Proceedings of the 3rd International Conference on International Law and Legal Policy
DOI: 10.54254/2753-7048/55/20240044

Legal Mechanisms for the Protection of Personal Information in Public Surveillance

Siyu Liu[1,a,*]

[1]*School of Humanities and Law, China University of Petroleum (East China), 66 Changjiangxi Street, Qingdao, China*
a. 2117020122@s.upc.edu.cn
**corresponding author*

Abstract: How public surveillance balances the relationship between preventing and combating crime and protecting citizens' personal information is a social issue of common concern to the people. With the advent of the digital age and the unprecedented development of Internet technology, public surveillance has spread to all corners of people's lives. Although big data technology brings a lot of convenience to people's daily work and life, it is also prone to cause personal information security problems. For example, the leakage of personal information and the release of personal information have had a great impact on the personal property and mental aspects of citizens. Lack of protection of citizens' right to personal information in public areas, exposing citizens to surveillance as if they were transparent. A strong sense of being monitored and controlled seriously affects the happiness index of citizens. Therefore, the question of how to use public surveillance to safeguard the public interest without infringing on individual privacy is particularly important.

Keywords: Public surveillance, Personal information, Protection

1. Introduction

In order to cope with emergencies or the needs of the judicial authorities in handling cases, the relevant administrative departments will access the surveillance video of public areas to compare the route trajectory of people, contact with the crowd and other information. This information will be used for the apprehension of suspects and the restoration of social order, but the access to personal information that is not handled properly also increases the likelihood of putting citizens at risk. Whether or not a citizen's right to privacy is violated depends mainly on whether or not the private information obtained has a negative impact on the citizen and the degree of acceptance by the citizen. Take the COVID-19 epidemic as an example, Chinese outbreak control authorities rely on surveillance in public areas to locate infected populations. Obtaining information on persons in close contact with them and publicizing it on the Internet. Despite serving the needs of epidemic prevention and control and maintaining public health security. But it also exposes the person whose information is made public to cyber violence, affecting the citizen's right to reputation and personhood [1]. The legal provisions relating to the protection of the right to personal information are imperfect and fragmented, resulting in a lack of awareness of the protection of citizens' personal information on the part of administrative agencies and relevant organizations and institutions. The pressing issue is how

DOI: 10.54254/2753-7048/55/20240044

to appropriately allow citizens to give up their private information when the relevant administrative departments or organizations safeguard the public interest.

2. Overview of Public Surveillance and Protection of the Right to Personal Information

2.1. Conceptualization of Public Surveillance and Personal Information

2.1.1. Concept of Public Surveillance

Surveillance according to the Xinhua Dictionary is interpreted as monitoring and control. It refers to the process of observing, recording and detecting a specific object, place, system or activity in real time through the use of various technological means in order to collect relevant information and analyze and process it.

Video surveillance of public places, referred to as public surveillance. It refers to the use of electronic equipment for real-time filming and monitoring of socially recognized service establishments or completely open or semi-open establishments for public use, and the storage of the filmed information [2]. Its purpose is to safeguard the public interest, and it can detect and deal with various security risks and abnormalities in a timely manner by observing the situation in public places in real time. Assisting in the investigation and collection of evidence in the event of violations of the law and providing assistance to the relevant law enforcement agencies or authorized units. It can be seen that public surveillance is directed at all people or things under the surveillance perspective, with the obvious characteristics of serving the public interest, real-time and informative, recording and tracking.

2.1.2. Right to Personal Information in Public Surveillance

The right to personal information has been a central theme in the protection of information rights in recent years. The right to personal information is distinct from and related to the right to privacy. By distinguishing between the two and setting different protection rules on this basis, we can better improve our privacy and personal information protection system.

The right to personal information and the right to privacy are two concepts that are either intertwined, distinct, or encompassing. The right to privacy and personal information both belong to the category of personality rights and interests, but the right to personal information is an active right that can be actively exercised to utilize. It manifests itself in the domination of personal information and autonomous decisions. In contrast, the right to privacy is a passive right whose object emphasizes the attribute of "invisibility" and is characterized by a reluctance to share information with others and exclusivity.

Based on the above basic demarcation, it can be seen that the personal information in the surveillance of public places includes the facial features, bio-information, identity, medical and health care, whereabouts, etc. of individuals captured by image capture, personal identification equipment and surveillance equipment. They are capable of identifying a specific natural person, either alone or in combination with other information. In addition to passive defense against infringement by third parties, the right holder can control and exploit them exclusively, actively and dynamically.

2.2. Existing Laws on the Right to Personal Information in China and Their Practical Application

2.2.1. Relevant Provisions of the Civil Code

Civil Code of the People's Republic of China (hereinafter referred to as the Civil Code) Passed in May 2020. It clarifies the nature of personal information and its place in the civil rights system, and

DOI: 10.54254/2753-7048/55/20240044

completes the design of the top-level framework for the protection of personal information. The protection of personal information is regulated in detail in the "Privacy and Personal Information Protection" section of the Title of Personal Rights, which specifies three principles and five conditions for the handling of personal information. The Civil Code defines the infringement of personal information as the unauthorized handling of personal information of others and the leakage, falsification and loss of personal information due to negligence.

With the rapid development of technology, the exposure and unauthorized use of personal information in real life is increasing, especially in cyberspace, where privacy infringements abound. In view of this situation, it is particularly urgent to respond effectively to the problems of leakage, falsification and loss of personal information. According to article 1034 of the Civil Code, According to the hierarchy of civil rights, in principle, except for some special sensitive personal information, when there is a conflict between general personal information and the right to privacy, the right to privacy should be given priority protection [3].

2.2.2. Relevant Provisions of Personal Information Protection Law of the People's Republic of China

With the enactment of the Personal Information Protection Law of the People's Republic of China, it marks a significant increase in the extent to which personal information is protected in our country. The Act further refines and improves the principles to be followed in the protection of personal information and the rules for the handling of personal information on the basis of the relevant laws. It clarifies the boundaries of rights and obligations in the handling of personal information, and constructs rules for the handling of personal information centered on "notification and consent".

In recent years, the misuse of personal information in China has occurred from time to time, which has led to a high level of public concern. In response to social concerns, the Personal Information Protection Law of the People's Republic of China strictly regulates the identification of personal information. It clearly stipulates that the installation of image capture and personal identification equipment in public places should be necessary for the maintenance of public safety, comply with the relevant state regulations, and set up a conspicuous reminder of the logo. This law imposes strict obligations on processors of personal information. Not only must it ensure that its own personal information processing activities comply with the law, assume due social responsibility and accept social supervision, but it must also enable it to process personal information legally and protect the security of personal information through measures such as the establishment of fair and equitable platform rules and the curbing of unlawful behaviors.

3. Conflict Analysis of Public Surveillance and Personal Privacy

3.1. Case Study: Community Public Surveillance and Owners' Right to Information Dispute

The collection of information on residents in community building should be based on the necessary, appropriate and accurate purpose of collection, and in a manner that minimizes the impact on the rights and interests of individuals. And now that communities are deploying surveillance cameras in public monitoring spaces to increase safety and security, the scope of personal information collection from residents has expanded.

In a residential district in Shanghai, in order to gradually promote the construction of a smart community, the neighborhood committee resolved to set up monitoring and control camera equipment in the district's main roads, public activity places and the interior of the elevator. Concerned about the risk of leakage and misuse of his personal identification information, daily whereabouts and private life, Mr. Zhang, an occupant, filed a lawsuit in the People's Court for violation of his right to privacy. The court considered the issue of balancing public safety and the right to privacy and ruled that the

DOI: 10.54254/2753-7048/55/20240044

OC could retain some of the surveillance equipment in key areas. However, it must strictly follow the relevant laws and regulations, ensure the safety and confidentiality of the monitoring data, and accept the supervision of the owner. The installation of public surveillance in the community in the case did not cause substantial infringement on the residents, but inadvertently increased their mental stress. It affects normal productive life. Therefore how to balance the relationship between public surveillance areas and personal information security has become an urgent problem.

3.2. Analysis of Conflict Points between the Right to Personal Information and Public Surveillance

There will inevitably be a conflict between the information stored in electronic surveillance in public places and the right to personal information. The purpose of public surveillance is often to maintain public safety, combat crime, or perform other social management tasks. In the process, surveillance may involve the collection, storage, analysis and use of personal information. Such collection and use of personal information may violate an individual's right to information, especially when the surveillance is too extensive, the data is used inappropriately, or the surveillance data is misused. Second, the right to personal information emphasizes the privacy and security of personal information, whereas public surveillance may require some degree of disclosure or sharing of personal information. Such disclosure or sharing may expose personal information to risks such as leakage and misuse, which may in turn violate an individual's right to privacy.

Electronic surveillance in public places is one of the main ways leading to the leakage of personal information. Clarifying the point of conflict between public surveillance and the right to personal information is of great significance to the protection of citizens' personal information. This paper considers two main points of conflict between the two:

First, the asymmetry of the rights of public and private subjects. There is a significant information imbalance between individuals and authorities. This imbalance is mainly characterized by differences in the information technology capabilities possessed by the public and private sectors. The use of emerging technological tools by rights authorities and their departments to make it easier to track and monitor people's behavior. Moreover, large-scale data and information collection ultimately flows to data controllers, leaving users at a disadvantage in relation to the subjects who collect and use the data. users' rights to make their own choices and to be informed are less likely to be protected. The mismatch between the costs and rewards of protecting the right to personal information. The mismatch between the costs and rewards of protecting the right to personal information also increases the likelihood that they will misuse technology to infringe on information relating to natural persons [3].

Second, the involvement of third services increases the risk of leakage. Data information obtained from continuous surveillance in public space is widely stored in third-party service organizations, increasing the risk of leakage in the three stages of data collection, data processing and data storage. The use of cloud computing information technology has led to the massive presence of personal data and information in the cloud. If sharing and access rights to data in the cloud are not managed properly, it could lead to data being accessed or misused by unauthorized personnel, putting privacy at risk.

3.3. Similarities and Differences between Chinese and Foreign Legal Frameworks for the Protection of the Right to Personal Information

With the rapid development of mobile technology represented by the Internet, the world has entered the era of digital economy. All countries are actively building a legal system for the protection of personal information. The protection of the right to privacy in the United States has risen to the level of the Constitution. In particular, the right to privacy was formalized as a general constitutional right

DOI: 10.54254/2753-7048/55/20240044

independent of the Fourth and Fifth Amendments in the 1965 case Griswold v. Connecticut. The United States enacted the landmark Privacy Act in 1974, which explicitly recognizes an individual's right to be left alone and establishes the legal cornerstone of the U.S. government's personal information privacy protections. The U.S. has also adopted a series of specialized individual pieces of legislation that provide clear and detailed regulations on the privacy of personal information. For example, the U.S. Federal Electronic Communications Privacy Act, enacted in 1986, and the Global E-Commerce Policy Framework document issued by the Clinton Administration in October 1997 [4]. The protection of the right to personal information in the United States is not only enshrined in the U.S. Constitution, but also in state laws. It is worth mentioning that California is better at protecting the right to personal information, and its California Online Privacy Act has played an important role in the construction of the legal framework for the protection of the right to personal information in the United States [5].

In Europe, the main laws enacted on the protection of personal information include the EU Directive on the Protection of Personal Information of 1995, the EU Directive on the Protection of Information in Electronic Communications of 1996, the Directive on the Protection of Information in the Telecommunications Sector of 1997, and the General Principles for the Protection of Personal Privacy on the Internet of 1999 [6]. It is regarded as the most authoritative and detailed legislation in the field of privacy protection in the world. Chinese Civil Code, which will come into effect on January 1, 2021, establishes a special chapter to include the protection of personal information and the right to privacy. The Personal Information Protection Act, which will come into force on November 1, 2021, will be passed through the legislation of each country, taking into account the advanced system of personal information protection law of the General Data Protection Regulation of the European Union.

In terms of protection principles and objectives, countries have emphasized the privacy, security and legitimacy of personal information. The United States, through its Constitution and a series of laws, ensures the sanctity of the individual's right to privacy. Europe, on the other hand, focuses on the free flow and rational use of personal information, while safeguarding the fundamental rights and freedoms of the individual. For its part, China has clarified in its legislation the basic principles of personal information protection, including the principles of legality, legitimacy and necessity, the principle of clarity of purpose and the principle of informed consent.

There are some differences between countries in terms of specific implementation measures and regulatory mechanisms. In addition to legislative protection, the U.S. actively promotes industry self-regulation to protect the privacy of personal information by diversified means. Europe, on the other hand, has strengthened the regulation and enforcement of the processing of personal information through the establishment of a unified supervisory authority and a system of data protection officers. China has provided strong institutional safeguards for the protection of personal information by stipulating in the Personal Information Protection Law the obligations and rights of personal information protection organizations, personal information processors, and the penalties for violations of the law.

4. Risks and Consequences of Leakage and Misuse of Public Surveillance Information

4.1. Lack of Unified Management of the Current Public Video Surveillance Application Specification

With the continuous development of the times, public video surveillance has been widely used, and our country is paying more and more attention to it in terms of legislation. In recent years, various ministries and commissions of the State and local people's governments at various levels have issued various regulations and local normative documents. To date, China has 26 provincial-level places, 18

DOI: 10.54254/2753-7048/55/20240044

municipal-level places have introduced local laws and regulations, a total of 48. Among them, divided into "technical defense management category" and "video management category", including local laws and regulations and local government regulations [7].

However, although the government attaches more and more importance to the supervision of public video surveillance, but compared to the rapid development of electronic information, local laws and regulations have not formed a unified specification. This has led to distinctive management in each region, which is better adapted to local human customs, but when it comes to cases of infringement of the right to personal information across regions, how to adjudicate has become a judicial challenge.

4.2. Consequences

4.2.1. Increased Discrimination and Inequality

Public video surveillance collects a large number of citizens' personal information and categorizes and filters it in a certain way, and this situation can lead to discrimination of the majority against the minority, which to a certain extent exacerbates social inequality. For example, why is it not unfair that public surveillance is more likely to monitor people with a criminal record, including specific alerts when an ex-convict is detected. Strengthening the management of public surveillance is meant to serve the purpose of maintaining social justice, which is already contrary to the original intent.

4.2.2. Other Adverse Consequences

Personal information has a value in itself, and the fact that it can be utilized to generate income further demonstrates the property value of personal information. Since personal information has property attributes, the probability is high that the leakage of personal privacy will lead to financial losses, including but not limited to the leakage of personal information may be used to apply for credit cards, make malicious overdrafts, telecommunication fraud, overdrafts and arrears on cards under false names, etc., leading to property losses.

Leakage of personal information may also lead to moral and reputational damage, and excessive spam and nuisance calls can seriously affect the comfort of citizens' personal lives. It can even lead to the creation of rumors that can affect an individual's reputation, as well as lead to citizens facing personal safety and, in extreme cases, kidnapping and stalking.

5. Improvement Path of Personal Information Protection in China

5.1. Activating Local Legislation

Based on the above analysis, the U.S. states have legislative mobility, resulting in a healthy interaction between federal and state legislation. Judging from the current state of local legislation in China, local legislation on public surveillance has been introduced one after another. However, only a small number of regions have enacted creative legislation on the protection of the right to personal information, and some of the regions that have enacted local legislation have not been able to make timely adjustments in accordance with the Law on the Protection of Personal Information [8]. China gives full play to the initiative of local legislation and introduces laws and regulations related to the protection of the right to personal information in line with local realities. Let it interact with laws related to public surveillance, so that central and local legislation can form a positive interaction and promote the protection of the right to personal information in the region.

DOI: 10.54254/2753-7048/55/20240044

5.2. Establishment of a Sound Information Property Security Management System

The property value of personal information creates the need for personal information to be protected by law, and it is of great significance to establish a sound information property security management system based on this. The system was established on the basis of: First, personal information not only has personal attributes, but also has property attributes, which, as a kind of personality right with property attributes, can be realized in the legal level of property. This kind of property not only will not damage the personal independence and integrity of personality, but through reasonable use, individuals can enjoy the benefits of information property. Especially in the digital society, personal information can be stored on data platforms and undergo a series of processes such as collection, processing, and handling, which makes it controllable and circulating, which gives personal information a property value that can be utilized and traded. Secondly, the California Consumer Privacy Act of the United States clarifies for the first time at the legal level the nature of the property right of personal information and specifies that enterprises or individuals should give certain economic incentives to the subject of the information when collecting, selling, sharing or retaining personal information, which includes, among other things, remunerations given to users. This provision not only elevates the legal status of personal information protection, but also provides a legal basis for assigning value to personal information in commercial utilization.

5.3. Improve the Rules of Personal Information Infringement Damages Relief

According to Article 69 of the Personal Information Protection Law, if the handling of personal information infringes on the rights and interests of personal information and causes damage, and the processor of personal information cannot prove that he or she is not at fault, the processor shall be liable for damages and other tortious liabilities. In fact, in the field of personal information protection, the personal information affected by a specific act of notification of consent is often more specific, and its intrinsic value is not easy to be measured accurately. Compared with the traditional infringement of rights and interests, the new type of damages brought about by the infringement of personal information is not only broader in scope, but also more insidious and difficult to be detected, and the specific amount of the economic loss has thus become difficult to be determined, resulting in the subject of personal information being difficult to obtain substantial relief after their rights and interests have been impaired [9]. The relevant departments should further optimize and improve the rules for the relief of personal information infringement damages, such as establishing the scope of personal information infringement damages, including direct economic losses and compensation for moral damages. For losses that are difficult to quantify, such as moral damages, they can be determined on a graded basis by reference to factors such as local economic development and average wage levels. In addition, the relevant administrative authorities can build a punitive compensation system on the existing basis to increase the burden of personal information infringement and effectively prevent the infringement of personal information.

6. Conclusion

Strengthening the protection of citizens' personal information through the use of legal means has a positive effect on maintaining social stability and promoting harmonious social development. This thesis proceeds with the search for a balance between the management of public surveillance in the fight against crime and the protection of citizens' personal information. Starting from the concepts of public surveillance and the right to personal information, we analyze the relevant laws and real-life cases, explain them in detail, compare the similarities and differences between Chinese and foreign laws, and draw lessons from them. At the same time, for China's current personal information protection problems put forward targeted measures to effectively reduce the occurrence of personal

DOI: 10.54254/2753-7048/55/20240044

information security problems, specifically including the following: Utilizing the initiative of local legislation, establishing a sound management system for information property security, and improving the rules for the relief of personal information infringement damages.

References

[1] *Xianchao Liu. Study on the Risk Tolerance of Citizens' Private Information Leakage in Response to Public Health Emergencies [J]. Library research ,2023,53(06):92-101.*

[2] *Liming Wang: On the Applicable Relationship between the Personal Information Protection Law and the Civil Code, in Huxiang Law Review, No. 1, 2021*

[3] *Lee A. Bygrave, Privacy and Data Protection in an International Perspective, Scandinavian Studies in Law,Vol.56,2010,p.177.*

[4] *lrvin David. Ethics, Encryption, and Evolving Concepts of Personal Privacy in the 'Black Box Library'[J]. The Serials Librarian, 2021,81(1):144-145*

[5] *Hyman D A, Kovacic W E. Implementing privacy policy: Who should do what [J].Fordham Intellectual Property, Eedia & Entertainment Law Journal,2019,29(4):1117- 1150*

[6] *Alrayes Fatma S., Abdelmoty A. 1.,El Geresy W. B., Theodorakopoulos G.. Modelling perceived risks to personal privacy from location disclosure on online social networks[J]. Interational Joumal of Geographical Information Science,2020，34(1):177-178*

[7] *Xufang Xiang. Legislative Study on Public Video Surveillance [D]. Zhongnan University of Economics and Law ,2021.DOI:10.27660/d.cnki.gzczu.2020.000267.*

[8] *Can Wang. Paths and Options for Improving the Legislation on the Right to Personal Information [J]. Information security research,2024,10(03):263-267.*

[9] *An Wang. Study on the Legal Protection of Personal Information in the New Situation [J]. Legality Vision,2024(09):49-51.*