Journal of Communication and Computer 19 (2021) 9-15
doi:10.17265/1548-7709/2022.01.002

Interpretation of Information Security and Data Privacy Protection According to the Data Use During the Epidemic*

Liu Yang, Zhang Jiahui, and Sun Kaiyang
School of Marine Law and Humanities, Dalian Ocean University, Dalian, China

Abstract: COVID-19 has swept the whole our country and the world in the beginning of 2020. 31 provinces and municipalities across the country have launched the first-level response to major public health emergencies since January 24, and China has carried out intensive epidemic control. It is critical for effectively responding to COVID-19 to collect, collate and analyze people's personal data. What's more, obtaining identity information, travel records and health information of confirmed cases, suspected cases and close contacts has become a crucial step in epidemic investigation. All regions have made full use of big data to carry out personnel screening, travel records analysis and other related work in epidemic prevention and control, effectively improving the efficiency of epidemic prevention and control. However, data leakage, personnel privacy data exposure, and personal attack frequently occurred in the process of personnel travel records analysis and epidemic prevention and control. It even happened in the WeChat group to forward a person's name, phone number, address, ID number and other sensitive information. It brought discrimination, telephone and SMS harassment to the parties, which caused great harm to individuals. Based on these, lack of information security and data security awareness and other issues were exposed. Therefore, while big data has been widely concerned and applied, attention should be paid to protecting personal privacy. It is urgent to pay more attention to data privacy and information security in order to effectively protect the legitimate rights of the people. Therefore, measures can be taken to achieve this goal, such as improving the relevant legal system, strengthening technical means to enhance the supervision and management of information security and data protection.

Keywords: Information security, data privacy, epidemic prevention and control, personal privacy protection.

1. Introduction

Big data has been playing a crucial role in the epidemic prevention and control in China. During the period of COVID-19, The National Technical Research and Development Department, together with the Ministry of Transport, the Ministry of Health, the Ministry of Public Security and the Ministry of Communications, has developed health codes, which greatly improves the efficiency of travel recording analysis, monitoring people from high-risk and medium-risk areas and close contacts. Relevant experts and scholars have relied on big data to actively establish models, predict epidemic trends, assess risks and carry out scientific research. Nowadays, the prevention and control work of COVID-19 has entered the stage of normalization. The application of big data technology in precision prevention and control of epidemic situation has become more and more mature, which will maximize the normal production and life of people. However, with the application of big data, the leakage of personal information and the network violence of confirmed

* This paper is support by: In 2019, Liaoning Provincial Department of Education Project named "Study on the Path Selection of Rural Revitalization in Ethnic Autonomous Areas of Liaoning Province"; The 3rd Azure Talent Project of Dalian Ocean University in 2018; In 2019, Liaoning Province's overseas training project "China-Canada Cooperation Research Plan on Marine Law and Policy" (2019GJWYB019); The Ministry of Education filed the 2017 National and Regional Research Center Project "Northeast Asia Research Center for Marine Law and Policy" (GQ17091).

Corresponding author: Zhang Jiahui, Master of Law, Dalian Ocean University, Dalian, China. E-mail: 871211883@qq.com

patients occurred from time to time. Athough the big data technology provides assistance for epidemic prevention and control, the potential risk of personal privacy data leakage still exists. Once citizens' personal privacy data was collected and used by criminals, it will cause damage to the interests of the parties. Therefore, with the wide attention and application of big data, personal information security and data privacy protection based on this background must be highly valued.

2. Literature Review

Nowadays, domestic and foreign scholars' research on information security and data privacy protection during the COVID-19 pandemic mainly focuses on the following aspects: (i) Balancing data privacy with public health benefit. Chinese scholar Wang Jun think that relevant information should be fully disclosed to meet the needs of the public and safeguard social public interests. The legitimate rights and interests of the personal data of those involved in the epidemic should also be protected to prevent privacy leakage [1]. Yan Yan, Xia Jinlian and others believe that on the premise of safeguarding the public interest, the rights of personal information should give way to social interest and accept a certain degree of restriction, but this restriction will inevitably lead to the impairment of personal privacy interests [2]. In the era of big data, information disclosure and privacy protection should maximize the balance between personal privacy and public interest in epidemic prevention and control [3]. Jeremy Wacksman believes that big data needs to be used properly to track contacts and laws on health data management need to be improved [4]; (ii) Formulating personal information disclosure standards during the epidemic of infectious diseases. Zheng Baozhang, Feng Shi and others believe that unified information disclosure standard should be established to make the use of personal information more standardized, which not only can protect the public right to know, but also minimize the risk of privacy disclosure of relevant personnel [5]. Zhang Han, Kang Fei, Wang Guiping and others suggest that national unified information release platform should be established to timely announce the latest epidemic situation under the principle of taking into account the protection of personal privacy [6]. Gao Yuling, Xu Yongjun and other scholars believe that in the collection and use of medical big data, differential privacy protection model should be established according to the data type and the scope of individual privacy involved, so that minimizing the risk of privacy disclosure of health and medical data based on maximizing data effectiveness [7]; (iii) Strengthening technology research and development, enhancing the protection of data security and privacy. Bai Juan proposes that technical means such as data desensitization, data encryption and data restricted release should be used to carry out the processing of important sensitive data, so that realizing the protection of privacy and security [8]. Zhan Nan suggests that users' personal information should be identified, encrypted and desensitized, so that minimizing its impact on citizens and individuals and realizing the protection of personal privacy data [9]. Emanuele Ventrella supports that controllers must provide users with clear and understandable information about the processing, as well as with the option to exercise their data subject rights via the application itself [10]; (iv) Health data privacy. Maria Tzanou believes that the GDPR (General Data Protection Regulation) is a complex and evolving body of law that aims to deal with several technological and social health data privacy problems, while safeguarding public health interests and addressing its internal gaps and uncertainties; (v) Learning from humanitarian expertise in data protection. The challenge of responsible data use during a crisis is not novel, the humanitarian sector has more than a decade of experience to offer, representative scholars mainly include Andrej Zwitter, Oskar J. Gstrein.

3. Problem Analysis

3.1 Analysis of Data Use and Related Issues in Epidemic Prevention and Control

According to article 1034 of the Civil Code of the People's Republic of China, "Personal information of natural persons is protected by law. Personal information is a variety of information recorded electronically or otherwise that can identify a particular natural person individually or in combination with other information, including the name of the natural person, date of birth, identity document number, biometric information, address, telephone number, E-mail address, health information and trace information, etc.; private information in personal information is applicable to the provisions on privacy; where there is no provision, the provisions relating to the protection of personal information shall apply". Thus, it has been discovered that personal information contains both private and non-private information. During the outbreak, the personal information collected by the government and medical institutions mainly includes personal information such as ID numbers, phone numbers, home addresses, travel records within 14 days, and close contacts. The purpose of investigating the above data information is to better reduce infection cases and curb the transmission of the epidemic. But personal privacy data will be maliciously spread on the network and infections will be suffered network violence due to some unreasonable investigation methods and the negligence of some staff. However, it is necessary for other people to know the travel records of infections. It can be found and checked as soon as possible if they have the same travel records with the infections, so as to eliminate the risk of sporadic cases. Therefore, China's units at all levels shall have a unified and clear provision: which citizens' personal information can be properly disclosed, which data information shall be encrypted and protected; according to the above discussion, how to find a balance between protecting the privacy and security of citizens' personal data and safeguarding public interests is a top priority.

3.2 Causes of Data Leakage and Related Analysis

(i) Subjective reasons: Due to the sudden outbreak, the investigation and collection of infections data are arranged hastily. Some staff have not received unified training and not been familiar with the relevant laws and regulations on data information privacy protection, so they didn't have a strong sense of confidentiality. For example, the encrypted computer was not used to record information in the process of investigating and collecting the patient's data and information privacy, but used personal electronic equipment. This may lead to such consequences: all citizens' personal privacy information would be leaked once personal electronic devices were accidentally lost, which is a threat to citizens' personal safety. Or some staff members have low professional quality and have no intention to take the privacy of citizens' personal data investigated at work as a conversation after dinner. What's more, some people will maliciously sell the private data information of infected in order to vent their negative emotions. Information disclosure for infected people, whether psychological or life, will hurt them, thereby affecting the entire social order.

(ii) Objective reasons: A number of privacy breaches have been linked to the healthcare system during the pandemic. The public security system uses the internal encryption network to transfer data, and all levels and police types in the public security system have set up their respective corresponding authority digital certificates to avoid errors in information management. However, different from the public security system, the medical system does not encrypt data collection, storage, use and other links, nor does it set internal access to information, and there is no perfect processing mechanism for data information.

Since each unit has different computer software or

operating systems for storing personal data and privacy information of citizens, which will cause certain technical problem. These technical problem will give opportunities for electronic fraudsters or various of violations to attack computer prevention and control systems, so that citizens' personal data privacy will be obtained illegally.

3.3 Difficulties in Personal Information and Data Protection During the Epidemic

3.3.1 The Law on the Protection of Citizens' Personal Information Data Still Needs to Be Improved

According to Article 1034 of the "Civil Code of The People's Republic of China", the personal information of natural persons shall be protected by law. The provisions on the right to privacy shall apply to the private information in personal information; In case no regulations are made, the regulations on personal information protection shall prevail. However, in the era of big data, even non-private personal information may be mined and utilized to identify other relevant information of natural persons. Therefore, personal information must be carefully used, and management of information collection and storage should be strengthened. For example, the network violence suffered by Miss Zhao, a girl who was confirmed in Chengdu. As the travel records of Miss Zhao involved multiple public places, some netizens believe that the behavior of Miss Zhao has increased the pressure of epidemic prevention. As a result, netizens even began to criticize her private life, causing Miss Zhao's private information was also targeted by human flesh search. In February 2020, National Internet Information Office of China issued the "Pay Attention to Personal Information Protection and Use Big Data to Support Joint Prevention and Control", which clearly stated that "the personal information collected for epidemic and disease of prevention and control shall not be used for other purposes. Any unit or individual could disclose personal information, such as name, age, ID number, telephone number, home address, etc., without the consent of the collector, due to the joint prevention and control work needs, and after desensitization of personal information except. However, how to ensure the public's right to know and minimize the risk of infections' privacy disclosure in practice? It remains to be explored and considered".

3.3.2 Loopholes in Citizens' Personal Information Data Storage

With the wide application of big data, the collected personal data can be permanently stored, and the storage itself also show the risk of privacy disclosure. This risk is reflected in two aspects, including external attack and internal leakage. External attack is generally from hacker. The current network security technology cannot absolutely resist the attack from hacker. In this case, the risk of being stolen still exists no matter who or how to store. However, internal disclosure is due to the lack of internal protection mechanism for personal data storage, or insufficient supervision and restriction of relevant staff, resulting in the disclosure of citizens' personal data. At the beginning of the epidemic prevention and control, personal information leakage problems also appeared. The information of confirmed infections, close contacts and overseas returnees is transmitted in the form of documents or screenshots on WeChat, Weibo and other platforms, affecting the daily lives of the parties. The information about personal information in epidemiological investigations is often very detailed, Disclosure of these information may bring great risks to the personal and property safety of all parties concerned. Especially for confirmed patients, permanent storage of network data means that the painful experience of COVID-19 will be permanently remembered. Although this is only a part of the patient's life experience, it is undeniable that this experience may indeed lead to the patient's distress in real life. If personal information, especially the private information that can identify the confirmed infections, is not well protected, it will have an impact on citizens'

lives once the data is disclosed. In order to minimize the impact of epidemic experience on patients, the most effective way to control the source of privacy disclosure is to strengthen the supervision and management of information security and data protection.

3.3.3 Citizens' Awareness of Data and Information Protection Is Generally Not High

The protection of personal information needs not only the norms of laws and regulations, but also the formation of the whole society's awareness of privacy protection. First of all, citizens' awareness of privacy protection should be improved. Most Internet users have not formed a clear understanding of the risk of personal information disclosure. Even if some users are concerned about the risk of disclosure of privacy information, it is difficult to use technical means to prevent the collection of personal data due to the lack of relevant professional knowledge. The direct consequence of this phenomenon is that personal information is unconsciously collected and used, which is extremely unfavorable to privacy protection. In response to this phenomenon, we should deepen the popular science publicity of privacy protection in the era of big data. In this context, we should clarify the necessity of privacy protection and guide citizens to protect their privacy information through publicity. Secondly, the privacy protection awareness of relevant staff should be improved. The personal data collected by enterprises are illegally stolen, and the flow regulation information mastered by the epidemic prevention department can be circulated on the network. The reason is that the privacy protection consciousness of the relevant staff is not strong, and the importance of protecting the personal information of the relevant staff has not formed a profound understanding. The relevant staff do not fully grasp the relevant laws and regulations, resulting in it becoming the victim of information disclosure. Emphasis should therefore be placed on strengthening the education and training of relevant staff and on increasing their protection awareness and responsibility.

4. Conclusions and Policy Recommendations

4.1 Improve the Goal of Using Relevant Legal Systems to Achieve Data Protection

The contradiction between personal information protection and public health security is actually the contradiction between personal interests and public interests. Individual justice interests are part of public interests. Public health security is the public interest, which also covers and reflects the fundamental and long-term interests of individuals. Therefore, the necessary information shall be disclosed in accordance with the specific provisions of laws and regulations in order to protect the public interests that reflects and represents personal interests. On the premise of protecting public interests, protect personal interests and personal information of relevant citizens to the maximum extent.

In response to the collection and use of personal information in epidemic prevention and control, the National Network Information Office has issued a "Notice on the Protection and Use of Big Data to Support Joint Prevention and Control", requiring governments and departments to attach great importance to personal information protection. This provision has strong guiding significance for the protection of personal information in epidemic prevention and control, and highlights the importance of national protection of personal information in epidemic prevention and control. However, in order to minimize unnecessary privacy disclosure, more complete and detailed laws and regulations are needed. Personal information disclosure standards for infectious diseases should be formulated as soon as possible. By establishing a unified information disclosure standard, the use of personal information is more standardized; specific criteria should identify which information should be disclosed and which information should not be disclosed or should be

avoided to the maximum extent possible, thus protecting the public's right to know and minimizing the risk of private disclosure by the persons concerned. Unified standards and principles are conducive to orderly epidemic prevention and effectively improve the effectiveness of epidemic prevention. Of course, in addition to improving laws and regulations on the use of personal information during the epidemic, the Internet information management department should also severely crack down on the disclosure of personal information, intensify efforts to combat illegal theft of personal information, and fully protect citizens' privacy.

4.2 Enhance the Supervision and Management of Information Security and Data Protection

During the outbreak, the risk of personal privacy data leakage can be avoided through strengthening technological innovation and technical means. For the collected personal information for epidemic prevention, special encryption systems can be developed to store and share, so as to prevent relevant departments from using private social platforms to transmit citizens' private data in their work. At the same time, strict access mechanisms should be established to ensure that only internal personnel responsible for specific quarantine work can access the personal information collected by real-name system, so as to minimize the dissemination of information and prevent internal leakage from the source.

At the same time, units with the right to investigate and collect citizens' private data should be required to establish a supervision and accountability mechanism to restrict the behavior of employee. If the unit causes the leakage of citizens' personal privacy data and information, it should be strictly accountable. The network information management department should promptly handle the illegal collection, use and disclosure of personal information in accordance with the relevant provisions of the "Network Security Law of the People's Republic of China" and the "Personal Information Protection Regulations" and other relevant provisions. Public security organs shall severely crack down on acts involving crimes according to law.

4.3 Enhance the Citizens' Awareness of Personal Data Protection

On the one hand, it is necessary to improve the protection awareness of relevant staff on citizens' personal privacy data and information. At the same time, it is also necessary to arrange training, so that citizens can learn more about the relevant laws and regulations such as "Network Security Law of the People's Republic of China" and "Personal Information Protection Regulations". Familiar with legal knowledge, so as to cultivate citizen's awareness of privacy protection and strengthen the sense of responsibility of staff.

On the other hand, it is necessary to improve citizens' network literacy. Consciously form the awareness of protecting private data information. For example, when using the Internet, citizens should not click on links of unverified information related to an outbreak investigation, so as to avoid the possibility of computer virus infection and personal information account theft. If personal information is requested by telephone in the name of government departments, citizens cannot easily inform them before confirming the identity of the caller; at the same time, citizens should shoulder social responsibility and maintain social order. In case of disclosure of personal data and information of other citizens, citizens should not expand the dissemination, but consciously protect others' data privacy information and reduce the harm of personal privacy data and information disclosure within the scope of citizen ability.

References

[1] Wang Jun (2020). "Weighing and Protecting the Public's Right to Know and Right to Privacy Under the Control of Major Epidemic in the City". *Henan Social Sciences* 28

(4): 74-81.

[2] Yan Yan (2020). "Citizens' Privacy Data Security in Public Emergencies: Thinking Based on the COVID-19 Epidemic". *Cyberspace Security* 11 (05): 12-17.

[3] Xia Jinlian (2020). "Information Disclosure and Privacy Protection in Epidemic Prevention and Control in the Era of Big Data". *Journal of Xichang University* (Social Science Edition) 32 (03): 42-48. 114, doi: 10.16104/j.issn.1673-1883.2020.03.010.

[4] Jeremy Wacksman (2021). "Digitalization of Contact Tracing: Balancing Data Privacy With Public Health Benefit". *Ethics and Information Technology* 23 (4): 1-7.

[5] Zheng Baozhang, and Feng Shi (2021). "Research on privacy Protection in the context of big data: From the perspective of the use of personal information in COVID-19 prevention and control". *Learning and Exploration* (4): 74-78.

[6] Zhang Han, Kang Fei, and Wang Guiping (2021). "Public Knowledge and Privacy Protection in Public Health Emergencies in the Context of Data: A Case Study of Novel Coronavirus Outbreak". *Science And Management* 41 (6): 47-55.

[7] Gao Yuling, and Xu Yongjun (2021). "Legal Issues and Countermeasures in the Use of Health and Medical Big Data Under Public Health Security". *Chinese Health Service Management* 38 (12): 918-921.

[8] Bai Juan (2021). "Information Security and Data Privacy Protection From Data Use During the Epidemic". *Network Security Technology & Application* (2): 62-64.

[9] Zhan Nan (2021). "Research on Personal Information Protection in Major Epidemic Prevention and Control: Based on Privacy Protection Design Theory". *Journal of Modern Information* 41 (1): 101-110.

[10] Emanuele Ventrella (2020). "Privacy in Emergency Circumstances: Data Protection and the COVID-19 Pandemic". *ERA Forum* (prepublish).

[11] Maria Tzanou (2020). "*Health Data Privacy Under the GDPR: Big Data Challenges and Regulatory Responses*". Taylor and Francis.

[12] Andrej Zwitter and Oskar J. Gstrein (2020). "Big Data, Privacy and COVID-19 — Learning From Humanitarian Expertise in Data Protection". J*ournal of International Humanitarian Action* 5 (1): 1-24.

[13] Zhang Weiqi, Jiang Yufei, and Yuan Huiyun (2021). "Research on Privacy Protection of Covid-19 Patients". *Chinese Medical Ethics* (10): 1316-1320.

[14] Li Yuan (2016). "Research on Personal Information Protection in Big Data Era". Ph.D. dissertation, Southwest University of Political Science & Law.