Personal Information Leakage Threats and Suggestions for Improvement in China's Epidemic Prevention and Control

Tianshu Chen

Guilin University of Electronic Technology ,Guilin, 541000, China

*Corresponding author.Email:724752407@qq.com

Abstract. The pandemic of the New Crown Epidemic has had an unprecedented impact on the protection of personal data, and the collection of personal data based on the Joint Prevention and Control Mechanism (JPCM) has increased the risk of personal data leakage and posed new challenges. The article firstly focuses on the connotation of personal data information, and clarifies the meaning of personal data information, as well as its nature of "identifiability" and "recordability". Then, through the definition of the theory, it explores the challenge of massive over-collection of information and diversification of collection subjects faced by the protection of personal data in epidemic prevention and control, concludes that the reason for the emergence of this challenge is the conflict between the security of personal data and the security of epidemic prevention and control and analyzes the relationship between the interests of the individual and the public interest. Finally, on the basis of this theory, the protection of personal data at the various risk nodes of personal data leakage will be achieved through the enactment of legislation to regulate the subjects, contents and rights concerned, increase the number of data and computer cross-management departments, and strengthen the supervision and management of the various aspects of the protection of personal data.

Keywords: personal information; data breach; conflicting rights; legislative regime and remedies

1 Introduction

Along with the new crown epidemic of the global pandemic, countries in order to prevent and control the epidemic,the implementation of a series of domestic such as screening suspected cases of nucleic acid testing and epidemiological investigations and a series of activities. In the process, goverment need to use digital means of collection of a variety of information from the public, this information can play a very positive role in controlling the epidemic, but at the same time, we must also see the risk of information leakage.

Article 6 of the Personal Information Protection Law of the People's Republic of China states that the collection of personal data shall be limited to the minimum extent

Y. Chen et al. (eds.), *Proceedings of the 2023 3rd International Conference on Modern Educational Technology and Social Sciences (ICMETSS 2023)*, Advances in Social Science, Education and Humanities Research 784,
https://doi.org/10.2991/978-2-38476-128-9_40

to achieve the purpose of processing, and excessive collection of personal data shall not be allowed. However, the actual situation is that in order to speed up the process of resuming work and production and reduce the risk of transmission of the epidemic, all regions and units collect as much personal data as possible. At the same time, the variety of data collection methods and parallel online and offline channels also tend to lead to an excessive scope of personal data collection, which poses a great threat to the protection of personal privacy.According to the actual situation of epidemic prevention and control in China in the past, article 32 of the Law of the People's Republic of China on the Prevention and Control of Infectious Diseases and Articles 10, 11 and 31 of the Regulations on Public Health Emergencies delegate the right to collect citizens' information to different departments. Therefore, multiple collection and repeated collection are common, which not only reduces the efficiency of epidemic prevention and control, but also wastes social resources. What is more serious is that once the personal data of confirmed patients, suspected patients or close contacts are leaked, it is very likely to cause irreparable impact. For example, after the diagnosis of a woman surnamed Zhao in Chengdu, Sichuan province, her personal privacy was frequently forwarded and received a lot of abuse[1].

Therefore, by analyzing the current situation of personal information protection in China through the past performance of China in epidemic prevention and control, and putting forward the corresponding legislative protection suggestions, not only can further improve the personal information protection law in China, but also can do a good job of protecting the personal information of the citizens in the prevention and control of epidemics in the future, which is of great reference significance to other countries in the world.

2 Reasons for challenges to personal information protection in China's epidemic prevention and control

2.1 Personal information protection faces conflict between public and private powers

Personal data in the era of epidemic prevention and control face the pull of both public and private power. On the one hand, public power is strengthened by the power of the data platform, mainly manifested in the informatization of public power[2], and on the other hand, private power is publicized[2], i.e., Internet giants such as Tencent and Alibaba break through the space of private law and move into the public sphere through their possession of information technology and digital resources, which makes the infringement of rights universal. Therefore, the State, Internet platforms and other subjects are collecting personal data through various channels, and the channels through which information subjects submit their information are numerous and dense, which exacerbates the possibility of data leakage.

Under the joint prevention and control mechanism, Epidemiologic Agencies Epidemiologic investigations through big data technology expose personal data to the public

while collecting healthcare big data information related to the outbreak.[3] In this process, due to the government's reliance on the private sector in epidemic prevention and control, mobile phones have become not only a tool for digital personalization, but also a mobile identity card for residents, and eventually these personal information is intentionally or unintentionally used commercially by mobile phone manufacturers, greatly increasing the risk of personal information disclosure.[4]

2.2 Conflict between personal interest and public interest

The contradiction between personal data protection and epidemic prevention and control security is actually caused by the conflict between individual interests and public interests, which are not merely antagonistic and conflicting, but on the contrary, the legitimate interests of individuals are often based on the premise of the realization of public interests, and the public interests also manifest the most essential interests of individuals. Therefore, in order to balance the relationship between the two, not only is it necessary to protect the public interest on behalf of the individual, i.e., necessary information should be disclosed in accordance with the specific provisions of laws and regulations, but it is also necessary to maximize the protection of the individual's interests under the premise of safeguarding the public interest, i.e., when it comes to the privacy of the subject of the information in question, to adopt specific legal means to maximize confidentiality. In conclusion, China has not formulated a special law in this area, and the provisions of personal data protection are mainly scattered in the administrative regulations, departmental regulations, so the legislation on resolving the conflict between personal interests and public interests still needs to be improved.

2.3 Inadequate protection of personal information by laws and regulations

Difficulties in the practical implementation of personal information protection.

Article 1035 of the Chinese Civil Code provides that "the processing of personal information shall follow the principles of lawfulness, legitimacy and necessity", which means that the processing of personal data shall not be excessive. Specifically, this provision does not specify how "necessity" should be grasped, which makes it difficult to apply the law. Moreover, these legal provisions are mainly general protection provisions on the use of personal data, and do not make specific provisions for the serious situation of personal data leakage under epidemic prevention and control.

Lack of recognition of rights in the protection of personal information.

The Chinese Civil Code provides that "the personal information of a natural person shall be protected by law" and that personal data may be used reasonably in the public interest or for the legitimate interests of that natural person. These legal provisions only state that citizens' personal data are protected by law, but the specific right of "citizens' right to information" is not mentioned or recognized. Meanwhile, in order to further refine the implementation of the protection of personal data under the epidemic prevention and control, the Central Internet Information Office issued the "Notice on Doing a

Good Job in Protecting Personal Information by Using Big Data to Support the Work of Joint Prevention and Control", of which Article 3 stipulates that: "No unit or individual shall, without the consent of the person whose information is being collected, disclose personal data, such as name, age, identity card number, telephone number, home address, etc.". except for the needs of the joint prevention and control work and after desensitization." Although the article tries to define and limit the scope of personal data collection, there is still a big problem in applying it due to the huge correlation of information and social relations interests involved behind the personal data of information subjects.[5] If only emphasis is placed on accurate prevention and control, then will bring suffering to many patients or suspected patients of the epidemic, not only in terms of the disease itself, but also in terms of the discrimination brought about by the disclosure of information about the disease, and the mental suffering that may be brought to the families.

3 Suggestions and improvement of legislative guarantee

3.1 Recommendations for regulation before personal information collection

Authorization of subjects collecting personal information.

First, it is recommended that the list of executive agencies authorized to collect and use relevant personal data be clarified, as well as the process of personal data collection by each unit be standardized to ensure that the information collected is used only for epidemic prevention and control and disease control. Second, in order to reduce the duplication of collection work, each unit must realize data sharing. In the process of data sharing, the sharing scope and sharing authority of each department should be clarified to ensure not only that the information collected by the data management department can be synchronized to the management personnel at the grassroots level, but also that anonymization, de-identification, access control and other means should be used to constrain the behavior of data sharing.[6] Third, it is recommended to raise the legal awareness of management departments and strengthen the confidentiality awareness of grassroots personal information collection staff to ensure that the risk of personal information leakage is eliminated at the source.

Contractual rules for trading personal information need to be clearly regulated.

Generally speaking, when a user checks the "Read and agree to..." box on the registration or login page, it means that the personal data subject has entered into a "transaction contract" with the personal data collection authority on a voluntary basis. This means that the personal data subject has voluntarily entered into a "transaction contract" with the personal data collection agency. In order to ensure that the data subject has a free and uninterrupted right to decide on the meaning of this expression, the subject's consent must not be inferred from a silent, pre-ticked box. Instead, "contracts of exchange" should be regulated more explicitly. Blanket open-ended processing of personal data and blanket consent are not enough; the "transaction contract" must specify the different ways in which different levels of personal data will be processed, the scope

of the processing, and the consequences of the processing. The rules should be expressed in a clear and understandable manner to ensure the rights of the subject of the personal data. Finally, the subject of personal information has the right to withdraw his/her personal information at any time, unless significant public interest is involved, to protect the subject's right to dispose of his/her personal information. Of course, the collection, release, and commercialization of personal information that was already lawful prior to the withdrawal will not be retroactively applied.

Ensuring parity of rights in data collection systems.

Although personal data information is enjoyed by its subject, but in the process of personal information disposal, the right of data disposal is not equal, personal data collection party is often the power of the superior. In this era of big data, personal information is always collected based on forced, fraudulent, unconscious and other reasons. Therefore, if citizens want to have equal rights to trade data with government departments and large corporations, the right to personal information should be protected through a series of laws and regulations. For example, when a government department or private enterprise collects citizens' personal information, it should provide the identity, contact information, and legal basis of the person who collects the information or the representative, so as to make it easier for the parties concerned to inquire, complain, or defend their rights after being infringed upon.

Auditing the fairness of Big Data algorithms.

Big data algorithms have played an invaluable role in the epidemic as science and technology have advanced by leaps and bounds, but this has also raised concerns about how big data algorithms calculate and analyze their personal information. For example, ChatGPT's different algorithms may lead to different morals and ultimately send misinformation to users such as racial discrimination[7]. Therefore, we need to ensure that all the big data algorithms of the software that collects personal data for epidemic prevention and control that flow into the market are compliant and legal, and kill those algorithms that threaten the security of personal information before they leave the factory by prior vetting.

3.2 Recommendations for remedy after personal Information leakage

Clarify the notification obligations of the leaking party.

Personal data leakage is a very common problem in data security risks, such as the loss of data transmission equipment, hacker attacks, staff errors, malicious leakage of the relevant informed personnel and other reasons. Then, personal data leakage in the epidemic, especially involving personal dignity and property security and other sensitive personal data, is very likely to cause serious mental and property damage to the data subject, so once the data leakage occurs, how all the parties cooperate to notify the relevant supervisory authorities and rights holders, as well as how to remedy the situation is also a very important link.

First of all, to determine the frontline first responsible person for the leakage of personal information as the notification subject, if the subject fails to fulfill the notification obligation, according to the size of the consequences of the determination of the size of its responsibility, as well as to determine the scope of its liability is criminal liability or civil liability. Second, the notification document needs to be clear and specific, containing the content, scope, and level of the personal information that has been leaked. Finally, it is clear how long the first responsible person needs to notify all parties after the leakage of personal information. Not only do they need to notify the competent authorities immediately to remedy the situation, but they also need to report to their own higher management within 12 hours after remedying the situation to no avail, and of course successful remediation should be reported to the higher management within 48 hours for the record.

Improving the legal liability of obligated subjects after a data breach.

China's current legislation on the protection of personal information mainly focuses on the punishment after the leakage, in China's Criminal Law, Civil Code, Personal Data Protection Law, Network Security Law, Prevention and Control of Infectious Diseases Law and so on have been involved. Although this aspect of China's more perfect, but the system is more decentralized, does not have a systematic legal mechanism, the introduction of departmental regulations, local laws and regulations, while the law accounted for less than 10%[8], and because of the lack of constitutional basis, so improve the legal responsibility of all parties still has a lot of room for development. The first priority is to establish the nature of the right of personal information from the constitutional level, so as to build a legislative framework for the protection of personal information, and to carry out relevant work from both the public and private law levels, and finally to realize the criminal liability, civil liability and administrative liability.

In addition, since epidemic prevention and control is based on the need to safeguard the public interest, it is natural that the use of personal data is more lenient than the general use of a commercial nature, and therefore it is necessary to add some additional exemption legislative proposals regarding the need to safeguard the public interest. However, this does not mean that the collector of personal data is exempted from complying with his other obligations in the field of personal data protection. In the case of very sensitive personal information, even stricter legal provisions will be applied.

4 Conclusions

In the past few years, under the influence of the epidemic, the collection, openness and sharing of personal data have given the general environment high-quality data resources, and China has also added a lot of investment in personal information protection, but the conflict between public power and private rights, and the balance between individual and social interests are all eternal topics for a country, and personal information leakage hasn't lowered the risk because of the investment of a drop in the bucket. Nowadays, the impact of the epidemic on society is not as serious as in the previous two years, but no one knows when the next social and public crisis will come.

In order to eliminate the phenomenon of over-collection of personal information, ensure that there is no proliferation of collection subjects, put the personal information protection law into practice, strengthen the legal awareness of information collectors, and guarantee the means of redress for citizens after their personal information has been leaked, China needs to look at every aspect of the operation of personal information, starting from the citizen's consent to the collection of personal information to the collection of personal information by the collector of personal information utilizing the algorithms of big data to serve the society and obtain the benefits. China needs to look at every aspect of the operation of personal information, starting from the citizen's consent to the collection of personal information to the collector's use of big data algorithms to serve society and gain benefits, and establish a legal system for the protection of personal information from the fundamental law to the private law, and from the substantive law to the procedural law.

References

1. Liu,W.H. (2020)How is the law supposed to protect you? Chengdu girl. Sichuan Legal Daily,5:1-8. https://doi.org/10.28664/n.cnki.nscfz.2020.001268.
2. Saeki Soichiro. (2022).Impact of the "Amendments to the Act of the Protection of Personal Information" to Global Health Research Conducted in Japanese Medical Facilities.. Journal of epidemiology, 32(9/10):438. doi:10.2188/JEA.JE20220141.
3. Guo,P.F.,Lin,H.X. (2022)Protection of personal information in public health events: from the perspective of COVID-19 prevention and control. Journal of Xihua University (Philosophy and Social Sciences Edition),41:63-74. https://doi.org/10.12189/j.issn.1672−8505.2022.01.008.
4. Hong,X.L. (2022)On data utilization and protection of personal information in epidemic prevention and control. Research on Local Legislation,4:49-59.
5. Chen,P. (2022)Research on protection of personal information in public health emergencies. Digital communication world,4:116-118. https://doi.org/10.3969/J.ISSN.1672-7274.2022.04.038.
6. Hacking technique. (2022)A brief analysis and reflection on the concepts of de-identification and anonymization. http://www.hackdig.com/08/hack-737048.htm
7. Berşe， S.， Akça， K.， Dirgar， E. et al. (2023)The Role and Potential Contributions of the Artificial Intelligence Language Model ChatGPT. Annals of Biomedical Engineering,26(11):59-60. https://doi.org/10.1007/s10439-023-03296-w
8. Liu,W.L. (2019)Personal information security problems and countermeasures under the background of big data era. Communication world,26(11):59-60. https://doi.org/10.3969/j.issn.1006-4222.2019.11.039.