

# Personal Privacy Protection Against the Background of the COVID-19 Pandemic: Status Quo, Dilemma, and Approach

Wuyu Xiao<sup>1</sup> Weijun Wu<sup>2</sup>

<sup>1,2</sup> University of Electronic Science and Technology of China, Chengdu, Sichuan, China

<sup>1</sup> Corresponding author. Email: xiaowuyu1129@gmail.com

## ABSTRACT

Since January 2020, the personal privacy protection has increasingly attracted widespread attention against the background of the COVID-19 pandemic. This study sorts out the current situation of privacy protection system in the response to the COVID-19 pandemic in China, and reveals the existing problems such as the widespread leakage of personal privacy, the network violence caused by the weak protection of personal privacy, and the difficulties in safeguarding and relieving personal privacy after being violated. From this point of view, it is suggested to first improve the relevant provisions on the existing laws and policies, establish the principle of paying equal attention to public welfare maintenance and privacy protection, refine the content of personal privacy, and improve the law enforcement mechanism of personal privacy protection; secondly, it is necessary to improve the ability of administrative organs to deal with crisis, enhance the public officials' awareness of privacy protection, strictly publicize government information in crisis response, and improve the supervision and correction mechanism in crisis response; and finally, it is required to create a good atmosphere for the personal privacy protection, pay attention to the knowledge publicity of personal privacy protection, increase the investigation and punishment of personal privacy infringement, and guide the network platform to strengthen the industry self-discipline management.

**Keywords:** COVID-19 pandemic, Personal privacy, Crisis countermeasures.

## 1. INTRODUCTION

Since January 2020, the novel coronavirus pneumonia epidemic has been quietly spreading in China, bringing indelible disasters to Chinese society and even the world. From the "SARS" pandemic in 2003 to the COVID-19 pandemic in 2019 and other major public health emergencies, Chinese governments had made considerable progress in the emergency management and governance capabilities, and a relatively complete governance system has been formed. With the increasing participation of Internet citizens and the development of big data technology, the government collected a large amount of data through the Internet during the COVID-19 pandemic, and used big data analysis to predict, prevent and control the spread of the COVID-19 pandemic. In this context, how to strengthen the protection of personal information and personal

privacy, balance the relationship between public interests and personal interests, and protect citizens' property, health and even life safety has become increasingly prominent.

## 2. LEGISLATIVE STATUS OF PERSONAL PRIVACY PROTECTION IN RESPONSE TO THE COVID-19 PANDEMIC

In terms of legislation, the legislation on government information publicity of public health emergencies originated from the promulgation of the regulations on emergency response to public health emergencies after the SARS pandemic in 2003, marking that China has entered the stage of comprehensive construction of emergency legal system [1]. On March 28, 2004, the State Council issued the "Emergency Handling Law of the People's Republic of China (Draft)", stipulating the

challenges faced by the Chinese government in dealing with unexpected public crises and proposing to establish and improve the corresponding legal system. After that, China had successively issued the "Emergency Handling Law", the "Infectious Disease Prevention and Control Law" and the "Government Information Disclosure Regulations" to deal with this problem. Before 2021, the relevant provisions on personal information protection under normal conditions were in various laws and regulations, and there was no special law to regulate it. Moreover, the subject, content and scope of protection were different, and it was difficult to unify in actual operation [2]. It was not until the promulgation of the "personal information protection law" in 2021 that the previous relevant laws and regulations on personal information protection were integrated, and the relevant obligations, responsibilities, legal responsibilities of state organs and personal information processors, as well as personal rights and personal information processing rules, were further improved, forming the current personal information protection system in China. Chapter 6 of the "Civil Code of the people's Republic of China" (the fourth edition), which was formally implemented in 2021, improved the right of privacy and personal information protection and further improved the personal information protection system [3].

In terms of policy, there were also above-mentioned legislative problems in the contents of the "Emergency Plan for Public Health Emergencies" of the state and local governments. Since the emergency plan was formally implemented in 2006, it has not been modified to this day. With the economic and social progress, some provisions in the "Contingency Plan" had been inconsistent with the current national conditions. At the same time, after studying the contingency plans of the governments of Beijing, Hubei Province and Chengdu, at present, the contingency plans for local public health emergencies in China generally showed the characteristics of local government plagiarizing the central government, serious homogenization plans at the same level, and neglecting the differences among different places. At the same time, it also highlighted the one-sidedness of the provisions on information release, overemphasizing the unity, timeliness and accuracy of information release. In addition, there was no more in-depth regulation on the content and scope of information release, and there was no description or regulation on how to

protect the personal information or personal privacy of the personnel involved in information release [4].

### **3. THE DILEMMA OF PERSONAL PRIVACY PROTECTION IN RESPONSE TO THE COVID-19 PANDEMIC**

Looking at the measures taken by various places in response to the COVID-19 pandemic since 2020, it is not difficult to find that there are many problems in the protection of personal privacy.

#### ***3.1 Widespread Leakage of Personal Privacy***

China's legislation and policies related to personal privacy are still in the initial stage of improvement. Therefore, from the national level to the social level and then to the personal level, the protection awareness of personal information and personal privacy still needs to be further improved. In terms of the comprehensiveness and timeliness of government information collection and information disclosure, the COVID-19 pandemic also shows the government's ability of social mobilization and information disclosure in response to public health emergencies. However, in the "special" period, the mobilization and appeal for citizens to actively fight against the pandemic, and the extensive collection, and processing and publication of citizens' personal information have also strong pressure from public interests on personal interests to a certain extent. In the face of social stability and public interests, it seems that the citizens' truthful provision of personal information or action track has become the only choice, and citizens' personal information has been widely published. On the contrary, it has become an important factor for the leakage of citizens' personal privacy. In the event of public health emergencies, the disclosure of personal information is mandatory. After citizens become patients or close contacts of the COVID-19 pandemic, their personal information will not only be collected and processed in more detail by relevant government departments, but also be published on various websites, increasing the risk of personal privacy disclosure. In addition, in the Internet age with the unprecedented speed of information dissemination, every time a citizen's personal privacy is leaked, it will be known, disseminated and discussed by countless netizens to varying degrees, and even vicious events of "Cyber Manhunt" and "rumor" have occurred repeatedly. When many local

governments in China release the action trajectories of patients and close contacts, the action trajectories inevitably contain related privacy contents such as different living habits, social status and travel modes of citizens, and there will be hot discussions on these contents on the Internet, and even unnecessary disturbance or damage to the real life of relevant people.

### **3.2 Network Violence Caused by Inadequate Protection of Personal Privacy**

The weak protection of personal privacy is first reflected in the improper collection and management of information. As there are many subjects of personal information collection and is a certain degree of autonomy, it is inevitable that various institutions will have problems of excessive collection, repeated collection, information disclosure and improper information management in varying degrees in the implementation of citizens' personal information collection and processing tasks, resulting in the infringement of citizens' personal privacy rights. However, in the Internet information age, due to the problems such as the large number of staff handling the personal information of citizens, the improper management of information within the department, and the lack of privacy protection awareness of staff, it is difficult to trace the divulger collecting personal information of citizens after it is leaked. Also, it is difficult to protect the personal privacy of citizens and punish infringers.

Inadequate protection of personal privacy is also reflected in improper disclosure of personal information. As there is the public health emergency, the personal information and action trajectory of citizens must be disclosed to the staff of epidemiological investigation based on the needs of epidemic prevention and control. If it is necessary, it is required to disclose the information to the society after desensitization [5]. However, there is no specific standard for information desensitization and information disclosure in the current legislation and government plans, and no unified standard has been formed in the practical operation of governments at all levels. Therefore, the disclosure of personal information and action track of cases and close contacts in different places is inconsistent. However, it is easy to infer the true identity according to the disclosed citizens' personal information and action track such as their residence, name (Surname), occupation, etc., and their

personal privacy such as ID number and contact information is also at risk of being disclosed [6].

### **3.3 Difficulties in Rights Protection and Relief After the Invasion of Personal Privacy Rights**

The lack of relief mechanism afterwards for the protection of personal privacy is reflected in two aspects. First, the relevant government rules and regulations and legislative texts are weak in safeguarding the rights of individuals after their privacy is infringed. Second, the government departments fail to take effective measures to remedy individuals whose privacy is infringed. These include the failure to delete relevant information in a timely manner, the failure to publicly refute rumors in a timely manner, and the failure to crack down on rumors.

As for the long-standing feature of insufficient protection of the personal privacy after being infringed, it is also related to the incomplete accountability system of personal privacy itself and the weak awareness of individual rights protection of citizens in addition to the imperfect pre-guarantee system and the punishment measures afterwards in the relevant contents of government regulations and legislation. First of all, the advance security system has been developed in the previous text. In the Internet age, the disclosure of citizens' personal privacy may bring unbearable pressure and trouble to them physically and mentally, and even seriously interfere with their normal life. However, the current punishment measures are out of balance with the losses of the victims, and the deterrent force to the infringers is insufficient. Secondly, in the era of big data, citizens' personal information is often exposed on the Internet. However, it is difficult and time-consuming to accurately identify infringers on the Internet. And many times, although the personal privacy of citizens is leaked, it has not produced serious consequences. In this case, most citizens will give up protecting their legitimate rights and interests.

According to Item 47 of the "Personal Information Protection Law", when the processing purpose has been realized, cannot be realized, or is no longer necessary to achieve, the processor of personal information shall take the initiative to delete personal information, and the individual has the right to request deletion. As far as the epidemic prevention and control itself is concerned, the release of personal information and action track of confirmed patients is to find close contacts and

send warnings to the society more quickly, so as to control the epidemic as soon as possible and ensure the safety of the people. If all the close contacts of the epidemic have been found, or when all the confirmed patients of the epidemic have been cured, the relevant published information should be deleted in time. However, in the actual prevention of the COVID-19 pandemic, many local governments still publish the information of confirmed patients that have achieved the purpose of processing and publishing on various official websites, and some of the information even involves the personal privacy of confirmed patients. In most cases, when the government is the processor of personal information and when personal privacy is faced with the public interest in an emergency state, it is not realistic to rely solely on the initiative of individual citizens to request deletion to achieve relief afterwards. The relevant government departments still need to further improve the dynamic management of citizens' personal privacy after the event, so as to truly serve the people and administer according to law and reasonably.

#### **4. WAYS TO PROTECT PERSONAL PRIVACY IN RESPONSE TO THE COVID-19 PANDEMIC**

In view of China's national conditions, it is suggested to focus on three aspects to improve the personal privacy protection in the future response to the COVID-19 pandemic.

##### ***4.1 Improving Relevant Provisions of Existing Laws and Policies***

In order to strengthen the protection of personal privacy in response to public health emergencies, it is suggested to improve the existing government rules and regulations. To improve the corresponding rules and regulations and the government's working principles, it is necessary to start with the improvement of legislation, so as to play a role in driving the government and radiating the society.

##### ***4.1.1 Establishing the Principle of Paying Equal Attention to Public Welfare and Privacy Protection***

In public health emergencies, the public interest and the personal interest is the most prominent. In order to find the best solution for the protection of personal privacy under public health emergencies,

it is necessary to clarify the balance between the protection of public interest and the protection of privacy under public health emergencies.

The principle of coordination between the right to know and the right to privacy, that is, coordination between the public interest and the personal privacy, should be as follows: the first is the principle of public interest priority. When there is a conflict between the right of personal privacy and the maintenance of public interests, the personal interests should be subordinated to the public interests. The protection of public interests under public health emergencies is mainly reflected in the protection of the citizens' right to know the latest situation and the right to life and health, which represents the interests of the largest majority of people. When they two conflict with the privacy rights of citizens, the personal privacy rights should be appropriately reduced to ensure the interests of more people to the maximum extent. Second is the principle of balance of interests. Although personal interests should give way to public interests, that is, personal privacy should give way to the public's right to know, the government should also distinguish different situations in the practice of disclosing information. If the government involves the personal privacy of citizens when disclosing the information, it should thoroughly desensitize the privacy before publishing it. At this time, the right to know should give due consideration to the privacy, so as to avoid the adverse consequences that may occur after the personal privacy of citizens is improperly disclosed.

To balance the relationship between the maintenance of public interests and the protection of personal privacy, it is necessary to combine the mandatory and limitation of information reporting and information disclosure. During the COVID-19 pandemic, citizens have the obligation to report their identity information and action track to the relevant departments. When it is necessary, the information will be disclosed to the society. At this time, the information reporting and information disclosure are mandatory, and the mandatory disclosure of patient information by the government is also an inevitable move under public health emergencies. Accordingly, when implementing the rights and obligations of information collection and information disclosure, the government should not only emphasize the enforceability, but also consider how to minimize the risk of citizens' personal privacy being leaked while ensuring the public's right to know.

#### *4.1.2 Refining the Content of Personal Privacy*

At present, the legislative system has consciously improved the relevant legal framework for personal information protection, but the relevant laws and regulations for the protection of personal information and personal privacy under public health emergencies are still in the initial exploration stage. Moreover, Item 1032 of the "Civil Code" has clearly stipulated that natural persons have the right of privacy, which represents that the right of privacy has officially become an independent personality right. Therefore, the relevant legislation should refine the specific content of personal privacy based on the relevant content of personal privacy in the "Civil Code" and the "Personal Information Protection Law", especially the specific definition, protection scope and protection methods of personal privacy in case of public health emergencies.

First, under "abnormal" public health emergencies, the scope of personal privacy protection should be appropriately narrowed, and it is suggested to focus more on the personal privacy protection of patients, close contacts and other direct parties to public health emergencies and develop a set of response mechanisms different from "normal" personal privacy protection. Then, when public health emergencies occur, personal privacy can be more effectively protected. Second, in terms of protection methods, special approval procedures should be set up, the principle of "minimum scope" should be followed, the scope of personal information that can not be published under "abnormal" circumstances should be clarified, and the personal information of citizens to be published should be subject to multiple approval and screening. For example, the government and the media should have special approval procedures for information disclosure involving citizens' personal privacy, and the channels of information collection and transmission should be strictly regulated. Third, if improper protection is found, there should be a timely correction mechanism in the legislation, such as deleting relevant information and blocking relevant web pages immediately. Fourth, when a citizen's right of personal privacy is damaged, there should be a corresponding special investigation and treatment mechanism. The investigation and treatment mechanism here should cover the whole process of the protection of the citizen's personal privacy, that is, there should be a corresponding punishment

mechanism for violations such as privacy disclosure, privacy dissemination, rumor and personal attacks by public officials and ordinary citizens, and a more stringent punishment should be established than that under the "normalization". In addition, when there is a public health emergency, if the personal privacy is infringed, various channels should be provided for relief. However, the relief should be limited considering the background of the public health emergency at the same time. Administrative actions should not be stopped immediately under the "normal" background, thus hindering the effectiveness of the government's response measures. The relief should be flexible according to the actual situation.

#### *4.1.3 Improving the Law Enforcement Mechanism for Individual Privacy Protection*

Among the solution paths of personal privacy protection in public health emergencies, it is inevitable to improve the law enforcement mechanism of personal privacy protection. First of all, public officials should adhere to the principle of administration according to law in the process of law enforcement and exercise discretion prudently. At present, the relevant legal provisions on the protection of personal privacy under public health emergencies are still insufficient. It is necessary for the relevant government departments to carry out the protection of personal privacy according to the relevant policies temporarily issued. Among them, there are bound to be many problems that require the departments to make the most appropriate decisions based on the discretion of the law. This requires the government and public officials not only to be familiar with and abide by the relevant provisions of the legislation in the process of law enforcement, but also have enough flexible decision-making ability. Secondly, public officials of the government, institutions and organizations should strengthen internal coordination and consolidate citizens' personal information collection and management capabilities. Relevant mechanisms should be established based on practical experience to identify departments and staff with the right to collect and process information, avoid excessive and repeated collection of citizens' personal information, and avoid a large number of unrelated internal personnel from contacting citizens' personal privacy, which will increase the risk of private information leakage. At the same time, it is necessary to establish a personal information management mechanism of citizens, properly

manage the citizen's personal information that still needs to be processed or used, strictly control the handling personnel, and achieve "accountability for default". For the invalid personal information of citizens, relevant archives and webpages shall be deleted actively and timely according to relevant laws.

#### **4.2 Improving the Crisis Response Ability of Administrative Organs**

In the response to the COVID-19 pandemic, administrative organs have exposed problems such as insufficient awareness of personal privacy protection, improper disclosure, and untimely and incomplete correction of errors. It is necessary to focus on these three types of problems to improve the crisis response ability of administrative organs.

##### **4.2.1 Enhancing Public Officials' Awareness of Privacy Protection**

Enhancing the public officials' awareness of privacy protection is conducive to protecting citizens' personal privacy and improving the ability and quality of public officials to serve the people. The researchers believe that there are three measures to enhance the awareness of public officials' privacy protection. First is to strengthen the training within the government, institutions and organizations, and emphasize that public officials should protect citizens' personal privacy in the related work involving citizens' privacy. Second, strict management mechanism shall be set for the positions, that is, the positions that work content can frequently contact the personal privacy of citizens and have the right to collect and deal with the personal privacy of citizens shall be targeted with corresponding work policies, confidentiality measures and strict punishment mechanism. Third, the government, institutions and organizations should form a special system for the protection of citizens' personal privacy as soon as possible, which should include the "normal" daily work and the "abnormal" special processing mode. At the same time, corresponding protection levels should be set for different types of privacy data, so as to ensure that public officials can effectively protect citizens' personal privacy according to the contents of the system in their daily work or in public health emergencies.

##### **4.2.2 Carrying Out Strict Government Information Disclosure in Crisis Response**

The government information disclosure in crisis response should focus on two aspects. One is the improvement of the release channel. A national unified information release platform should be established for public health emergencies. The open platform of national government affairs data should be used to integrate and update the latest epidemic data and information of various provinces and cities in real time. The information of the platform should be taken as the standard from the central to local, from the official media to the We-Media, so as to ensure the unity, timeliness and accuracy of information release. At the same time, the national unified information release platform can also help provinces and cities to break through the boundaries of cross-regional health certificates and help establish a national unified personal health code. After having a unified epidemic information release platform, what needs to be unified and improved is the release standard. In other words, before information disclosure, the information content should be thoroughly desensitized according to the unified standard, and then released after multiple approval and evaluation. According to the investigation, the public has different needs for the personal information involved in the epidemic. Therefore, at this stage, it is suggested not only to pursue the speed of information release, but should comprehensively consider whether the content and scope of the published information meet the public's needs for information. In addition, it is required to never publish the non-key information of the personnel involved in the pandemic, such as family address, name, occupation, etc., and take into account the unity and integrity of the structure and format. On the other hand, it is suggested to improve the remedy mechanism of information disclosure afterwards. For false and untrue public information, the government should promptly issue a rumour rejection announcement to avoid the public from panic or breeding more rumours due to untrue information. At the same time, if the rumour caused by the correct information disclosure has a wide range of spread, the government should promptly come forward to officially refute the rumour and punish the rumour mongers in a timely manner.

### ***4.2.3 Improving the Supervision and Correction Mechanism in Crisis Response***

At present, the supervision, correction and relief mechanism of personal privacy protection under public health emergencies need to be further improved. The government, institutions and organizations should build a special team of emergency supervision to conduct internal supervision on the emergency decisions of the government, institutions and organizations under public health emergencies, and correct the possible non-standard behaviors or adverse consequences in a timely manner. At the same time, the establishment of the supervision group also helps the relief after the infringement of citizens' personal privacy. After the outbreak of the COVID-19 pandemic, the personal privacy of a small number of people involved in the epidemic has been publicized, and their personal privacy has been seriously infringed. In the follow-up relief and treatment of these events, the current legal relief methods only include administrative reconsideration and administrative litigation. At the same time, the "Personal Information Protection Law" also stipulates that personal information processors should promptly delete the public information that has become invalid or has achieved its purpose in a timely manner. And individuals also have the right to request deletion. However, from the perspective of the awareness of personal privacy protection, it is not enough to rely on citizens' initiative to request the government to delete information, or apply for administrative reconsideration and file administrative litigation. Administrative organs should form self-supervision, pay attention to citizens' relief work afterwards, and actively and properly manage citizens' private information.

## ***4.3 Creating a Good Atmosphere for Personal Privacy Protection***

### ***4.3.1 Paying Attention to the Knowledge Publicity of Personal Privacy Protection***

In order to achieve the protection of personal privacy, the promotion of laws and relevant departments and the promotion of social common awareness are necessary. In the prevention and control of the COVID-19 pandemic, there are problems of improper management of information

collectors in the leakage and dissemination of personal privacy. There are also communicators who do not understand the importance of personal privacy protection and do not know that their communication behavior has infringed upon the privacy of others, and even spread rumors, personal attacks, and telephone harassment to others, causing greater damage to the privacy of others. Against the background of the normalization of public health emergencies, the government should pay more attention to the knowledge publicity of personal privacy protection. Not only should the government, organizations and institutions strengthen the publicity to improve the overall personal privacy protection awareness of public officials and front-line workers, but also should call on the society to abide by the law and discipline, and widely publicize the personal privacy protection knowledge through community, street and grass-roots front-line staff. Finally, the whole society respects the privacy of others and people are good at using legal weapons to protect their privacy rights.

### ***4.3.2 Strengthening the Infringement Investigation and Punishment of Personal Privacy***

At present, there are no special regulations on investigating and punishing the infringement of personal privacy rights in public health emergencies, and the relevant regulations on the infringement of privacy rights mostly focus on the category of civil infringement, and the methods are mainly to stop the infringement, restore the reputation, make an apology, compensate for the loss, etc., and the punishment means are relatively soft. In addition, there are still gaps in the relevant provisions of the government, grass-roots autonomous organizations or medical institutions violating the infringement of personal privacy. According to item 68 and item 69 of the "Law on the Prevention and Control of Infectious Diseases (revised in 2020)", when disease prevention and control institutions and medical institutions deliberately disclose the relevant information and materials of infectious disease patients, pathogen carriers, suspected infectious disease patients and close contacts that involve personal privacy, the health administrative department of the people's government at or above the county level shall impose punishment, revoke the practicing certificate, and investigate the criminal responsibility. However, such laws are somewhat weak in practice, and there are problems of

insufficient investigation and deterrence. Therefore, the investigation and punishment of personal privacy infringement, especially the punishment measures for personal privacy infringement under public health emergencies, should be improved as soon as possible, and the punishment provisions in "special period" and "peace period" should be distinguished, and the punishment for personal privacy infringement in "special period" should be increased as appropriate.

#### 4.3.3 *Guiding the Network Platform to Strengthen the Industrial Self-discipline Management*

With the development of the Internet, the network platform has gradually replaced newspapers, radio, television and other traditional media and become the main carrier of information dissemination and communication among Internet users. The development of large and small cases of personal privacy infringement during the COVID-19 pandemic is inseparable from the spread of users on major Internet platforms. Therefore, it is imperative to guide the network platform to strengthen the self-discipline management of the industry. Under the guidance of the government, the industry should spontaneously establish internal norms to deal with public health emergencies, and strengthen self-regulation and self-supervision. All network platforms should fully implement the real name of users as soon as possible and at the same time, strengthen the screening of contents related to public health emergencies, avoid the dissemination of false news or improper remarks, and prevent the breeding of illegal acts. In addition, all network platforms should also respond to the government's call and rely on the platform's advantages to vigorously publicize the protection of personal privacy and improve the privacy protection awareness of network platform practitioners and platform users.

## 5. CONCLUSION

Considering the normalization of the COVID-19 pandemic, the protection of citizens' personal privacy should attract more active attention from the public. China should improve the legislative vacancy of personal privacy protection under public health emergencies as soon as possible. The government should also formulate more perfect emergency plans and management mechanisms that are in line with the current background, improve its own crisis management ability, and at the same

time drive the society to create a good atmosphere for personal privacy protection. Only in this way, the system of personal privacy protection under public health emergencies will be more perfect, and the basic rights and interests of citizens will be more effectively protected.

## AUTHORS' CONTRIBUTIONS

Wuyu Xiao is responsible for the overall research and writing of the article, Weijun Wu is responsible for the overall framework of the paper and its revision.

## ACKNOWLEDGMENTS

This study is supported by the phased achievements of 2021 Sichuan Soft Science Project (2021JDR0339) and Project OF 2020 Regional Public Management Informatization Research Center (QGXH20-02) — "Research on Optimization of Government Information Disclosure Mechanism on Public Health Emergencies".

## REFERENCES

- [1] Hu Qiang, Li Xue. Research on legal issues of government information disclosure on Chinese emergencies [J]. Estate and Science Tribune, 2013, 12(21): 68-69. (in Chinese)
- [2] Zhang Yong. Legal Protection of Personal Information Related to the Epidemic in the Context of Big Data [J]. Henan Social Sciences, 2020, 28(04): 56-65. (in Chinese)
- [3] Xie Zengyi. The regulation focus on personal information processing in the workplace: Based on different stages of labor relations [J]. Legal Science Monthly, 2021(10):167-180. (in Chinese)
- [4] Li Xuefeng. Research on countermeasures to improve the national emergency management system for public health emergencies [J]. World Health Digest, 2020(04):13-21. DOI:10.14150/j.cnki.1674-7453.2020.04.002. (in Chinese)
- [5] Wang Dongfang. Limitation and Optimization of Disclosure of Personal Privacy Information in the Prevention and Control of Major Epidemics [J]. Journal of Intelligence, 2020, 39(08): 117-121. (in Chinese)



- [6] Zhang Xinbao, Wei Yanwei. Study of the Privacy and Personal Information Protection in the Judicial Information Disclosure [J]. Journal of Comparative Law, 2022(02):104-120. (in Chinese)