Conflicts Between COVID-19 Pandemic Prevention and Control and Protection of Right to Privacy and Their Solutions

Muke Tao[1,*] Yaqi Zheng[1] Yunlu Du[1] Yongqian Tian[1] Yuqing Zhang[1]

[1] *College of Humanities, Hubei University of Chinese Medicine, Wuhan, Hubei, China*
[*] *Corresponding author. Email: 286996515@qq.com*

ABSTRACT
This article discusses the characteristics of privacy in the prevention and control of the COVID-19 pandemic, sorts out typical cases, and introduces corresponding measures under the prevention and control of pandemics outside the territory. In response to the conflict between the public's right to know and the protection of privacy, the conflict between the protection of privacy and the use of digital technology, it is proposed to clarify the boundaries of the right to know and the protection of privacy, clear the boundaries of the collection and disclosure of private information, strengthen the supervision and law enforcement of the disclosure of private information, and enhance and improve the rights relief system and other countermeasures.

Keywords: *Prevention and control of the COVID-19 pandemic, Right to privacy, Right to know, Digital technology.*

1. INTRODUCTION

At the beginning of 2020, the COVID-19 pandemic has begun to raging around the world. The unpredictability and variability of the pandemic has brought huge challenges to prevention and control. Scientific, orderly, and timely release of pandemic information has played an extremely important role in China's rapid control of the spread of the pandemic. However, as information about the pandemic, especially information about patients and persons involved in the pandemic, is increasingly disclosed in detail, the issue of privacy protection of natural persons has also begun to arouse concern. There have been illegal acts of disclosing the private information of natural persons such as patients and people involved in the pandemic without any treatment within the country, which has caused great distress and harm to the parties concerned, and also caused social panic. Against the special background of pandemic prevention and control, how to maintain the balance between public and private interests, and how to deal with the challenges brought by modern technology to privacy protection are worthy of people's deep consideration.

2. CHARACTERISTICS OF RIGHT TO PRIVACY UNDER THE PREVENTION AND CONTROL OF THE COVID-19 PANDEMIC

2.1 The Particularity of the Subject of the Right to Privacy

The subject of the right to privacy is a natural person. Natural persons can be divided into general subjects and special subjects. The healthy group does not pose a threat to the lives and health of others, and therefore enjoys all the content protected by the general right of privacy as the general subjects. The sick or suspected groups carry or are suspected of carrying infectious viruses, which pose a certain threat to the lives and health of other healthy groups. Therefore, the enjoyment of privacy content should be analyzed in detail from the two dimensions of the condition of the sick individual and the current social state. The right to privacy of such groups may be subject to certain restrictions and belong to special subjects.

2.2 The Particularity of the Content of Right to Privacy

2.2.1 Right to Privacy and Confidentiality

In the prevention and control of the COVID-19 pandemic, some private information of special subjects is generated before the outbreak and is closely related to the public interest after the outbreak. Therefore, the private information may be restricted and protected. Therefore, the right to privacy and confidentiality enjoyed by a special subject is to have the right that the agencies, which have obtained the information, need to keep the private information that has notified. These agencies should follow strict confidentiality obligations and specialize the information collected, such as names, phone numbers, ID card numbers, detailed home addresses, family information, and other private information that has nothing to do with the purpose of pandemic prevention and control. In principle, they should not open to the outside world. No private information shall be disclosed to the public or individuals in any way without expressly stipulated by laws and regulations or without the explicit consent of the rights subject.

2.2.2 Right to Privacy Control

The right to privacy control refers to the right of natural persons to use, utilize and dispose of their privacy according to their own wishes. For example, when a natural person goes out and needs community registration, choosing to disclose some personal information to cooperate with the progress of the pandemic prevention work is a manifestation of the right holder's exercise of privacy control. Of course, natural persons who exercise their privacy control rights under the pandemic should abide by the law and must not abuse their rights. Practices such as concealing, false reporting, and providing false body temperature information are all undesirable.

2.2.3 Right to Maintain Privacy

The right to privacy protection refers to the inviolability that the right holder enjoys to his own privacy, and he/she can seek public relief and private relief when he/she is illegally violated. Under the prevention and control of the COVID-19 pandemic, in order to curb the further spread of the pandemic, it is necessary to collect personal information of natural persons. Right holders have the right to require relevant agencies to "desensitize" their private information to protect their privacy rights. If a large number of private information has been disclosed and disseminated and the subject of rights suffers cyber violence, the right owner can take judicial remedies.

2.3 Expansion of the Object of the Right to Privacy

During the COVID-19 pandemic, modern technologies and methods such as big data and artificial intelligence have effectively strengthened the prevention and control of the pandemic. In this context, the scope of personal information data collected is also increasing, and data privacy and traditional privacy have cross-integrated, which gradually increases the scope of privacy objects. For example, in addition to the information contained in physical space, private space also includes information about private life, work unit, and personal experience in cyberspace.

3. PRIVACY PROTECTION PRACTICES UNDER THE PREVENTION AND CONTROL OF THE COVID-19 PANDEMIC OUTSIDE THE TERRITORY

3.1 Extraterritorial Practice

3.1.1 South Korea

In South Korea, data collection and control are mainly based on mobile apps. The government has also temporarily developed a self-isolation security protection app, which not only allows self-isolated confirmed patients to keep in touch with medical staff, but also uses positioning technology to track the location of the confirmed patients. The government has tracked and collected all mobile phone location information and created a public virus map to "digitize" individuals. Each confirmed person has a code name. Only their gender and age range are displayed on the map, allowing anyone to check whether they have an intersection with any new coronavirus patient, helping the public check for avoiding infection. Some typical push messages may be something like this: "A woman in her 60s has just tested positive. Please click on the link to see where she has been before being hospitalized..."

3.1.2 Singapore

Singapore mainly relies on the data tracking method of the "Trace Together" mobile app. The government launched a mobile app called "Trace Together" in the early stage of the fight against the pandemic. When users approach or interact with each other, the APP will send Bluetooth signals to each other to record the distance and duration of the encounter. The APP stores these data for 21 days. If the user is infected, the government can visit the data back.

3.1.3 European Union

The EU mainly focuses on anonymized data and aggregated data analysis of geographic location information. Mobile operators in the use area will share customer location data with the European Commission to monitor the spread of the coronavirus. However, operating organizations (such as communications operators or Internet companies) can only use the user's location data if they are anonymous or with personal consent. During the pandemic, the European Data Protection Board (EDPB) issued a statement that restricts the rights of data subjects in a state of emergency[1], reminding member states that they can exercise emergency legislative power to help prevent and control the pandemic. The EDPB pointed out that in order to maintain public health goals that are in the public interest, Article 23 of the GDPR allows the state to restrict the rights of data subjects when necessary, but it should also protect the rights of personal data, because this is "basic respect for the values of democracy, the rule of law and human rights that form the basis of the European Union".

The European Commission's guidance on data protection during the pandemic is also worthy of reference. On April 16, 2020, the European Commission issued the "Guidance on Apps Supporting the Fight Against COVID 19 Pandemic in Relation to Data Protection". The guidance aims to provide the necessary framework to ensure that citizens' personal data are adequately protected when using the program and to restrict violations. This will increase citizens' trust in innovative applications to ensure the maximum participation of citizens, so as to give full play to the potential of the application. The guidance is mainly for apps that are voluntarily downloaded and related to the fight against the pandemic. These applications may include the following functions: 1) providing information about COVID-19; 2) providing symptom check functions such as self-assessment and questionnaire; 3) contacting tracking function that reminds people who have been near the infected person to be tested or self-isolated; 4) providing communication functions between isolated patients and doctors, including remote medical functions such as diagnosis and treatment suggestions. At present, eight EU countries including France, Germany, and Italy have jointly developed an application that ensures privacy protection and has a "contact tracing" function — Pan-European Privacy-Preserving Proximity Tracing.

3.1.4 The United States of America

The U.S. Congress has introduced two major privacy legislation proposals (the Republican Party's "COVID-19 Consumer Data Protection Act" and the Democratic Party's "Public Health Emergencies Privacy Act"), with the intention to use the pandemic to promote the introduction of a federal privacy bill.[2] Both bills require relevant agencies to obtain users' explicit consent before collecting, using, and disclosing relevant information, provide users with options to withdraw their consent, and delete relevant data in a timely manner after the end of a public health emergency. In terms of supervision methods, both bills require relevant agencies to regularly submit transparency reports to the public on the amount, scope, type, and purpose of the collected data.[2]

In terms of specific measures to deal with the COVID-19, first, the United States used a team led by MIT computer scientist Ramesh Raskar to release an application prototype called Private Kit: Safe Paths. The application can store the user's GPS location data for 28 days. If the user's virus test result is positive, they can choose to share their historical location data with the health department for others to identify potential infections. Second, the U.S. government actively seeks to cooperate with technology companies such as Microsoft, Google, and Facebook on the prevention and control of the coronavirus. These companies have always been very cautious about user data, and generally adopt anonymization or aggregated data to provide trend analysis.

3.1.5 Germany

Germany's "allowing the authorities to track the location of people's mobile phones" mentioned in the amendments to the pandemic had to be deleted

due to public protests. Germany can only adopt the method of cooperation between telecom operators and the Robert Koch Institute, an official disease control and prevention agency. Telecom companies share anonymous big data to let the authorities know the traces of people across the country and even in the community. A poll showed that in order to curb the pandemic, 70% of respondents are willing to provide information on personal health, movement data, and social relations to public pandemic prevention agencies. However, the real concern of the people is not whether it involves proper personal privacy, but whether there is a monitoring mechanism in the process of using information to avoid abuse and whether there will be a punishment mechanism for abuse in the future.

4. CONFLICTS BETWEEN THE PREVENTION AND CONTROL OF THE COVID-19 PANDEMIC AND THE PROTECTION OF RIGHT TO PRIVACY

4.1 Conflicts Between the Right to Privacy and the Public's Right to Know

From the perspective of the object of rights protection, the right to know is the right to understand all potential or existing threats enjoyed by an individual's personal and property from being illegally infringed; the right to privacy is the right that is given to individuals not to be intrusive by others due to the needs of personal dignity and freedom of personality. Both are the protection of individual rights, but conflicts between the two occur from time to time.

The public's right to know is a positive right to resist, while the right to personal privacy is a negative defensive right.[3] In the face of a sudden pandemic, the public is eager to understand and know relevant information of the people involved in the pandemic out of consideration of their own rights to life, health, and body, and requires administrative agencies to publish this information without reservation, but this information is likely to involve personal privacy. On the one hand, the principle of priority of public interests requires individuals to put collective interests first, and when necessary, they must sacrifice personal interests to defend collective interests. Therefore, under the prevention and control of the pandemic, personal interests need to yield to public interests, and personal privacy rights will be derogated or tightened to protect the public's right to know, so as to better protect citizens' right to life and health. On the other hand, the excessive concession of personal right to privacy to the public's right to know will not only lead to the disclosure of the private information of persons involved in the pandemic, which is not conducive to the protection of privacy rights; but it will also trigger social panic, which is harmful to the prevention and control of the COVID-19 pandemic.

4.2 Conflicts Between the Right to Privacy and the Application of Digital Technology

In pandemic prevention and control, the application of digital technology in pandemic prevention and control can be summarized into four categories: The first category is digital documents. This technology is usually used in isolation, replacing traditional telephone interviews and on-site inspections with digital remote inspections. This not only saves manpower, but can also generate documents for people's current location, where they have been, and their physical conditions. The second category is to use mathematical models to try to characterize the transmission characteristics of diseases by collecting population flow information, and use this as a basis for pandemic prevention. The third category is contact tracing, which uses digital technology to identify those who have "close contacts with people infected with the virus" and help close contacts get timely care and treatment to prevent further spread of the virus. The last category is telemedicine, which provides users with remote diagnosis, treatment and other non-emergency medical services.

In the application of digital technology, the issue of privacy protection mainly focuses on the link of "contact tracing". Location data is highly sensitive and can be used to identify the identity of a specific natural person and reflect the trajectory of a specific natural person. Once leaked, illegally provided, or misused, it is extremely harmful to personal and property safety, and can easily lead to personal reputation, physical and mental health damage or discriminatory treatment, which directly involves the vital privacy interests and personal safety of the data subject.

In fact, even if anonymous data is used, there is still the risk of identifying individuals. whether it is a confirmed patient or a suspected infection, it may cause "stigma". For example, companies patronized by suspected or confirmed infected persons may also be leaked and cause loss of income, even after

these places have been closed and disinfected. On the other hand, the contact tracing system, like any information system, also has the possibility of network security risks, data leakage and ransomware attacks. The blackmailer can use the contact tracing system to ask the company to pay a ransom by falsely claiming that he has been diagnosed and has visited the company. Finally, if there is no clear and actionable advice to the contact, it may also produce wrong information, cause counterproductive behavior, and even panic.

5. THE PATH TO RESOLVE THE CONFLICT BETWEEN THE PREVENTION AND CONTROL OF THE COVID-19 PANDEMIC AND THE PROTECTION OF RIGHT TO PRIVACY

5.1 Clarifying the Boundary Between the Right to Know and the Protection of Right to Privacy

5.1.1 Principle of Proportionality

The principle of proportionality requires that the public interest promoted by the means of public power behavior is proportional to the damage it causes.[4] Specifically, the public authority should first measure the interests of the time when the administrative act is implemented, and confirm that the extent to which the administrative act damages the rights of citizens will not exceed the public interest that it promotes. For example, while implementing relevant quarantine measures, the life of the quarantined persons should also be guaranteed, and the balance between public interests and citizens' private interests should be actively maintained.

5.1.2 Principle of Necessity

The principle of necessity, also known as "minimal invasiveness", refers to the collection, processing, and dissemination of private information by relevant departments and personnel in the prevention and control of the pandemic to take measures that minimize the damage to the person being collected. Pandemic prevention measures should be based on the logical tension between the legitimacy of the public interest purpose of "anti-pandemic" and the least infringement of citizens' rights to privacy. The tension contains the two-level balance of "reasonable protection-necessary restriction" of personal privacy, and the dual balance of "individual rights to privacy-collective public interest". Under the same effective choice of measures to stop the spread of the novel coronavirus and control the spread of the COVID-19 pandemic, the administrative agency should choose the measures that will minimize the damage to the rights of citizens in order to achieve a win-win situation in the prevention and control of the COVID-19 pandemic and the protection of citizens' personal interests.

5.1.3 Principle of Security

Public authorities collect and use personal privacy information based on the needs of pandemic prevention and control, and should ensure the security of this information in all links such as storage, use, and transmission. For example, in the prevention and control of the pandemic, due to the leakage of traffic information, some infected people and their private lives have frequently become targets of attacks. The main reason is that there are loopholes in the flow adjustment operation process. The tools used in paper forms, WeChat, phone calls, and Alipay lack professional processing mechanisms for the processing and confidentiality of personal private data, and they may be leaked, lost, or abused at any time. In the previous typical cases, there have been several incidents of public officials leaking and spreading the privacy of individuals involved in the pandemic. This shows that some administrative agencies have loopholes in the management of pandemic-related information and insufficient education on the legal protection of staff privacy.

5.2 Clarifying the Boundary Between Collection and Disclosure of Private Information

5.2.1 Clearing the Collected Subjects

The Law on the Prevention and Control of Infectious Diseases, the Law on Response to Emergencies, and the Regulations on Public Health Emergencies and Emergency Responses stipulate that the subjects who have the right to collect and disclose citizen information in the prevention and control of epidemics include disease prevention and control institutions, medical institutions, designated professional technical institutions, as well as streets, towns, neighborhood committees, and village committees. Other subjects are not allowed

to collect and disclose citizens' personal information without authorization. It should be noted that properties, communities, etc. are not subjects of law enforcement. If authorized by relevant government agencies, they should be regarded as entrusted. Therefore, these organizations cannot force citizens to provide personal private information, but should take the citizens' explicit consent as a prerequisite.

5.2.2 Clarifying the Collected Content

Although individual rights to privacy need to be transferred to the public's right to know when the pandemic breaks out, there is a bottom line of this transfer. The content of information collection should be limited to "related to the COVID-19 pandemic" and must be closely related to the purpose of pandemic prevention and control. Information about the trajectory of COVID-19 patients, asymptomatic infected persons, etc., such as the number of trains taken, places visited, and routes of action are items that can be collected. Conversely, information that has nothing to do with the pandemic, such as name, phone number, ID number, detailed home address, work unit, etc., is content that cannot be collected.

5.2.3 Strictly Observing Private Information, Non-desensitization and Non-disclosure

"Non-desensitization and non-disclosure" is the bottom line that must be adhered to, and it is also the best balance between pandemic prevention and control and privacy protection. The realization of citizens' right to know is achieved by administrative agencies by desensitizing their published information.[5] Taking the disclosure of patient information as an example, the place of residence and the trajectory of actions within a certain period of time are related to the prevention and control of those who have "intersected" with them. The disclosure of their real names, ID numbers and other information does not affect the prevention and control effect. They are unnecessary, and the disclosure will be excessive. Of course, from the perspective of improving credibility and attracting public attention, relevant departments can still choose to disclose relevant information, but it must be desensitized, that is, processing sensitive information that can identify specific individuals, so that specific individuals cannot be identified through this information and cannot be restored. It is also necessary to establish a mechanism for the circulation of personal information to retain traces, and to implement individual responsibility in the collection and aggregation of confirmed personal information. The deletion and destruction of personal information that is no longer needed after the pandemic is over should be promoted in a unified manner. If data should be retained for follow-up medical observation and research, the relevant data should also be desensitized, and the data subject should be notified and given their explicit consent.

5.3 Strengthening the Supervision and Enforcement of Personal Information Disclosure

Relevant departments should attach great importance to the protection of personal privacy information, and adopt strict management and technical protection measures in accordance with the principle of "who collects it and who uses it". No institution or individual shall disclose, tamper with, or destroy the personal privacy information it collects. The protection of the source of information should be strengthened, especially the government agencies, hospitals, and scientific research institutions that have personal privacy information. These units should actively take measures to prevent information leakage; information screening and remediation mechanisms should be established to reduce the negative impact caused by information leakage.

The current privacy protection legislation and basic system design should focus on strengthening the law enforcement link, especially the local organizations should combine their own actual conditions and regulate law enforcement in the spirit of the rule of law. In addition, the investigation and punishment of violations should be strengthened, and severe punishment measures should be taken for those who take advantage of the opportunity to spread maliciously or disclose personal private information.

5.4 Improving the Rights Relief System

In the prevention and control of pandemics involving a large number of modern technologies, personal rights to privacy are easily violated, and the road to relief is full of thorns. According to the proof rule of "who asserts, who gives evidence", the plaintiff (victim) needs to prove the four elements of tort liability, namely, infringement, damage result, subjective fault, and causality. However, due

to the concealment of the Internet transmission system, it is difficult for victims to provide evidence. Therefore, in order to better protect personal rights to privacy, it is necessary to adapt to the development of the times, modify and improve the distribution rules, compensation system, compensation system, and social assistance system of the burden of proof, so as to provide powerful system guarantees for the rights subjects to relieve their rights. In addition, if the aggrieved party involves a large number of information subjects, qualified subjects such as consumer rights protection organizations and non-profit public welfare organizations can initiate public interest litigation[6] to help the victims protect their legal rights and interests.

6. CONCLUSION

The COVID-19 pandemic is a public health emergency, and all information is disclosed for "public safety" and "pandemic prevention and control". The prevention and control of the pandemic must not only adhere to openness and transparency, but also prevent the pandemic in accordance with the law, protect personal privacy, and implement precise policies.

AUTHORS' CONTRIBUTIONS

Yuqing Zhang contributed the central ideas and was responsible for the final revision of the paper. Muke Tao designed the thesis outline, coordinated the writing arrangement of the paper, and revised the first draft. Yaqi Zheng revised the thesis outline, collected and analyzed data. Yunlu Du and Yongqian Tian collected and analyzed typical cases. All authors analysed the literature and were involved in writing the manuscript.

REFERENCES

[1] European Data Protection Board. Thirtieth plenary session: EDPB response to NGOs on hungarian decrees and statement on article 23 GDPR [EB/OL 」.(2020-06-03) [2017-07-01].hops:// edpb. europa. eu / new s / new s/ 2020 thirtieth}lenary}ession}dpb}esponse}gos}ungarian-decrees}nd}tatement}rticle en.

[2] Yang Chunbaixue, Chen Tian, pandemic Response and Data Protection in Europe and America [J]. Information and Communications Technology and Policy, 2020(08): 63-67. (in Chinese)

[3] Zuo Lili, Conflictions and Solutions between the Public's Right to Know and the Personal Privacy [D]. Northeastern University, 2015. (in Chinese)

[4] Liu Quan, Reconstruction on the Principles of Legitimate Purpose and Proportionality [J]. China Legal Science, 2014(04): 33-150. (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] Peng Zhiyuan, Challenges and Corresponding Strategies for the Privacy Protection in the Big Data Era [J]. Journal of Leshan Normal University, 2015, 30(01): 103-107+127. (in Chinese)