Legal Dilemma and Relief of Citizen's Information Protection under Prevention and Control

ZiXian Duan*

School of Politics and Law, Shangrao Normal University, Jiang Xi, China

*Corresponding author: duanzixian0421@163.com

Abstract. The protection of personal information is more complicated during the epidemic. When there is a conflict between personal rights and public interests, how to balance the relationship between them becomes the current. To start from the concept discrimination of personal information, this paper dialectically analyzes its relationship with personal data and privacy and then analyzes the relevant legal principles in its internal jurisprudence. Based on text analysis, this paper divides the personal information collection stage, processing stage and post-processing stage, examines the related problems in each stage, and then proposes relevant solutions, such as classifying the information scope and clarifying the boundaries of rights and obligations, in order to improve the legal system.

Keywords: Personal information, information boundary, legal relief.

1. Introduction

The outbreak of the COVID-19 epidemic in 2019 had a profound impact on everyone's life. With the increasing efforts to prevent and control the epidemic, various epidemic prevention and control policies issued by various localities inevitably infringe upon citizens' personal privacy.

For example, the epidemiological investigation of COVID-19 patients is often released to the public. The details of the patients are also spread wildly by netizens. Recently, the "Kohler bathroom case" and Shaanxi Baoji spreading rumors led to related issues such as how to protect personal information under the epidemic better.

It is worth noting that although the academic circle has carried out much research, there are still some deficiencies. Combining the literature, we can find that the number of existing related papers is relatively small, and the discussion is relatively simple.

Among them, Pan Wenwen, Liu Zhenyu and other scholars systematically discussed the exploration of the balance between the utilization and protection of personal information under the background of epidemic prevention and control, which is of great enlightening significance. Guo Pengfei, Lin Huixiang and other scholars take COVID-19 epidemic prevention and control as a perspective. This paper analyzes the three principles that should be followed in protecting of personal information in public health events and puts forward specific measures for the protection of personal information in public health events.

Although the existing literature has put forward specific measures for the protection of personal information, there is no clear and persuasive theoretical consensus on some key issues, and some viewpoints may even deviate from the purpose of the regulation. It is worth carrying out continuous discussion.

This paper attempts to start from the following three aspects: unclear boundaries of personal information collected during the epidemic, improper handling, and inadequate relief afterward, through the study of the concept and legal analysis of personal information, and then a comprehensive understanding of the plight of personal information protection under the epidemic, in order to provide some ideas and ideas for solving the problem.

2. Personal Information Protection: Conceptual Research and Jurisprudence Analysis

2.1. Conceptual Research

According to the laws and regulations of our country, personal information refers to the information that can be saved or stored by various media, can be identified by the subject, and reflects the various identity characteristics of natural persons. Meanwhile, anonymous personal information is not included [1].

By clarifying the legal concepts related to personal information, such as personal data, personal privacy, etc., it is possible to identify the connotative characteristics of personal information better.

Personal data refers to the data that contains the information of a specific natural person, excluding the data processed anonymously. The differences between personal privacy and personal data are as follows [2]:

First, the path of identifying objects is different. Whether the data belongs to personal data is not only an objective fact but also depends on whether the data processor has the purpose of identification, especially for identifiable data and associated path data. These data are subjective and objective legal facts, not just objective data. In contrast, the identification of our country only adopts the standard of objectivism, that is, whether the objectively existing information can identify specific natural persons through technical means, it is not like the European Union to determine the personal belief by the subjective standard of whether the data processor has the purpose of identification.

Second, the object of identification is different. Cyber Security Law does not explain what dimensions of personal information identity contains. In China's judicial practice, personal identity "mainly refers to those 'core identities' authenticated by the state, such as name, ID card number, passport number, etc." The objects identified in Hong Kong are mainly limited to the Hong Kong identity card number and other numbers that can be uniquely identified. Therefore, the concept of personal identity in the Internet Security Law contains a smaller range of characteristics, such as psychological, spiritual and cultural, which are not listed in the Internet Security Law.

Third, the subject of identification is different. The adjustment subjects involved in the personal information part of the Network Security Law are mainly network operators and providers of network products or services, so the identification subject is limited to the subjects mentioned above.. The Security Code is a standard for enterprises whose main business involves personal information processing. It has a scale of more than 200 people, so the identification subject is only limited to enterprises with more than 200 people and the main business involves personal information.

2.2. urisprudence Analysis

For public interest during the epidemic, COVID-19 infected people needed to truthfully publish their itinerary and other information within a certain period, which was not sufficiently de-identified at first. People in the area can easily use this information to identify the diagnosed person.

Therefore, the collection of information during the epidemic should follow the following principles: The principle of legality, the principle of legitimacy, the necessary principles, the principle of good faith, the principle of purpose limitation, and the principle of openness and transparency [3-5].

The principle of legality emphasizes that the relevant subjects should strictly abide by the relevant provisions of laws and regulations in collecting, processing, and using citizens' personal information and legally apply citizens' personal information following strictly in accordance with the procedures.

The principle of legitimacy and the principle of purpose restriction requires that the relevant subjects should use the personal information of citizens based on the relevant legitimate needs such as public social welfare or national interests, and there shall be no matters of abusing power for personal gain and infringing upon the legitimate rights and interests of citizens.

The principle of necessity emphasizes that the relevant subjects should implement the concept of minimum in the process of collecting, processing, and using citizens' personal information and should

not excessively collect citizens' personal information; the principle of good faith requires that relevant subjects should form reasonable trust with citizens, abide by promises and be responsible in accordance by the law.

The principle of openness and transparency emphasizes that the relevant subjects should implement the procedures of information disclosure to the citizens who are collecting personal information in the whole process so that citizens can know the specific use of their personal information.

Furthermore, the main significance of paying attention to the legal protection of personal information under epidemic prevention and control is[6]:

On the one hand, to safeguard the legitimate rights and interests of citizens and protect citizens' rights such as personality rights and information rights. On the other hand, it can reduce the occurrence of related infringement cases caused by personal information in time to build a core society and implement the people-oriented social concept.

3. Review of the Dilemma

3.1. Collection stage: the boundary of personal information collected is unknown

In order to better prevent and control the epidemic, the state and relevant departments need to collect the personal information of confirmed diagnoses, suspects, and close contacts, including name, age, mobile phone number, etc., the most important of which is the personal itinerary, which is helpful to find the source of infection, delineate the risk area and take countermeasures at an early date[7].

The information control of confirmed diagnoses, suspects, and intimate receivers is insufficient.

First, although the personal information in the document announcement has been processed to a certain extent, it is far from achieving the effect of de-recognition.

Second, the public posted other information online out of well-intentioned reminders or other purposes. Personal information of those diagnosed and intimate that had nothing to do with the prevention and control of the epidemic was wantonly made public, forwarded, commented on to remind or express dissatisfaction. Although some individuals in the epidemic have a specific social mentality of revenge, knowing full well that they are infected or likely to be infected, they still go out without masks and wander around, but most of them are people who run for a living without knowing it.

At the same time, the public will wantonly speculate on suspects, causing harm to others, such as unfair treatment, discrimination, abuse and condemnation.

In the prevention and control process, the state authorizes large enterprises with advanced scientific and technological advantages to rely on big data's technology to collect information about diagnosed, secret, and suspected persons.

The relevant departments should strengthen control over these subjects of information collection, restrict their sharing with third parties, and prevent them from using trafficking information, using the collected information to evaluate their consumption level and preferences, and watching dishes. Moreover, it ensures that the information can be effectively forgotten after use [8].

3.2. Processing stage: the main body of personal information collection has unclear powers and responsibilities

The legitimate subjects of personal information collected are disease prevention and control institutions at all levels, village committees, and neighborhood committees. Shopping malls and restaurants will also require you to show the health code, and travel code and register your personal information based on epidemic prevention and control [9].

The starting point of this kind of registration is good, but whether it is legal and compliant is worth considering, and whether the relevant subjects can keep and forget the information after the event is also open to question.

First of all, according to Chinese laws, in the event of a major public health emergency, grass-

roots organizations should assist the health administrative departments at or above the county level in epidemic prevention and control, such as information collection, investigation, verification etc [10].

Secondly, for the personal information collected by the subjects, as mentioned above, the principle of protection should be lawful. To the greatest extent possible, the personal information of citizens should be reasonably used, and the use and processing of information should be held responsible in accordance by the law.

Finally, to collect citizens' personal information, the principle of citizens' voluntariness and the principle of information collection boundaries should be implemented, and citizens' privacy should not be excessively collected or interfered with to avoid infringing on citizens' information rights.

In the epidemic prevention and control, the above subjects are faced with the problem of unclear rights and responsibilities in the stage of information collection.

On the one hand, the subjects who do not have the right to collect information wantonly infringe upon citizens' privacy, resulting in the disclosure of citizens' personal Sinahi resulting in adverse social impact. On the other hand, the subjects with the right to collect information excessively collect citizens' personal information, which makes citizens' personal life restless and infringes upon citizens' right to personal information to a certain extent [11].

3.3. Afterwards stage: there are still some deficiencies in the relief of personal information

After the end of the epidemic, users' personal information should be fully protected from being maliciously collected by APP and effectively exercise the "right to be forgotten". For the public information at the beginning of the epidemic, if the infected person's address is exposed, the government department should delete the relevant information afterward to avoid continuous infringement on the information protection of others.

As the epidemic rebounded again in 2022, returning home has also become a major problem. There is a phenomenon of "different hearts and minds" in some areas, and the real conditions for returning home do not have a unified standard, which is even different from the return policy announced on the official account.

There are two reasons [12]: for the time being, the district is afraid of the emergence of infected people and intimate contacts in this area, so it is simply "across the board"; second, managers have an excessive understanding of the relevant documents, and it is not necessary to "go out" to specifically refer to provinces, cities, districts or doors. The safest thing is the most conservative understanding.

It will increase the conditions for returning to their hometown, and may, to a certain extent, guide the masses to treat people differently and fear them and the phenomenon of going back and forth for the sake of normal convenience. Some infected people are discriminated against and treated unfairly in work, life and marriage choices because of inadequate information management after recovery.

4. Discussion on the protected ways

4.1. Clarify and classify the boundaries

According to the law of our country, the relevant administrative subjects should implement the principle of minimum scope when collecting citizens' personal information.

The principle emphasizes that, on the one hand, citizens' personal information has important legal interests and carries citizens' personal dignity and should be fully protected; on the other hand, excessive processing of personal information can easily cause unpredictable danger and damage to these interests, and then cause adverse social impact, damage the appearance of social harmony, and is not conducive to the construction of a country under the rule of law[13].

In practice, it is typical for APP of smart terminals such as mobile phones to illegally obtain personal information, collect personal information beyond the scope, and excessively ask for authority. For APP that deal with personal information in violation of the necessary principles, the State Internet Information Department has ordered them to be removed from the shelves, requiring

APP operators to rectify and reform in accordance by the law.

In collecting information on epidemic prevention and control, we should also abide by the necessary principles and collect information according to different degrees of infected people and close contacts. For example, the ID card number is widely collected in practice, which is unnecessary.

4.2. Standardize the rights and responsibilities of the subject of personal information collection

In order to pursue procedural justice and efficiency, I think we can choose to set up a particular information management system to collect and deal with public information uniformly. Take the ID card information of the public security organs as the basic structure to collect information, and combine the banking system's asset information as a supplement; for public health emergencies such as COVID-19, desensitize and desensitize the personal information of those who are diagnosed and secretly received[14].

In real life, some executees who can perform but refuse to do so are restricted from high consumption, but they continue to enjoy a high-consumption life by means of utilizing transferring assets and riding high-speed rail with passports.)

In the processing of personal information, the processor has the technical advantages that the individual does not possess, and it is difficult for the individual to know what kind of personal information will be processed in what way and it is difficult for the individual to know what kind of processing purpose the personal information is used.

It is known that information asymmetry results in the disadvantaged situation of those who collect the information. Therefore, in the process of information collection, attention should be paid to the open and transparent procedures for information collection. Through this procedure, reasonable trust is formed between the processor and the person to whom the information is collected,demonstrating the law's stability and protecting the personal information of citizens' rights[15].

In addition, processors should also perform a high and reasonable duty of care in case of emergency when dealing with citizens' personal information. It should be made clear that citizens' personal information embodies both personal and property, so it is necessary to grasp the information processing procedure reasonably. The information collected is no longer collected twice. The personal information that has been used should be deleted in a timely and legal manner to protect citizens' personal information from disclosure and avoid infringement of citizens' right to personal information.

Therefore, in the context of epidemic prevention and control, citizens' personal information should be classified and graded on timer. Different collection, processing, and use procedures are adopted for each category and level of information. For example, essential information can be obtained by retrieving citizens' household registration information, and essential information can be inquired about using face-to-face question-and-answer or telephone and recorded. By classifying citizens' personal information, citizens' legitimate rights and interests can be better protected, and various problems caused by procedures such as information collection can be dealt with more conveniently.

4.3. Diversify and perfect the ways of personal information relief

It should be made clear that in terms of the return policy, people with a history of COVID-19 medical history should not be restricted and increased in theoretical documents or practical treatment, and their equal right to return to their hometown should be guaranteed after they have been quarantined in compliance with the regulations[16].

Their real names should not be publicized in the publicity of home isolation. However, it should be referred as "returnees in the city", "returnees in the province", "returnees from outside the province" and so on. It is used to protect their personal information fully.

Meanwhile, the contact information of the person in charge of supervision should be publicized to protect the community people's right to know fully and the personal information rights and interests of those who return home so as not to cause panic among community personnel while supervising

home testing.

In addition, timely relief should be provided to the disclosure of citizens' personal information due to unexpected circumstances, such as deleting relevant articles, apologizing, correcting information statements, and so on, to prevent further expansion of adverse effects and protect citizens' legitimate rights and interests. For personal information violation, relief can be taken by way of litigation, and timely public interest litigation can be brought to protect legitimate rights and interests.

Finally, the state should increase legal publicity on personal information protection so that every citizen can understand the importance of legal interests. In addition, legal protection of personal information can be popularized through legal publicity so that citizens can take up legal weapons in time to protect their legitimate rights and interests in the face of relevant legal incidents.

To sum up, the legal protection of citizens' personal information under epidemic prevention and control is a hot social issue worth studying. Moreover, it is also a rights and interests event closely related to us. The study of this paper is only to select part of the problem to discuss and put forward a relatively reasonable solution. The problem is still further in-depth study, with a view to the final improvement and solution.

References

[1] Wang Liming,A study on the Major and difficult problems of Personality Rights[M]. law Press,Beijing. 2019.

[2] Wang Liming,Research on Civil and Commercial Law[M].Renmin University Press of China, Beijing:,2000.

[3] Fan Yuan,Smart City and Information Security in the Digital economy era, 2nd Edition[M]. electronic Industry Press, Beijing,2020.

[4] Yumang,Regulation[M].intellectual property Press, Beijing. 2019.

[5] Huang Zhixiong,On Network sovereignty[M].social Science Literature Press, Beijing,2017.

[6] Wang Longde,Emergency Management of Public Health emergencies: theory and practice[M].people's Health Publishing House, Beijing,2008.

[7] Gong Yucui,Luo Yanhua,Nursing and Management of COVID-19 patients[M]. science Press, Beijing,2020.

[8] Shoubu,Practical Guide to Network Security Law[M].Shanghai Jiaotong University Press, Shanghai,2017.

[9] Pu Chuan, Health Law,Xu Chen, Health law,Jiangsu[M].Phoenix Science and Technology Press, 2018.

[10] Xi Wangyuan,Cyber Crime and Security[M].Renmin University Press, Beijing,2019.

[11] Yang Lixin,Interpretation of Chinese Civil Law and case commentary Personality right Editing[M].China legal Publishing House, Beijing,2020.

[12] Xia Bing,Network Security Law and Network Security level Protection 2.0[M].electronic Industry Press, Beijing,2017.

[13] Huang Junhui,Liu Baoping,Standard for emergency management in hospitals[M].central South University Press, Changsha,2004.

[14] Raymond Wax,Privacy[M].Yilin Publishing House, Nanjing,2020.

[15] Lang Qingbin, Sun Yi,Research and practice of personal Information Security[M].people's Publishing House, Beijing,2012.

[16] Shen Yanhong,Research on Administrative legal Regulation of Social crisis Prevention and Control[M].Wuhan University Press, Wuhan,2013.