Interpretation of Article 40 of the Current Constitution: Freedom of Communication and Protection of Communication Secrets under the Background of Big Data

Yang Bai*
China Jiliang University, Hangzhou, Zhejiang, China
**Corresponding Author.*

Abstract: In the context of big data, network communication has taken on a novel form. Technological advancements have undeniably facilitated daily life, yet they have simultaneously introduced fresh challenges concerning citizens' freedom of communication and the constitutional right to the protection of communication secrets. This paper endeavors to delve into and deliberate on several pivotal questions: do the rights to personal information and privacy in contemporary communication fall within the purview of constitutional protections? Have the fundamental prerequisites for communication in the new internet era undergone any transformations? Do intentionally collected or inadvertently acquired data constitute a form of accessing citizens' communication content, and if so, does this amount to an infringement? Furthermore, this paper proposes a perspective on safeguarding citizens' fundamental communication rights, emphasizing the importance of striking a balance between technological progress and the protection of individual liberties.

Keywords: Big Data; Freedom of Communication; Communication Secrecy; Personal Information

1. Background and Problem

1.1 The Meaning of Modern Communication

Since ancient times, communication has been an important means of communication for people, serving as a carrier for the divergence and overflow of social relationships. At first, the invention of communication methods fulfilled people's expectations of breaking through the limitations of information exchange space. Communication speed required timeliness, and content required confidentiality. Ancient communication methods demonstrated the ingenuity of ancient wisdom. There are records of the ruling class beginning to centralize the management of postal services during the Yin and Shang dynasties. By the Zhou dynasty, postal services had developed significantly. At that time, communication was mainly used for the transmission of official documents and military information. People were familiar with the beacon towers in the Western Zhou Dynasty, which used fireworks as information elements to quickly transmit military information. "Beacon" was a fire signal used for night alarms, while "Sui" referred to the smoke produced by burning wolf dung and used for daytime alarms [1]. In addition to timeliness, confidentiality is also an important guarantee for the smooth operation of military orders. In ancient times, Yin Shu divided bamboo slips with pre written characters into three parts, with each person holding one piece, and then combined them into one after delivering them to the recipient, in order to display the complete content for the purpose of confidentiality. This shows that there were already means to protect communication secrets at that time.

Today, the meaning and significance of communication have undergone tremendous changes. Telephone, telegraph, radio, television, etc. all belong to the narrow category of communication. Generalized modern communication has a broader scope, where information can be referred to as communication from the sender to the other end through any transmission medium. The transformation of the meaning of communication relies on the leapfrog development of network technology. In recent years, the emergence of 5G mobile communication technology has changed people's lifestyles and redefined communication. Based on mobile communication networks and big data

technology, email, online chat tools, transaction software with chat functions, service application software, and even live streaming rooms have become carriers of information. The content sent and received through these software contains a large amount of personal information, transaction protocols, and other data, which have the characteristics of openness, dynamism, and complexity. That is, the communication channel has openness, and its parameters are dynamically time-varying; Users have dynamism, the service targets are not specific, and there are "virtual" characteristics; The network environment is complex, with large-scale, high-frequency, large bandwidth, and multi interface networks being multiplexed in the same time and space [2]. Does the new form of communication bring new issues in the protection of constitutional rights, which inspires the author to think.

1.2 The Provisions in the Constitution Regarding Freedom and Confidentiality of Communication

The current public and private laws in China provide a more scientific, rigorous, and comprehensive legal source for safeguarding citizens' freedom and confidentiality of communication. Article 40 of the Constitution stipulates: "The freedom of communication and communication secrets of citizens of the People's Republic of China are protected by law. Except for the need for national security or the investigation of criminal offenses, no organization or individual may infringe upon the freedom of communication and communication secrets of citizens for any reason in accordance with the procedures prescribed by law by public security organs or procuratorial organs. Set up features such as concealment, destruction Illegal opening of other people's letters and other situations that infringe upon citizens' communication rights, without specifying specific infringement situations and specific safeguard measures, especially in the context of big data technology.

Scholars such as Chen believe that Article 40 of the Constitution adopts the method of legal reservation, and even strengthens the method of legal reservation, providing higher protection for freedom of communication and communication secrets than the rights to expression and privacy [3]. Scholar Lin believes that legal reservation allows ordinary law to implement and protect basic rights, while also allowing ordinary law to restrict basic rights, that is, allowing the legislative body to define and protect basic rights. This is a way for legislators to defend against the abuse of administrative power. Once the legislative body is weak and its legislative power is easily eroded and sidelined, legal reservations still cannot effectively protect basic rights [4].

1.3 Problems

The effective protection of citizens' freedom of communication and the right to communication confidentiality requires high legislative skills from legislators. Article 40 of the Constitution only stipulates that national security organs, public security organs, and procuratorial organs may inspect citizens' communication content for limited purposes, procedures, and methods. This provision sets an internal limit for freedom of communication, but in practice, some legal norms in legislation stipulate that citizens' communication content can be inspected in other situations except for national security or the need to investigate criminal offenses. A typical example is Article 76 of the Gansu Province Road Traffic Safety Regulations: "For the purpose of investigating accident cases, the traffic management department of the public security organs may access the communication records of the parties involved." and Article 50 of the Inner Mongolia Autonomous Region Implementation Measures of the Road Traffic Safety Law of the People's Republic of China: "The traffic management department of the public security organs may access and copy the communication records and other information of the parties involved for the purpose of investigating traffic accidents." The issue of whether the above provisions are constitutional has sparked heated discussions in academia. During the special review in 2018, the relevant legislative departments considered that the above provisions violated the spirit of civil liberties stipulated in the Constitution, lacked legal basis and exceeded legislative authority, so the department revised the above provisions [5]. The legislation of subordinate laws violates constitutional principles, indicating that even under the premise of increasing legal reservations, legislation and administration have not fully protected citizens' freedom of communication and communication secrets.

After the arrival of the big data era, various

network platforms have experienced explosive growth in data, and the frequency of interaction between data communication entities is incalculable. The core of big data is prediction, which covers various aspects of people's lives such as behavior, hobbies, habits, health, etc. To achieve the goal of prediction, mathematical algorithms (examples) need to be loaded into massive amounts of data to predict the likelihood of events occurring [6], without massive data support, prediction cannot be achieved. In this context, how to protect the personal information security of citizens in big data communication is one of the challenges faced by disciplines such as social law, public management, and information technology.

The author believes that to discuss the protection of personal information in modern communication, three issues need to be explored: first, whether the right to personal information and privacy belong to the rights protected by the Constitution; Second, whether the basic guarantee conditions for communication in the new era of Internet have changed; The third is whether intentionally crawling or unintentionally obtaining data constitutes viewing of citizens' communication content and whether it constitutes infringement.

2. The Right to Personal Information and Privacy in the Constitution

The Criminal Law and the Civil Code respectively provide corresponding criminal and civil responsibilities for the protection of personal information. The Civil Code also stipulates that natural persons have the right to privacy, granting citizens legal rights to personal information and privacy from both public and private law. But the Constitution does not list the rights to personal information and privacy, adopting a basic rights approach that is not listed [7]. From the perspective of interpretive approaches, there are roughly three understandings in academia regarding the nature of communication secrets: privacy rights theory, mixed rights theory, and independent rights theory. Most scholars in Europe, Japan, and China agree with the theory of privacy rights. Although the provision on communication secrets in the Japanese Constitution is included in the freedom of expression clause, constitutional scholars represented by Nobuyuki Ashibe believe that there is an important difference between communication secrets and freedom of expression. This difference lies in the fact that the protection of privacy and expression can only be protected by the natural state, but is based on the fulfillment of obligations by communication industry practitioners. I also agree with this viewpoint, and in addition, I would like to express the following reasons.

Firstly, the object of freedom of expression is an unspecified object. In the network environment, virtual technology processes network user IP addresses, and information channels are established in virtual interactive spaces, making the object's non specificity more apparent. Therefore, the main manifestation of the right to freedom of communication expression is the expression of will. And the right to privacy is relative, contained in private behavior with a few specific objects, and there is a clear difference between the two. Secondly, from a social psychology perspective, unlike expressing intentions, privacy is associated with a person's self-esteem, and most people strive to maintain their self-esteem, while behaviors that violate privacy may lead to a state of low self-esteem. Salmela Aro and Nurmi's research found that people with low self-esteem often encounter various difficulties in their lives, while Donnellan's research found a weak correlation between low self-esteem and antisocial behavior [8]. There are also scholars in our country who hold similar views. If there are existing behaviors such as administrative agencies retrieving personal call records, and if similar behaviors have a universal impact on the self-esteem of unspecified natural persons, then the infringement of privacy rights by administrative power should be prevented. Therefore, the right to privacy should be protected by the constitution through administrative laws to defend against excessive use of administrative power. Professor Xiang Zhang believes that the constitutional obligation to protect personal information rights is a national obligation derived from the objective value order function of basic rights, which also includes the construction of systems, procedures, organizations, and other aspects, which means the coordination of different departmental legal mechanisms such as administrative law, civil law, and criminal law [9], I believe that this collaboration will also play a role in defending administrative power. Although the right to personal information is not directly expressed in

the Constitution, it is also included in the basic rights stipulated in the Constitution. The promulgation of the Personal Information Protection Law not only proves the synergy between the Constitution and departmental laws, but also suppresses the improper benefits and distribution caused by the demand for collecting personal communication data.

3. Basic Guarantee Conditions and Communication Rights for Modern Communication

Although traditional postal services still serve as universal communication services, the use of smartphones as hardware and software tools such as WeChat, QQ, micro-blog, and email have largely replaced traditional communication methods. This has led to profound changes in the basic conditions for safeguarding citizens' freedom of communication and the storage media for communication secrets. According to the International Telecommunication Union (ITU), the three major application scenarios of 5G are enhanced mobile broadband (eMBB), ultra high reliability low latency communication (uRLLC), and massive machine to object communication (mMTC). The core technology elements that support these application scenarios mainly include software, mobile terminals, mobile communication base stations and other infrastructure, wireless networks and their communication protocols, cloud servers (storage), and cloud computing. Mobile terminals and mobile communication base stations are the new conditions for achieving communication freedom, and mobile terminals and cloud servers are also carriers for storing personal information and communication secrets. The object of citizens' communication rights also changes accordingly. The constitutional guarantee of citizens' freedom and privacy of communication not only reflects the interaction and balance between individual rights and the development of the Internet industry, but also reflects the dilemma and breakthrough of basic rights in emerging fields [10]. On the one hand, the state guarantees the basic communication rights of citizens, and on the other hand, it engages in a game between public power and the basic rights of citizens. As mentioned earlier, taking the retrieval of call records by public security traffic management departments as an example, with the support of modern communication technology, it has become very easy to retrieve communication content from the network. Personal information and communication secrets have been transferred to social order under public power, and the boundaries of public power have been broken, while compressing the space for citizens' freedom of communication.

Network communication also brings the possibility of technical infringement, which poses a risk of infringement to the data stored on the network. This is reflected in the following four aspects: network attackers can exploit vulnerabilities in software or network components that can be accessed without authorization to make persistent or privileged access to the system or network; If 5G devices and infrastructure are damaged due to network layer attacks, attackers can access the 5G network without authorization, thereby intercepting, manipulating, and destroying critical data; The inherent vulnerabilities in 5G network infrastructure may be exploited by attackers, posing a threat to data security [11]. Therefore, the protection of communication rights under new technologies is not just a single issue of legal protection, but a comprehensive issue across multiple fields and disciplines, and cannot be generalized.

4. Infringement of Communication Secrets in the Context of Big Data

In order to understand the current judicial situation of communication freedom and communication secrets, the author searched for keywords such as "communication secrets", "communication freedom", "Article 40 of the Constitution", and "personal information of citizens", and obtained a total of 18098 judicial judgment documents, including 16938 criminal case documents, accounting for 93.6% of the total. The vast majority of cases involve parties committing the crime of infringing on citizens' personal information, and such criminals often also commit fraud at the same time. Victims often discover that their personal information has been violated due to fraud crimes. Through simple analysis, it is found that cases of infringing on citizens' personal information have the following three characteristics.

Firstly, it is difficult to discover, including the difficulty of the victim's own discovery and the difficulty of discovering through technical means. Taking the Tumu Yang fraud case, Guangfa Yuan, Ke Tang, Zilong Li and other

fraud cases, as well as the Cong Shi, Huachuan Wang and other fraud cases as examples, the victims discovered that they had fallen into the trap of online fraud at the time of the incident. However, in the subsequent investigation and trial, it was discovered and determined that the criminals illegally purchased a large amount of citizens' personal information for the purpose of committing fraud. The fundamental purpose of criminals is to seek improper benefits through fraud, and the act of purchasing citizens' personal information has become a condition for committing fraud. Compared to the owners of personal information, the collectors and processors of online personal information are in a dominant position, holding the value and processing ability of personal information, making it difficult for victims to know the fact that personal information has been leaked at first. In the context of modern technology, it is difficult to resist illegal activities for the right to personal information. Technical tools have emerged between the infringing behavior and the infringing object, and the typical technical means used by this tool are web crawlers. A web crawler refers to a program or script that automatically crawls network information according to certain rules. Of course, not all web crawling technologies are unfriendly. For search engines, they achieve efficient information acquisition and aggregation through web crawling technology, and the web pages being crawled are also promoted through search engine links [12]. However, the purpose of crawling citizens' personal information processors through web crawlers is not always legitimate. Web crawlers affect the protection of personal information data, and the act of crawling loses its resistance to illegality. Network service providers should not be aware of the communication content and personal information contained in it, but in reality, servers do have the function of storing personal information, which is not prohibited by current laws and provides usable space for web crawling technology.

Secondly, it is difficult to provide evidence. In the above-mentioned fraud cases, a large amount of personal information was sold, resulting in a tendency for personal information data to be monetized, making it valuable. This clearly violates the principles of "not collecting personal information without consent" and "not collecting if possible, and not processing if possible". It can be imagined that under this principle, the general owners of personal information will undoubtedly prohibit their personal information from being collected and used. However, the concealment of technical crawling is strong. In addition to being difficult to detect during the process, even if natural persons discover the fact that their personal information has been sold, it will be difficult to provide corresponding evidence due to a general lack of professional technical ability.

Thirdly, it is difficult to hold accountable. Daofa Wang believes that if the principle of fault liability is used for personal information processors, it is not conducive to the protection of personal information rights holders. Instead, the limitations in the scope of application and the special issues in the application requirements should be considered, and the principle of presumption of fault liability should be applied to personal information processors [13], this principle is particularly necessary in the protection of networked personal information. In addition to illegal crawling behavior, crawling tools are also a key element in proving evidence of personal information infringement. It cannot be ignored that web crawlers are highly likely to become tools for infringing personal information or communication secrets, and in previous cases, it has been rare for program providers to be held accountable. The author believes that one of the reasons for this situation is that under the framework of the principle of fault liability, it is difficult for personal information rights holders to collect illegal evidence, or evidence involving software programming is difficult to form an effective evidence chain due to its special technical nature.

5. Conclusions

Freedom and confidentiality of communication, as fundamental rights protected by the Constitution, are aimed at safeguarding the legal interests of citizens and maximizing the protection of public interests while also protecting individual interests. In the Internet environment, it is inevitable to consider the invasiveness of technological behavior in the network, and use multiple means to reduce the risk of protection failure of citizens' personal interests infringed by legislative lag. One of the participants in online activities is netizens. Although the concept of netizens is different from that of citizens, it cannot be ruled out that

netizens enjoy the basic constitutional rights that citizens should have. The interests of netizens in online activities still need to be properly protected. In summary, this article holds the following views.

5.1 Redefining the Infringement Subject of Freedom of Communication and Protection of Communication Secrets

The expression of the crime of concealing mail in China's Criminal Law is: "Postal workers who open, conceal, destroy or discard mail or telegrams without authorization shall be sentenced to fixed-term imprisonment of not more than two years or criminal detention." The subject of this crime is a special subject, including postal workers, including salespersons, issuers, sorters, deliverymen, receivers and couriers of the national postal industry management department, as well as agents and postal workers entrusted by the postal department; Objectively speaking, it refers to the act of privately opening, concealing, or destroying mail or telegrams. In reality, the subjects that may infringe on citizens' freedom of communication include Internet platform enterprises, network hardware developers, network software developers, and even individuals. These entities are engaged in sorting and delivering information online, and their core nature is also the transmission of citizens' personal information. Email, chat text and voice in network communication, including identifiable personal information such as work unit, activity location, facial features, name, phone number, home address, family information, property status, bank account number, password, etc. These information can be sent separately or combined with other information. Although these contents have different meanings from the confidentiality law, as long as these contents do not want to be known by others, they are personal secrets. The difference between online information and traditional email is that the latter solidifies the content at the time of delivery, while the former is sent through binary ASCII code transcoding. In other words, without the participation of online processors of personal information, personal information does not have direct readability and will not be leaked. Therefore, it is advisable to consider including the above-mentioned subjects in the scope of freedom of communication and infringement of communication secrets.

5.2 Strengthen the Coordination between Laws and Technical Regulations

The Constitution delegates the safeguarding of freedom of communication and the confidentiality of communications to common law, subject to legal reservations, while the protective role of common law necessitates harmonization and coordination through administrative regulations, departmental norms, local regulations, municipal by-laws, and normative documents and technical standards. Consequently, technical standards can be perceived as an extension of legal enforcement mechanisms. The Cybersecurity Law emphasizes the state's proactive engagement in cyberspace governance, network technology research and development, as well as standard setting. The author contends that the "standards" mentioned here ought to be encompassed within the ambit of technical regulations. Article 10 of the Standardization Law mandates the formulation of compulsory national standards for technical requirements that ensure the safety of human health, life, property, national security, and the ecological environment, while also catering to the fundamental needs of economic and social administration. Although this scope does not explicitly mention network security, it is undeniable that, in the digital era, protecting citizens' fundamental rights constitutes a basic necessity for economic and social management. Therefore, the establishment of mandatory standards in this domain aligns with the legislative intent of the Standardization Law.

However, mandatory standards possess notable limitations, including a narrow scope, fragmented formulation bodies, and a strong governmental steer. Notably, the proliferation of local mandatory standards may, to a certain extent, impede economic and social progress. According to the principle that "recommended standards referenced in laws and regulations must be implemented within the scope prescribed by those laws and regulations," recommended cybersecurity standards must be adopted through laws and regulations to acquire mandatory force. This underscores the importance of an effective coordination mechanism between laws, regulations, and technical standards to ensure that technical standards fulfill their legitimate functions.

References

[1] Jing'an Xiang, A Brief Introduction to Postal Communication in Ancient China. Wenbo. 1990 (06): P50.

[2] Yingmin Wang, Zhaohui Sun, Detailed Explanation of 5G Mobile Communication Network System Design and Standards. People's Posts and Telecommunications Press. 2020 (04): P18.

[3] Daoying Chen, The Nature, Scope, and Limitations of Communication Secrets in the Internet Age. Jinan Journal (Philosophy and Social Sciences Edition). July 2022 (282nd issue): P9-P10.

[4] Laifan Lin, Lectures on Constitutional Law (Third Edition). Tsinghua University Press. 2018: P337-P338.

[5] Xuanyi Zhao, Research on the Constitutional Protection of Citizens' Freedom of Communication in China. Liaoning University, 2022: P15.

[6] V. Mayer Sch Ö nberger, Kenneth Cukier, Big Data Era. Zhejiang People's Publishing House. 2013: P16.

[7] Zhongxia Li, Constitutional Construction of Privacy Rights in the Digital Age. Journal of East China University of Political Science and Law. 2021 (3): P45-P46.

[8] D. Myers, Social Psychology. People's Posts and Telecommunications Press, 2016: P52-P53.

[9] Xiang Zhang, Constitutional (Academic) Evidence of Personal Information Rights - Reflection on the Differentiation between Protection Theory and Dominance Theory. Global Legal Review, 2022 (1): P67.

[10] Yinan Shuai, Constitutional Guarantee of the "New Form" of Basic Rights -- Taking Citizens' Right to Freedom of Communication in the Internet Era as an Example. Legal Review. 2018 (6), (212 in total): P121.

[11] Lingbo Sun, Discussion on the Development Trends and Innovative Progress of 5G Network Security. Network Security Technology and Applications. 2022(9): P81.

[12] Xiaodong Ding, Who Exactly Does the Data Belong to: Viewing Platform Data Ownership and Data Protection from Web Crawlers. Journal of East China University of Political Science and Law. 2019(5): P71.

[13] Daofa Wang, Research on the Presumptive Liability of Personal Information Processor's Fault. Chinese Law. 2022 (5): P19.

