

Research on the Legal Regulation of Personal Information Protection and Utilization in the Prevention and Control of COVID-19 Epidemic

Weimin Ouyang^{1,*}

¹*Shanghai University of Political Science and Law, Shanghai, 201701, China*

^{*}*Corresponding author. Email: oywm@shupl.edu.cn*

ABSTRACT

In the prevention and control of COVID-19 epidemic in China, big data technology provides crucial scientific and technological support. Big data technology, on the one hand, played a huge role in the key issues of the prevention and control of COVID-19 epidemic that quickly identify potential infections, on the other hand, because China's laws and regulations are not sound on the protection and utilization of personal information, there are legal obstacles in the collection, utilization and sharing of personal information. It is not conducive to making full use of personal information in prevention and control of COVID-19 epidemic. To this end, this paper combed the relevant laws and regulations on the protection and utilization of personal information in China, especially the laws and regulations on the protection and utilization of personal information under the situation of epidemic prevention and control, studied the complex legal relationship between them, and proposed promulgating the Personal Information Protection Law, as a long-term mechanism, to construct China's legal standard system for the protection and utilization of personal information, and proposed that the National People's Congress of China should issue an emergency bill according to the work needs, giving the government the power to deal with emergencies.

Keywords: *prevention and control of epidemic; personal information; sensitive information; legal regulation*

1. INTRODUCTION

On December 31, 2019, the official website of Wuhan Health Committee issued the Report of Wuhan Health Committee on the Current Pneumonia Epidemic Situation in our city [1], which disclosed for the first time 27 cases of pneumonia of unknown cause related to South China Seafood City, which have been confirmed as acute respiratory infectious disease caused by COVID-19. This pneumonia epidemic in COVID-19 coincides with the peak of migration during the Chinese New Year, which brings severe challenges to the prevention and control of the epidemic. For example, 5 million people left Wuhan before the implementation of travel control. Obviously, there must be a significant number of people infected with COVID-19 among these 5 million people, and these infected people have become the source of pneumonia in COVID-19.

Therefore, where these 5 million people went became the focus of epidemic prevention and control. At this time, big data technology has played a huge role in quickly and accurately identifying infected persons and potentially infected persons.

For example, transportation departments such as aviation, railway, highway and ferry search and analyze passenger travel data, three major operators such as China Mobile, China Unicom and China Telecom accurately locate users' mobile phone positions based on mobile phone signaling, Internet enterprises call users' mobile phone location data,

mobile travel services provided by apps such as navigation software and taxis, delivery address data in apps such as e-commerce and take-out platforms, and mobile payment position data, etc., all of which can obtain user location information. On the one hand, big data technology plays an irreplaceable role in solving the key problem of quickly identifying potential infected persons; on the other hand, due to the imperfect legislation of personal information in China, big data technology has the risk of violating laws and regulations in the collection, utilization and sharing of personal information.

2. PERSONAL INFORMATION ISSUES SUCH AS WHEREABOUTS IN EPIDEMIC PREVENTION AND CONTROL

The Prosecution Opinion holds that the criminal suspect Lu Yong's behavior violated the first paragraph of Article 177-1 of the Criminal Law of the People's Republic of China, and was suspected of obstructing the credit card management.

Under the situation of advancing the modernization of national governance system and capacity, it is high time to use big data technology to improve emergency handling and emergency management capabilities. The harsh reality of epidemic prevention and control requires the collection and utilization of a large amount of personal information.

However, due to the incomplete legislation of personal information in China, big data technology has the risk of violating laws and regulations in the collection, utilization and sharing of personal information. It is necessary to strike a balance between the use and protection of personal information in epidemic prevention and control. Therefore, we briefly analyze the domestic laws and regulations related to the protection and utilization of personal information in epidemic prevention and control.

2.1. Relevant provisions on personal information in China's information network laws and regulations

Article 1 of the Decision of The Standing Committee of the National People's Congress on Strengthening Network Information Protection adopted at the 30th meeting of the 11th National People's Congress in The Standing Committee on December 28, 2012 stipulates that the state protects electronic information that can identify citizens' personal identity and involve citizens' personal privacy [2]. No organization or individual may steal or obtain citizens' personal electronic information by other illegal means, or sell or illegally provide citizens' personal electronic information to others. This regulation does not put forward the term personal information, but it makes a general regulation on personal information, and its content is rather abstract.

On July 16, 2013, Order No.24 of the Ministry of Industry and Information Technology of the People's Republic of China promulgated the Regulations on the Protection of Personal Information of Telecommunications and Internet Users [3], which stipulated the standards for the collection and use of personal information of telecom operators and Internet information service providers, security measures, supervision and inspection, and legal responsibilities. Article 4 of the regulations is as follows: The personal information of users mentioned in these regulations refers to the information collected by telecom operators and Internet information service providers in the process of providing services, such as user name, date of birth, ID number, address, telephone number, account number and password, which can identify users alone or in combination with other information, and the time and place of using the service. Among them, "the time and place of using the service" is actually the personal whereabouts information of the user. Article 9 of this regulation also stipulates the right of informed consent for the collection and use of personal information, as well as the right to inquire and correct personal information, and stipulates that users' personal information other than those necessary for providing services shall not be collected or used for purposes other than providing services.

2.2. The relevant provisions of China's criminal law and civil law concerning personal information

Article 253, Article 253-1 of the Criminal Law stipulates the crime of infringing citizens' personal information, but does not specify what personal information is [4]. Article 111 of General Principles of Civil Law stipulates that personal information of natural persons shall be protected by law [5]. Any organization or individual who needs to obtain other people's personal information shall obtain and ensure information security according to law, and shall not illegally collect, use, process or transmit other people's personal information, or illegally buy, sell, provide or disclose other people's personal information. Like the Criminal Law, there is no definition of personal information.

The crime of infringing citizens' personal information is defined in Article 253-1 of the Criminal Law, but it does not define what personal information is. Article 111 of the General Provisions of the Civil Law provides that the personal information of natural persons shall be protected by law. Any organization or individual that needs to obtain the personal information of others shall obtain and ensure the information security according to law, and shall not illegally collect, use, process or transmit the personal information of others, or illegally buy, sell, provide or disclose the personal information of others. Like the Criminal Law, there is no definition of personal information.

On May 8, 2017, the Supreme People's Court and the Supreme People's Procuratorate issued the Interpretation of the Supreme People's Court and the Supreme People's Procuratorate on Several Issues Concerning the Application of Laws in Handling Criminal Cases of Infringement of Citizens' Personal Information [6]. The first article stipulates that the "citizen's personal information" stipulated in Article 253 of the Criminal Law refers to various information recorded by electronic or other means that can identify the identity of a specific natural person alone or in combination with other information or reflect the activities of a specific natural person, including name, ID number and communication. For the first time, personal information is defined comprehensively, and activity information and identity information are juxtaposed, which are included in the protection scope of criminal law. Moreover, the whereabouts is listed as a separate type of personal information, which is clearly protected.

The Network Security Law of the People's Republic of China [7], which came into effect on June 1, 2017, is the first law in China that clearly stipulates the protection and utilization of personal information. Article 76 (5) of the Law clearly stipulates that personal information refers to all kinds of information recorded by electronic or other means that can identify a natural person's personal identity alone or in combination with other information, including but not limited to the natural person's name, date of birth, ID number, personal biometric information, address,

telephone number, etc. Compared with the Regulations on the Protection of Personal Information of Telecommunications and Internet Users, the content of personal information increases personal biometric information, and reduces the time and place of using the service.

Article 41 of the Network Security Law of the People's Republic of China stipulates that network operators should follow the principles of legality, justice and necessity in collecting and using personal information, publicize the rules for collecting and using information, clearly indicate the purpose, method and scope of collecting and using information, and obtain the consent of the collected person. Network operators shall not collect personal information unrelated to the services they provide, collect and use personal information in violation of the provisions of laws and administrative regulations and the agreement of both parties, and shall handle the personal information stored by them in accordance with the provisions of laws and administrative regulations and the agreement with users. Article 43 stipulates that individuals have the right to delete and correct their personal information, but does not stipulate the right to inquire.

2.3. A brief description of personal information and personal sensitive information

For a long time, the current domestic laws and regulations on personal information are mainly based on the position of information controllers, emphasizing the use of personal information, ignoring the protection of personal information rights, without distinguishing the more sensitive private information in personal information. It was not until the Civil Code of the People's Republic of China was passed on May 28, 2020 that the definition of personal information was formally put forward in the form of law for the first time, and personal information was clearly distinguished from private personal information [8]. Article 1034 of the Civil Code of the People's Republic of China passed on May 28, 2020, the personal information of natural persons shall be protected by law. Personal information is all kinds of information recorded electronic or other means that can identify a specific natural person alone or in combination with other information, including natural person's name, date of birth, ID number, biometric information, address, telephone number, e-mail, health information, whereabouts information, etc.

The above definition of personal information and sensitive personal information is still based on the position of information controller, without considering that general personal information will become sensitive personal information under certain circumstances. For example, an individual's name belongs to general personal information under normal circumstances, but the name of the staff of the state secrecy department is upgraded to personal sensitive information. For example, during the prevention and control of pneumonia in COVID-19, Hubei Province, especially Wuhan City, became a key epidemic area. The

names, addresses and communication contact information of people in this area are upgraded to personal sensitive information, because in this specific case, once this personal information are leaked, illegally provided or abused, it may endanger personal and property safety and easily lead to personal reputation, damage to physical and mental health, or discriminatory treatment, etc.

Whether personal information is sensitive or not depends on the specific situation, which is determined by the scene, and is not static. The same personal information is generally personal information in some scenes, but it may be sensitive personal information in other scenes, and vice versa.

3. PROBLEMS IN CHINA'S PERSONAL INFORMATION LAWS AND REGULATIONS ON EPIDEMIC PREVENTION AND CONTROL

At present, the legal system of personal information protection in China is not perfect, with scattered contents and narrow scope of protection. Below we discuss the problems in China's General and special laws on personal Information concerning epidemic prevention and control.

3.1. Problems in China's General Law on Personal Information concerning epidemic prevention and control

The Network Security Law of the People's Republic of China is the main law for the protection and utilization of personal information. Article 41 of the Law stipulates that when collecting and using personal information, network operators shall follow the principles of lawfulness, justness and necessity, make public the rules for collecting and using information, express the purpose, method and scope of collecting and using information, and obtain the consent of the collected person.

However, passengers' personal information collected by transportation departments such as aviation, railway, highway and ferry, users' personal information collected by China Mobile, China Unicom and China Telecom, personal information collected by Internet companies, navigation software, taxis, e-commerce, take-out platforms, and all these personal information are not collected for epidemic prevention and control. Personal information collected is not used for epidemic prevention and control. According to the provisions of Article 41 of the Network Security Law of the People's Republic of China, the purpose of changing the personal information collected should be approved by the collected person. However, all kinds of data controllers not inform the collected persons when they use personal information in epidemic prevention and control. Because the Network Security Law of the People's Republic of China does not stipulate the exception of informed consent, the Network Security Law of the

People's Republic of China does not provide a legal basis for data controllers to use personal information in the prevention and control of epidemic situation.

In order to make good use and protection of personal information in the prevention and control of pneumonia in COVID-19, the Central Network Information Office published the Notice on Personal Information Protection and Joint Prevention and Control with Big Data on February 9, 2020.

Article 1 of the notice stipulates that all local departments should attach great importance to the protection of personal information. Except the institutions authorized by the health department of the State Council in accordance with the Network Security Law of the People's Republic of China, the Law of the People's Republic of China on the Prevention and Control of Infectious Diseases and the Emergency Regulations for Public Health Emergencies, no unit or individual may collect and use personal information without the consent of the collected person on the grounds of epidemic prevention and control and disease prevention. Unless otherwise provided by laws and administrative regulations, such provisions shall prevail.

Accordingly, the health department under the State Council can authorize specific institutions to collect personal information needed for epidemic prevention and control, without obtaining the consent of the collected person in advance, thus obtaining the exception of informed consent. However, the Network Security Law of the People's Republic of China is a law enacted by The Standing Committee of the National People's Congress, and the Central Network Office has neither the right to amend nor interpret it. Therefore, this notice of the Central Network Office violates Article 97 of the Legislative Law of the People's Republic of China in legal terms. Of course, this is also an extraordinary measure taken due to the emergency of epidemic prevention and control.

3.2. Problems in China's Special Law on Personal Information concerning epidemic prevention and control

The above is the legal response to the general law on personal information in epidemic prevention and control. It can be found that the current general law is insufficient and it is difficult to provide effective legal support for epidemic prevention and control. Now, we examine the special laws related to the protection and utilization of personal information of epidemic prevention and control species.

In the context of epidemic prevention and control, the Law of the People's Republic of China on the Prevention and Control of Infectious Diseases and the Emergency Regulations of Public Health Emergencies are two directly related laws and regulations. According to Article 12, Article 32 and Article 33 of the Law of the People's Republic of China on the Prevention and Control of Infectious Diseases, disease prevention and control institutions and medical institutions have legal authorization to change the purpose of using personal

information in order to control the epidemic situation. However, there is no sub-license right, and other departments have not obtained legal authorization to change the purpose of using personal information according to the Law of the People's Republic of China on the Prevention and Control of Infectious Diseases.

Article 11 of the Emergency Regulations on Public Health Emergencies stipulates the main contents to be included in the national emergency preparedness plan; paragraph (3) stipulates the system of collecting, analyzing, reporting and informing emergency information; paragraph (4) stipulates the emergency treatment technology and monitoring institutions and their tasks.

According to the above regulations, in the prevention and control of pneumonia in COVID-19, the national and local health administrative departments can formulate emergency preparedness plan for pneumonia emergencies in COVID-19 according to law, and can take the collection, analysis, report and notification of personal information as medical measures into the emergency preparedness plan, and stipulate that big data and artificial intelligence technology can be used for personal information processing.

Article 44 of the Regulations stipulates that patients who need isolation treatment and medical observation measures in emergencies, suspected patients and close contacts of infectious disease patients should cooperate when the health administrative department or relevant institutions take medical measures; Refusing to cooperate, the public security organ shall assist in enforcement according to law. In the emergency preparedness plan of pneumonia outbreak in COVID-19, the collection, analysis, report and notification of personal information is regarded as a medical measure. According to Article 44 of the Regulations, the health administrative department and relevant institutions have the power of mandatory collection, analysis, reporting and notification of personal information without seeking the consent of the collected person, thus obtaining the exception of the informed consent of the collected person. However, according to the regulations, the mandatory collection and processing of personal information is limited to known patients who need isolation treatment and medical observation measures, suspected patients who are in close contact with infectious disease patients, and the mandatory collection and processing of personal information is not universal. However, big data analysis technology aims to quickly identify potential infected people in a wider range of unspecified people, and it is necessary to universally obtain the exception of informed consent of the person whose personal information is collected.

To sum up, during the period of pneumonia prevention and control in COVID-19, China's laws and regulations, whether general laws or special laws, could not provide sufficient legal support for the compulsory collection of personal information and changing purpose of the use of personal information. It was not until the Civil Code of the People's Republic of China was passed on May 28, 2020 that the exception of informed consent for personal

information processing was formally put forward in the form of law for the first time.

Article 1036 of the Civil Code stipulates three cases in which the actor does not bear civil liability when handling personal information, and the third case is "other acts reasonably implemented to safeguard public interests or the legitimate rights and interests of the natural person". Therefore, disease prevention and control institutions, medical institutions and their authorized institutions can legally handle personal information processing without obtaining the informed consent of the owner of personal information.

4. CONCLUSIONS AND SUGGESTIONS

In epidemic prevention and control, the collection and processing of personal information, such as whereabouts, plays a decisive role in epidemic investigation. However, due to the imperfect legal system for the protection and utilization of personal information in China, it is not only reflected in the lag in time, but also in the obvious flaws in the legislative level, which is not only difficult to meet the actual needs in ordinary times, but also ineffective in extraordinary times. Fortunately, the Chinese government enjoys high prestige, the people trust the government and are willing to serve the government management, and the epidemic prevention and control can still be carried out in an orderly and efficient manner under the situation of insufficient support of laws and regulations.

On the one hand, it is necessary to revise and improve the laws and regulations on personal information protection and utilization in emergency situations such as epidemic prevention and control of infectious diseases, speed up the legislative process of China's personal information protection law, and build a relatively sound legal system for personal information protection and utilization in China. On the other hand, in very urgent situations, according to the needs of work, the National People's Congress issues an emergency bill, giving the government the power to deal with emergency situations and temporarily restrict some rights of citizens, so as to better cope with emergency situations.

ACKNOWLEDGMENT

This work was supported by the Artificial intelligence Law Discipline Construction Fund of Shanghai University of Political Science and Law

REFERENCES

- [1] Wuhan Health Committee, The Report of Wuhan Health Committee on the Current Pneumonia Epidemic Situation in our city, December 31, 2019. DOI: <http://wjw.wuhan.gov.cn/front/web/showDetail/2019123108989>. (In Chinese)
- [2] General Office of the Standing Committee of the National People's Congress, The Standing Committee's Decision on Strengthening Network Information Protection, Beijing: China Democracy and Legal System Press, 2013. (In Chinese)
- [3] Ministry of Industry and Information Technology of the People's Republic of China, Provisions on the Protection of Personal Information of Telecommunications and Internet Users, July 16, 2013, DOI: www.miit.gov.cn/n1146285/n1146352/n3054355/n305724/n3057729/c4700145/content.html. (In Chinese)
- [4] Standing Committee of the National People's Congress, Criminal Law of the People's Republic of China: the latest amendment according to Criminal Law Amendment (X), Beijing: Law Press, 2017. (In Chinese)
- [5] Wang Liming. Detailed Explanation of General Principles of Civil Law of the People's Republic of China, Beijing: China Legal Publishing House, 2017. (In Chinese)
- [6] Supreme People's Court and Supreme People's Procuratorate, Interpretation of the Supreme People's Court and the Supreme People's Procuratorate on Several Issues Concerning the Application of Laws in Handling Criminal Cases of Infringement of Citizens' Personal Information, May 8, 2017, DOI: https://www.spp.gov.cn/spp/zd gz/201705/t20170510_190149.shtml. (In Chinese)
- [7] Standing Committee of National People's Congress, Network Security Law of the People's Republic of China, Beijing: Law Press, 2016. (In Chinese)
- [8] Office of the Central Network Security and Informatization Committee, Notice on Doing a Good Job in Personal Information Protection and Using Big Data to Support Joint Prevention and Control, February 4, 2020, DOI: http://www.cac.gov.cn/2020-02/09/c_1582791585580220.htm. (In Chinese)