Advances in Economics, Business and Management Research, volume 185
Proceedings of the 1st International Symposium on Innovative Management and Economics (ISIME 2021)

Personal Information Security in the Context of the Epidemic Prevention and Control

Qipeng Hu[1,*]

[1] *School of Law, Humanities and Sociology, Wuhan University of Technology, Wuhan, Hubei, China*
[*] *Corresponding author. Email: 328118020@qq.com*

ABSTRACT
With the continuous application of new technologies and the rapid development of society, the meaning of personal information has surpassed the scope of privacy, and is continuously extended and expanded. The security of citizens' personal information has also attracted more and more attention. Since the outbreak of COVID-19, the collection, monitoring, analysis, and application of personal information related to the epidemic prevention and control have been overwhelming, and the security of citizens' personal information has become more and more prominent. During the epidemic, issues such as the unclear procedures for collecting and using personal information, the failure of the principle of informed consent, and the imperfect legal system related to the protection of personal information have further magnified the challenges faced by personal information security. During the epidemic, it is particularly important to correctly understand the division of personal information and personal privacy, rationally analyze the legal regulations of personal information application, balance epidemic prevention and control and personal information protection, and properly resolve personal information security risks. The security of citizens' personal information should be protected by perfecting the construction of legal system, clarifying the principle of information protection, and tapping the potential of information protection technology.

Keywords: *Epidemic prevention and control, Personal information security, Privacy, Legal regulation.*

1. INTRODUCTION

Since the outbreak of COVID-19, China was the first to be hit by the strong impact of the epidemic. Due to the need for epidemic prevention and control, all provinces and cities across China have successively initiated first-level responses to major public health emergencies and adopted certain control measures. All sectors of society have worked together to fight against the epidemic. In this process, Internet technologies such as big data and cloud computing have been further widely used. The anti-epidemic technology based on information and data has achieved positive results in virus traceability, regional prevention and control, personnel monitoring, convenience for people's lives, and resumption of work and production. At the same time, there have some situations in which citizens' personal information has been exposed, leaked, sold, illegally used, etc., which not only aggravated citizens' doubts about personal information security, hindered normal epidemic prevention and control, but also gave criminals an opportunity to take advantage of the situation and threatened the personal and property safety of citizens. On February 4, 2020, the Office of the China Central Cyber Security and Informatization Commission issued the "Notice on Doing a Good Job in Personal Information Protection and Using Big Data to Support Joint Prevention and Control Work", fully highlighting the importance that the competent government departments attach to the protection of personal information during the epidemic. However, in the actual work of personal information protection during the epidemic period, various regions still have the problems of uneven protection strength, scope, methods, and effects. During the epidemic period, there is still room for further discussion and improvement of personal information protection.

2. THE REAL DILEMMA OF PERSONAL INFORMATION SECURITY DURING THE EPIDEMIC

The large-scale collection and use of personal information is an important foundation and a powerful weapon for the overall prevention and control of the epidemic, at the same time, it will inevitably increase the risk of personal information security issues. Personal information security issues concern every citizen of the country that provides personal information. During the epidemic, personal information security issues have repeatedly appeared in the media, constantly stimulating the sensitive nerves of the public and arousing collective worries in society.

2.1 The Situation of Personal Information Security During the Period of Epidemic Prevention and Control

During the epidemic, the collection and use of personal information is different from that in peacetime, involving a wider range, having greater impact, and being more targeted and more prone to have risks and problems.

2.1.1 The Collection of Personal Information

First, the collection content of personal information covers a wide range. Personal information includes name, address, ID number, contact information, license plate number, work unit, contact history, kinship, physical examination report, current medical condition information, individual biometric information, etc. And some personal information are required to be extremely detailed, with a tendency of generalize. Second, the subjects of personal information collected vary greatly. The subjects of personal information collected include people's governments at all levels, health administrative departments, communities, village committees, community properties, hospitals, media, non-profit organizations, enterprises that resume work, Internet companies, etc. Generally speaking, the focus of different subjects that collect personal information is different, and the scope and limits of information collection should be different. However, not all institutions and units are qualified to collect personal information. Third, there are various ways of collecting personal information. The collection methods of personal information are various, such as personal and vehicle information registration at road checkpoints, inspections to measure body temperature, travel application forms during regional control, tracking and investigation of the travel records and contact history of infected patients, health reports submitted by people returning to work and production, mobile apps or Internet software, etc. for information filling. Generally speaking, according to the personal wishes of information subjects, it can be divided into active reporting and passive collection; according to the channels of personal information collection, it can be divided into written collection and network collection; according to the scope of personal information collection involving information subjects, it can be divided into comprehensive investigations and key monitoring, etc. A wide variety of information collection methods ensure the comprehensive, efficient and accurate information collection, and also provide more means and opportunities for infringing on personal information.

2.1.2 The Use of Personal Information

First, from the perspective of the purpose of use, there are legitimate and improper uses. The vast majority of personal information is used for the epidemic prevention and control. In order to promote the public interest, personal information is used for scientific overall decision-making, virus traceability and isolation, epidemic trend prediction, early warning of epidemic risk, vaccine clinical research and development, and reasonable deployment of materials, which is justified. At the same time, personal information is used for profit, advertising, fraud, discrimination and insults in the name of epidemic prevention and control, and it is even suspected of illegal crimes. Second, from the perspective of users, personal information should be used correctly by institutions or organizations authorized or permitted by law, but there are still problems that unqualified subjects disclose personal information without authorization, causing social panic. Third, from the perspective of usage limits, there are cases where personal information is used beyond the necessary limits. Personal information related to personal privacy and security, such as ID numbers and home addresses of some patients diagnosed with COVID-19, was disclosed, which exceeded the reasonable use scope of personal information.

2.2 Personal Information Protection Drivers During the Epidemic Prevention and Control Period

Protecting the security of citizens' personal information is not only an inevitable requirement for epidemic prevention and control, but also the manifestation of the concept of people-oriented development. During the epidemic, the collection, use and protection of personal information are interrelated and mutually promoted. Therefore, to prevent and control the epidemic, personal information protection must be paid attention to.

The name, ID number, address, communication method, whereabouts, medical files and other personal information collected during the epidemic are relatively complete and authentic. Once such information is leaked, it may be used by criminals and become the basis of such illegal acts of a precision fraud, threatening the personal and property safety of citizens and affecting social stability. Therefore, the protection of citizens' personal information is a need to protect individual citizens, and it is also a need for the construction of the rule of law.

The effective protection of personal information during the epidemic can reduce citizens' concerns about personal information security to a certain extent, and is beneficial to encourage and guide citizens to actively cooperate with relevant epidemic prevention and control departments and agencies in the necessary information collection work, so as to ensure the effective circulation of personal information and help the epidemic prevention and control.

The personal information collected during the epidemic contains a large amount of sensitive information and personal privacy, and carries other legitimate rights and interests worthy of legal protection, such as privacy rights, name rights, and portrait rights. Protecting the personal information of patients can effectively prevent others from harming the personal dignity of the information subject in the name of epidemic prevention and control, prevent the information subject from being subjected to discriminatory treatment, and can also avoid the negative social impact caused by information leakage. [1]

2.3 Personal Information Security Concerns During the Epidemic Prevention and Control Period

During the epidemic prevention and control period, the list of confirmed patients went viral, personal information was sold for profit, and fraudulent text messages emerged one after another. Social incidents caused by personal information security issues have repeatedly emerged, indicating that there are still deficiencies in personal information protection.

2.3.1 The Standards for Information Collection and Use Are Not Clear

During the COVID-19, the requirements and standards for epidemic prevention and control in different regions are also different, leading to huge differences in the content and methods of personal information collection. In addition, there is no unified standard for personal information filling, which causes citizens to face various information filling requirements. At the same time, it is difficult to distinguish and judge whether there is excessive collection of personal information by itself, which is not conducive to citizens' spontaneous implementation of personal information protection. There are also problems of repeated collection of personal information, poor information sharing, and excessive information disclosure.

2.3.2 The Principle of Informed Consent Is Invalid

The principle of informed consent refers to the principle that when collecting personal information, the information provider should fully inform the information subject of the collection, processing and utilization of relevant personal information, and obtain the explicit consent of the information subject. The principle of informed consent is the basis for the protection of personal information. In practice, the information provider regards the principle of informed consent as the "universal rule" for the collection of personal information. [2] However, in the collection activities of personal information during the epidemic prevention and control period, there were cases where the principle of informed consent was not followed. In the epidemic prevention and control, virus screening, emergency rescue, and material deployment are racing against time to improve efficiency. Under such special circumstances, following the principle of informed consent will consume a lot of time,

manpower and material costs, which is not in line with epidemic prevention and control. Therefore, the principle of informed consent is invalid, but this also opens a gap for the protection of personal information.

2.3.3 Personal Information Interests Conflict with Social Public Security

Personal information includes personality attributes and property attributes, and these two attributes can be fully reflected in the process of social interaction, and the use of personal information can generate economic benefits. [3] According to the law, in the process of epidemic prevention and control, the information subject must unconditionally cooperate with relevant departments and institutions to collect personal information for the need of social and public security, and the relevant departments can use the collected personal information reasonably and legally. Therefore, the information subject has also sacrificed potential personal economic interests to a certain extent, and balancing the contradiction between personal interests and public safety is directly related to the overall stability of the epidemic prevention work.

3. ANALYSIS ON THE STATUS QUO OF CHINA'S PERSONAL INFORMATION PROTECTION LAWS

China has not yet issued a special law on the protection of personal information, and the relevant regulations on the protection of personal information are scattered among numerous laws and regulations. "The General Principles of the Civil Law", "the Law on the Prevention and Control of Infectious Diseases", etc. only provide principled provisions for personal information. "The Criminal Law" stipulates the crime of infringing on citizens' personal information, and people shall bear legal responsibility for serious disclosure of citizens' personal information. However, this is the accountability after the fact, does not play a role in precautions. Therefore, the protection of personal information during the epidemic still lacks a systematic and complete legal basis.

3.1 Protection of Personal Information in the Constitutional Field

In China, the right to personal information is not explicitly included in the basic rights of citizens in the "Constitution". Article 38 of "the Constitution" stipulates that the dignity of citizens is not violated. It is forbidden to use any method to insult, slander, and falsely accuse citizens." Personality rights are the basic rights of Chinese citizens, and personal information is an important part of personality rights and is also protected by "the Constitution". This is constitutional basis for legal protection of citizens' personal information in China. [4]

3.2 Personal Information Protection in the Field of Civil Law

According to Article 111 of the "General Principles of the Civil Law", the personal information of natural persons is protected by law. Any organization or individual who needs to obtain the personal information of others shall obtain and ensure the safety of the information in accordance with the law, and shall not illegally collect, use, process or transmit the personal information of others, and shall not illegally trade, provide or disclose the personal information of others. This is a new personal information protection clause added to the "General Regulations of the Civil Law". This clause attaches importance to the legality of the source of personal information. Article 36 of the "Tort Liability Law" also stipulates the respective rights and responsibilities of network service providers, infringed persons and users, and also stipulates the privacy rights of citizens in the field of private law. Citizen privacy is closely related to personal information, and the protection of privacy has greatly promoted the protection of personal information.

3.3 Personal Information Protection in the Field of Criminal Law

Article 253 of the "Criminal Law" stipulates that in violation of relevant state regulations, selling or providing personal information of citizens to others (the circumstances are serious) shall be sentenced to fixed-term imprisonment of not more than three years or criminal detention, concurrently or solely with a fine; if the circumstances are particularly serious, the punishment shall be sentenced to fixed-term imprisonment of not less than three years but not more than seven years, with a fine. The "Criminal Law" stipulates the crime of

infringing on citizens' personal information, clarifies that citizens' personal information is protected by the criminal law, and has a strong deterrent effect, effectively deterring and cracking down on illegal acts infringing on citizens' personal information.

3.4 Personal Information Protection in the Internet Field

Article 2 of the "Decision on Strengthening the Protection of Network Information" stipulates: "in their business activities, network service providers and other enterprises and institutions shall collect and use citizens' personal electronic information, follow the principles of lawfulness, fairness and necessity, clarify the purpose, method and scope of collecting and using information, and collect and use information in accordance with the provisions of laws and regulations and the agreement of both parties with the consent of the collected person." Article 41 of "the Cybersecurity Law" stipulates: "when collecting and using personal information, network operators should follow the principles of legality, propriety and necessity, make public the collection and use rules, clearly state the purpose, method and scope of the collection and use of information, and obtain the consent of the collected person." "The Decision on Strengthening the Protection of Network Information" and "the Cyber Security Law" clearly define the principles for the collection and use of personal data, emphasize that personal data should not be collected illegally, and enrich the construction of the legal system for the protection of personal information. However, this is only for the field of the Internet, and has certain limitations.

4. LEGAL REGULATIONS ON THE USAGE OF PERSONAL INFORMATION DURING THE EPIDEMIC

During the epidemic prevention and control period, a small number of citizens refused to provide personal information necessary for epidemic prevention or concealed personal information on the grounds of protecting personal privacy, and questioned the eligibility and legitimacy of personal information collection and use, which triggered widespread discussion in the society. On the one hand, this reflects citizens' concerns about the security of personal information. On the other hand, it also shows that citizens have problems such as unclear distinction between personal information and personal privacy, unclear cognition of the subject qualification and use scope of personal information. Therefore, it is of practical significance to delimit the scope of personal information and personal privacy and to identify the qualifications for the collection and use of personal information.

4.1 Discrimination of Personal Information and Personal Privacy

Personal information is a concept that is constantly evolving and changing. With the advancement of society and the application of new technologies, the connotation of personal information is constantly expanding and extending. In today's society, personal information refers to various personal identification information that can distinguish a natural person from others, as well as personal information of words and deeds, data information, etc. that form a corresponding relationship with personal identification information, including name, ID number, and communication contact information, residential address, account password, property status, whereabouts and other information. It can be seen that there are two points to be grasped in the definition of personal information. One is that the subject must be a natural person, and the other is that the information is identifiable. [5]

The legislation of various countries in the world does not clearly define the concept and meaning of personal information and personal privacy. However, it is an indisputable fact that personal information and personal privacy are closely related. Article 12 of the "Universal Declaration of Human Rights" stipulates: "No one shall arbitrarily interfere with others' privacy, family, house or communication, and shall not attack others' dignity or reputation. Everyone has the right to obtain legal protection against such interference or attacks." Article 8 of the "European Convention on Human Rights" stipulates: "Everyone has the right to protect his private and family life, his house and communications." This is the most authoritative source of international law in protecting personal privacy. [6] There are also different interpretations of privacy in China. For example, "the so-called privacy refers to personal private affairs and personal information that are unknown by others." [7] "The privacy refers to the private life and private information owned by natural persons." [8] "The privacy refers to personal life, personal information and private field." [9]

Generally speaking, with the rapid development of information technology, the scope of personal information has far exceeded privacy [10]. In theory, some scholars put personal information into the category of privacy [11], but the two aspects focus on the different items. Personal privacy is more focused on information that people do not want to disclose. In addition to personal privacy, personal information also contains other identifiable information. Although personal information and privacy are for the purpose of maintaining human dignity [12], but it cannot simply equate personal information with personal privacy.

4.2 Legal Identification of Personal Information Collection During the Epidemic

Item 1 of Article 12 of the "Law of the People's Republic of China on the Prevention and Control of Infectious Diseases" stipulates: "All units and individuals within the territory of the People's Republic of China must accept preventive and control measures, such as investigation, testing, collection of samples and isolation for treatment of infectious diseases by disease prevention and control agencies and medical institutions, and truthfully provide relevant information. Disease prevention and control institutions and medical institutions shall not divulge relevant information and materials involving personal privacy". Article 18 and Article 19 of the "Emergency Response Law of the People's Republic of China" stipulate that in the detection and early warning stage, the State Council shall establish a unified national emergency information system. "The people's government at or above the county level and its relevant departments and professional institutions should collect information on emergencies through multiple channels." Article 40 of the "Regulations on Public Health Emergency Responses" stipulates: "When infectious diseases break out or become prevalent, neighborhoods, towns, neighborhood committees, and village committees should organize forces and cooperate in unity, make the prevention and treatment in groups, assist the health administrative department, other relevant departments, and medical and health institutions to collect and report epidemic information, decentralize personnel, implement public health measures, and publicize the knowledge of prevention and control of infectious diseases to residents and villagers."

Based on this, during the epidemic period, people's governments at all levels, health administrative departments at all levels, communities, village committees, sub-district offices, medical institutions, and professional technical institutions designated by other relevant departments have a legal basis for collecting residents' personal information. No other unit or individual may collect and use personal information without the consent of the person being collected on the grounds of epidemic prevention and control and disease prevention.

However, in actual situations, companies need to cooperate with disease control agencies in the collection, investigation, and reporting of personal information related to the epidemic. There is a certain controversy as to whether authorization and consent are still required by such personal information processing activities. In accordance with the "regulations on personal information security", "it is important to obtain authorization and consent", and "there are situations directly related to public safety, public health, and major public interests". As required or entrusted by competent authorities, enterprises shall conduct analysis, utilization and research on user data to assist in epidemic prevention and control, or cooperate with Centers for Disease Control (CDC) in collecting, screening and submitting personal information related to epidemic, without obtaining authorization. [13]

Regarding the collected information, the laws also have clearly stipulation, which is, "being related to the epidemic" or "being related to infectious diseases". During this epidemic, the collection of information of ordinary people should be limited to contact information, travel history, contact history, current disease symptoms and other necessary information for epidemic prevention and control, while private information such as ID numbers and work units should not be disclosed.

4.3 Legal Identification of the Use of Personal Information During the Epidemic

Item 3 of Article 38 of the "Law on the Prevention and Control of Infectious Diseases" stipulates: "When an infectious disease breaks out or spreads, the health administration department of the State Council is responsible for publishing information on the epidemic situation of the infectious disease to the public, and may authorize the health administration department of the people's

government of provinces, autonomous regions, and municipalities to provide information to the public, and publish the information on the epidemic situation of infectious diseases in this administrative region." Article 53 of the "Emergency Response Law" stipulates: "The people's government that performs unified leadership responsibilities or organizes the handling of emergencies shall publish relevant information on the development of the incident and emergency response work in a unified, accurate and timely manner in accordance with relevant regulations."

According to the laws, the State Council, the people's governments at all levels, and the health administrative departments of the provincial governments have the right to publish information on epidemic prevention and control to the public. Any other organization or individual, including communities, village committees, and administrative staff, has no right to publish personal information of residents. Regarding the personal information collected or possessed, relevant agencies shall keep it properly to prevent it from being stolen or leaked; information shall not be used for purposes other than the epidemic; information shall not be disclosed without the consent of the person being collected.

In summary, during the epidemic period, organizations or authorized enterprises that meet the requirements of the law have the right to collect and use personal information related to the epidemic in accordance with the law. There is no legitimate basis for the fact that citizens refuse to provide personal information necessary for epidemic prevention work or conceal personal information on the grounds of protecting personal privacy. However, the relevant departments should take necessary measures to protect the security of personal information so as not to affect the credibility.

5. COUNTERMEASURES FOR PERSONAL INFORMATION SECURITY DURING THE EPIDEMIC

The protection of personal information during the epidemic requires multi-party collaboration and joint efforts, but at the same time, it is necessary to pay attention to the huge demand for personal information applications during the epidemic, so as to avoid excessive protection that affects the overall situation of epidemic prevention. Personal information protection is based on the continuous improvement of the legal system. It is suggested to strengthen industrial supervision, innovate technological means, and reasonably grasp the limits of personal information protection.

5.1 Improving the Construction of Legal System for Personal Information Protection

To protect the security of personal information, it is not enough to rely solely on various departmental laws and local regulations. It is necessary to promote the formulation of a special protection law of personal information, improve the construction of a legal system of personal information protection, guide the improvement of administrative regulations and local regulations by higher laws, and use a clear legislative basis to protect citizens' personal information security. [14]

5.2 Promoting the Combination of Personal Information Protection and Utilization

The protection of personal information should follow the principles of legal disclosure, purpose limitation, minimum scope, information security, and time-limited storage to ensure that personal information can be reasonably, legally, and effectively used in epidemic prevention and control to safeguard public interests. [15] It is suggested to encourage and support multiple data subjects to participate in the protection and benefits of personal data information, and create a pattern of joint construction, governance and sharing for the protection and use of personal data information. [16]

5.3 Strengthening the Industrial Supervision of Personal Information Protection

During the epidemic period, all walks of life have grasped a large amount of personal information of citizens to a certain extent. Administrative authorities such as the Public Security, Market Supervision Bureau, and the Office of Cyberspace Affairs should strengthen the supervision of the industries' collection of personal information during the epidemic, and crack down on violations of the collection, use, disclosure and disposal of personal information, and guide all walks of life to protect the security of citizens' personal information.

5.4 Tapping the Innovation Potential of Personal Information Protection Technology

It is suggested to improve the security of personal information with the help of new Internet technologies such as blockchain. The anti-epidemic technology represented by Internet technology has made great contributions to the prevention and control of the epidemic, but at the same time, it is accompanied by more security risks and no lack of qualitativeness. Relevant departments and enterprises should continue to develop and apply safer and more reliable new technologies to fill in gaps in information protection in technology and reduce unnecessary exposure of personal information.

6. CONCLUSION

Epidemic prevention and control and personal information security are the focal points of the common concern of all sectors of society. While fighting against the epidemic, protecting citizens' personal information is a topic that requires in-depth research. A correct understanding of the current situation and characteristics of personal information security during the epidemic, and a reasonable grasp of the limits of personal information collection and use during the epidemic, will help balance the relationship between epidemic prevention and control and personal information protection. The establishment of a legal system of personal information protection should be accelerated, the principles of personal information protection during the epidemic should be clarified, the implementation of relevant rules and regulations should be strictly supervised, the innovation investment in information protection technology should be increased, and a comprehensive, integrated, and targeted personal information protection system should be built , so as to maximize the protection of citizens' personal information security.

AUTHORS' CONTRIBUTIONS

This paper is independently completed by Qipeng Hu.

REFERENCES

[1] Shi Cheng. Legal protection of personal information in the prevention and control of major epidemics [J]. Journal of China University of Mining & Technology (Social Science Edition), 2020, 22(02): 63-74. (in Chinese)

[2] Zhang Xinbao. Collection of Personal Information: Restricting the Application of the Principle of Informed Consent [J]. Journal of Comparative Law, 2019(06): 1-20. (in Chinese)

[3] Tian Wei. Civil law protection of personal data rights under the big data environment [D]. Guizhou University, 2017. (in Chinese)

[4] Shao Guosong. "The Right to be Forgotten": A New Proposal for Personal Data Protection [J]. Social Sciences in Nanjing, 2013. (in Chinese)

[5] James B. Rule, Graham Greenleaf. Global Privacy Protection [M]. Edward Elgar Publishing, 2010: 81.

[6] Yan Li, Wu Heqi. The Value and Privacy Risks of Deploying AI in Handling a Public Health Emergency:Also on a Criminal Law-based Approach to Privacy Protection [J]. Journal of Nanjing Normal University (Social Science Edition), 2020(02): 32-41. (in Chinese)

[7] Liu Kaixiang. General Theory of Civil Law [M]. Beijing: Peking University Press, 2006: 149. (in Chinese)

[8] Zhang Xinbao. Legal protection of privacy right [M]. Beijing: People's Publishing House, 2004: 12. (in Chinese)

[9] Ma Junju. Lectures on the Theory of Personality and Personal Rights [M]. Beijing: Law Press, 2009: 260. (in Chinese)

[10] Li Xiaohui. Research on Information Rights [M]. Beijing: Intellectual Property Press, 2006:118-119. (in Chinese)

[11] Adam Carlyle Breckenridge. The Right to Privacy 1 [M]. University of Nebraska Publishing, 1970.

[12] James Q.Whitman. The Two Western Cultures of Privacy: Dignity Versus Liberty[J]. Yale Law Journal, 2004, (113): 1151-1221

[13] Liu Xuetao. How to balance the prevention and control of COVID-19 and the protection of personal information [N]. The Democracy and Legal System, 2020-02-29 (002). (in Chinese)

[14] Jiang Bolong. Analysis on the Path of Legal Protection of Personal Information [J]. Journal of Shenyang Official, 2020, 22(01): 37-41. (in Chinese)

[15] Han Xinyuan. The collection and use of personal data should follow the five principles [N]. Procuratorate Daily, 2020-03-28(003). (in Chinese)

[16] Mao Muran. On the Legal Obstacles of China's "Act on the Protection of Personal Information" and its solutions [J]. Journal of Soochow University, 2020, 41(01): 59-68. (in Chinese)