing and use of data for commercial or professional purposes by non-public bodies.

2.1.3 Netherlands

Two decrees were issued under the Data Registration Act. Firstly, the decree on Sensitive Data sets out the limited circumstances in which personal data on an individual's religious beliefs, race, political beliefs, sexual orientation, medical, psychological and criminal history can be included in the personal data file. Secondly, the Act on regulatory exemptions exempts certain organizations from the registration requirements of the Data Registration Act[3].

The Data Registration Act defines the Registration Chamber as a data protection authority that supervises the operation of personal data files.

2.2 The Non-EU Countries

2.2.1 Switzerland

The Federal Act of Data Protection of 1992 requires private companies to register if they regularly process sensitive data or transfer it to third parties and Federal agencies must register their databases. Transfers to other countries must be registered and the receiving country must have equivalent laws[4]. Violations of the law will be subject to criminal punishment. In June 1999, the EU Data Protection Working Group determined that Swiss law complied with the EU Directive. In July 2000, the European Commission formally adopted this position, thus approving all future transfers of personal data to Switzerland.

In addition to the Data Protection Act, there are legal protections for privacy in the Civil Code and the Criminal Code, as well as special rules.

2.2.2 Iceland

The Act on Protection of Individuals with regard to the Processing of Personal Data regulates the processing of personal data by government agencies and companies issued to comply with EU directives. The Act covers the automatic and manual processing of personal information.

The Act on Biobanks sets out rules for the "collection, keeping, handling and utilization of biological samples from human beings" to ensure confidentiality and prohibit discrimination. The law requires the informed consent of the person taking the sample. However, according to the Act, if samples have been collected for clinical tests or treatment and the doctor gives general information to the patient, the consent of the patient may be assumed for the storage of the biological sample in a biobank.

3 PERSONAL HEALTH DATA PROTECTION UNDER THE US LEGAL SYSTEM

At the federal level, earlier regimes such as the Fair Credit Reporting Act of 1970, the Privacy Act of 1974, the Financial Privacy Act of 1978, and the Electronic Communications Privacy Act of 1986 focused on protecting privacy and were designed to protect personal information through industry and market coordination. In 2018, California enacted the Consumer Privacy Act, which is currently the most stringent consumer personal information protection law in the United States, which imposes new obligations on relevant entities to disclose the categories of consumer personal information collected, introduces information access and the right to be forgotten to state residents, and consumers can refuse to sell personal information to third parties, providing a legal way for consumers to control personal information. In March 2021, Virginia passed the Consumer Data Protection Act, becoming the second state to enact comprehensive privacy legislation.

Although the United States attaches great importance to the privacy protection of personal information, it advocates the free flow of personal information across borders to maximize economic benefits. For the cross-border flow of personal information, the United States tends to market regulation, and attempts to achieve the unity of state supervision and commercial freedom through two regulatory methods: "industry self-discipline" and "post-event accountability"[5].

The United States has made detailed regulations on the transaction rules of medical information, medical privacy, patient identification and other issues to ensure the security of medical information. For example, the HIPAA Act requires healthcare organizations to take a series of measures to protect patients' privacy and identity information, including restricting access to and disclosure of information, enhancing information encryption and secure storage, and more[6]. In addition, the U.S. has regulations and guidelines in place to ensure that the transaction of medical information is regulated and ethical, and to encourage healthcare organizations to use secure technologies and protocols for electronic medical record recording and data exchange. According to the Act, all organizations involved in personal health information, including medical institutions, insurance companies, health care plans, etc., must take the necessary measures to protect this information from disclosure or misuse. These measures include, but are not limited to, establishing internal regulations, improving cybersecurity measures, training employees, etc. If the bill is violated, the organization in question will face legal action and may be subject to fines or other penalties.

The HIPAA Act regulates consumer credit information and requires the protection of consumer rights. In addition to personal health information, the HIPAA Act also regulates consumer credit information. The Act requires that any organization must comply with relevant regulations when collecting, using or disclosing consumer credit information to ensure that consumers' rights and interests are effectively protected. If the Act is violated, organizations may face penalties such as legal action or fines.

U.S. law also governs the collection and use of email addresses and phone numbers. These provisions are designed to protect consumers' privacy interests against the misuse or unauthorized use of their personal information. For example, before collecting or using an email address or phone number, organizations must obtain explicit consent from consumers and must inform consumers of the purpose and scope of the use of the information. Organizations may face fines or other legal penalties if they violate these regulations.

In the United States, consumers of personal health data have the following rights:

(1) Right to know: Consumers have the right to know the purpose, scope, method and time of collection, use, sharing and disclosure of their personal health data.

(2) Right of access: Consumers have the right to access their personal health data and may request a copy of the data from the data controller.

(3) Right to object: Consumers have the right to object to the collection, use, sharing and disclosure of their personal health data by the data controller, and may request the data controller to stop collecting, using, sharing and disclosing their personal health data.

(4) Right to complain: Consumers have the right to lodge a complaint with a supervisory authority about violations of HIPAA regulations and other relevant regulations by the data controller.

4 PERSONAL HEALTH DATA PROTECTION IN ASIAN COUNTRIES

4.1 Japanese

Article 21 of the 1946 Constitution states: "Freedom of assembly, association and freedom of speech of the press and all other forms of expression shall be guaranteed[7]; Censorship shall not be maintained and the secrecy of any means of communication shall not be violated." Article 35: "The right of all persons to be secure in their homes, papers and effects, against entry, search and seizure, shall not be impounded unless there are good grounds for issuing a search warrant and specifying the place to be searched and the things to be seized; each search or seizure shall be carried out on the basis of a separate warrant issued by the competent judicial officer"[8].

The 1988 Act for the Protection of Computer-Processed Personal Data Held by Administrative Organs regulates the use of personal information in computer files held by government agencies[9]. It is based on OECD guidelines and sets out obligations for safety, access and correction. Agencies must limit the information they collect to relevant information and publish a bulletin listing their file systems. Information collected for one purpose cannot be used "for purposes other than the purpose for which the file is kept"[9]. The Act is overseen by the Government Information Systems Planning Division of the Agency for Management and Coordination.

4.2 China

The Personal Information Protection Law of the People's Republic of China is the first special law on the protection of personal information in China. Since then, China has formed a network legal system with the Network Security Law, Data Security Law and Personal Information Protection Law as the core, providing the basic institutional guarantee for data application and the protection of personal information rights and interests.

In 2018, the National Health Commission of the People's Republic of China issued the "National Health Care Big Data Standards, Security and Service Management Measures (Trial)" (National Health Planning Issue (2018) No. 23). It requires to strengthen the security management of the collection, storage, utilization and sharing of medical big data services, highlights the main responsibilities of responsible units, and strengthens the supervision responsibilities of regulatory departments. The "Data Security Law of the People's Republic of China" was officially implemented on September 1, 2021. It requires all regions and departments to be responsible for the data collected and generated in the work of their regions or departments and data security. In the healthcare industry, personal healthcare data is even more important.

On March 7, 2023, the National Data Bureau was established to coordinate the integration, sharing, development and utilization of data resources and promote the construction of digital China. It can be seen that the Party and the state attach great importance to data governance and utilization in the field of healthcare. The construction of a data basic system and the improvement of legislation are currently major issues that the Party and the state need to solve urgently.

5 CONCLUSION

5.1 Comprehensive Comparative Analysis among Different Jurisdictions

5.1.1 Enacting personal information protection law and corresponding specific sectoral laws as the basis for personal health data protection

Countries such as Japan, the United States, and Germany have enacted specific personal information protection laws, and some have added relevant provisions to other sectoral laws, such as Switzerland and France, which have incorporated legal protection of privacy into their civil and criminal codes. In addition, Switzerland has added

special rules relating to the protection of workers' privacy from surveillance, telecommunication information, health care statistics, professional confidentiality including medical and legal information, medical research, police files and identity cards.

5.1.2 Establishing a special department to regulate personal health information

Switzerland established the Federal Data Protection Commission under the Federal Data Protection Act 1992, which maintains and publishes a register of data files, supervises data protection matters of the federal government and private organizations, provides advice, issues recommendations and reports, and conducts investigations. It is also responsible for consultations with the private sector. The German Federal Data Protection Commission is responsible for supervising the Data Protection Act. The Federal Data Protection Commissioner maintains a register of automated databases containing personal information, which is accessible to the public. The Commissioner is also vested with the right to prosecute. These agencies are responsible for supervising and protecting the processing of personal data in their respective countries and ensuring the enforcement of data protection regulations. They undertake duties such as supervision, investigation, issuance of recommendations and adjudication to safeguard the rights and interests of data subjects and data protection compliance.

5.1.3Moving closer to international standards

In terms of enacting or strengthening privacy legislation, a number of countries in the Human Asia-Pacific region have taken inspiration from the European Union's (EU) General Data Protection Regulation (GDPR) by adopting, or planning to adopt, similar or more strict regulations. One example is Japan, which in 2019 received sufficient approval from the European Commission to enable frictionless data sharing between the EU and Japan[10]. In many ways, the GDPR is the most successful privacy law to date, moving toward global harmonization and impacting the Asia-Pacific region both directly and indirectly.

5.2 Proposals for Improving the Legal Protection of Personal Health Data in China

5.2.1 Clarifying the definition and scope of personal health data, the rights of data subjects and the obligations of data holders

Clarifying the definition and scope of personal health data is the basis for improving the protection of personal health data in China. Only by clearly including personal health data in the scope can we ensure that these data are protected by relevant laws. At the same time, clarifying the definition and scope of personal health data can also facilitate data management and utilization. In addition, clear definitions and scopes also provide clearer legal references for law enforcement and enable better handling of cases related to personal health data in judicial practice.

The formulation of laws and regulations should also clearly stipulate the rights of data subjects and the obligations of personal data holders. Effective monitoring mechanisms and complaint channels should be established, and mechanisms for penalizing violations should be implemented, so as to safeguard the rights of data subjects and supervise the fulfillment of obligations by personal data holders.

5.2.2 Strengthening cooperation among relevant departments and establishing a department specialized in personal health data protection

China's current personal health data protection involves the cooperation and supervision of multiple departments. The National Health and Wellness Commission (NHSC) is mainly responsible for formulating and supervising relevant policies and norms in the healthcare industry, while the State Drug Administration (SDA), the State Medical Protection Administration (SMPA), and other departments are also involved in the protection of personal health data [11]. On top of that, local departments such as provincial health commissions, drug regulatory bureaus, and medical protection bureaus also have similar responsibilities. As can be seen, there is currently no separate department for personal health data protection in China, and regulatory functions are relatively decentralized. However, as the importance of personal health data becomes more and more prominent, China can learn from the regulatory measures of other countries and strengthen the cooperation of relevant departments or set up a specialized department in order to pool expertise and resources to develop and implement more unified protection standards.

5.2.3 Making timely theoretical and institutional innovation based on international standards

Through comparative research, this paper finds that many countries outside the region as well as regional international organizations have developed some advanced practices in the legal protection of personal health data. China can learn from foreign data protection models and form a legal protection mechanism with Chinese characteristics by combining China's basic national conditions and legal status quo; at the same time, it can give full play to the potential of international cooperation, provide a variety of legal tools for the protection system, and provide all-around protection of personal health data, so as to better safeguard the privacy of Chinese citizens.

COMPETING INTERESTS

The authors have no relevant financial or non-financial interests to disclose.

ACKNOWLEDGEMENT

This work is supported by the Innovation Project of University Students of Guangdong Province [X202311846077]. The authors thank Dr. Zhaoxia Deng, the assistant professor of the Guangdong University of Foreign Studies, for her guidance during the completion of this paper.

REFERENCES

[1] Santa Slokenberga, Jane Reichel, Rachel Niringiye, June Okal. EU data transfer rules and African legal realities: is data exchange for biobank research realistic?. 2019, (1),30-48.

[2] Santa Slokenberga. Biobanking and data transfer between the EU and Cape Verde, Mauritius, Morocco, Senegal, and Tunisia: adequacy considerations and Convention 108. 2020.

[3] Chen Qian, Zhang Zhicheng. Legal Protection of Sensitive Personal Data: EU Legislation and References. Journal of Xiangtan University (Philosophy and Social Science). 2018, (03), 34-38. doi: 10.13715/j.cnki.jxupss.2018.03.007.

[4] Nóra Ni Loideain. Regulating health research and respecting data protection: a global dialogue. 2020, (2),115-116.

[5] Bradford Laura,Aboy Mateo & Liddell Kathleen. International transfers of health data between the EU and USA: a sector-specific approach for the USA to ensure an 'adequate' level of protection. 2020, (1), lsaa055-lsaa055.

[6] Li Yang. U.S. Senators Introduce the Personal Health Data Protection Act to protect consumer health data privacy. Internet World. 2019, (06), 57.

[7] 2015 APEC PRIVACY FRAMEWORK.

[8] Asia Pacific Data Protection and Cybersecurity Guide 2020.

[9] Asia Pacific Data Protection and Cyber Security Guide 2017.

[10] Unity in Diversity The Asia Pacific Privacy Guide, July 2019.

[11] Yuanxin Li, Darina Saxunová. A perspective on categorizing Personal and Sensitive Data and the analysis of practical protection regulations. 2020, 1110-1115.