Problems of Crimes of Infringing Citizens’ Personal Information and Suggestions for Improvement

Haoran Fu1, a, *, Jie Li1, b

1 School of Economics, Anyang Normal University, Anyang, China.
a hao3681@foxmail.com, b 584576227@qq.com

Abstract

The crime of infringing on citizens’ personal information refers to the criminal act that the perpetrator violates the state’s legal norms on the protection of personal privacy and obtains citizens’ personal privacy information by using illegal means such as stealing, swindling and stealing, causing serious consequences. On the basis of defining the concept and characteristics of the crime of infringing on citizens’ personal information, this paper puts forward relevant improvement measures in view of the practical problems arising from the crime of personal information in judicial practice.

Keywords

Personal information, Fines, Subject identity, Illegal use.

1. Introduction

With the rapid development of our society, especially the rapid development of information technology, we are shopping on the Internet and using mobile payment more and more times, but these platforms all need our personal information. Because we are all in a big data era, the government and businesses will become more and more convenient with our personal information processing decisions. However, if these information data are collected in large quantities and are not well protected, personal information will be leaked and personal information security problems will occur. In our life, due to the lack of effective regulations on the collection and storage of personal information, personal information of our citizens is seriously leaked. Personal information not only has identity significance, but also can generate huge economic benefits and has wide application in many fields. Personal information also contains a large amount of property information, which criminals often use to carry out telecommunication fraud after obtaining. As early as 2016, there have been many serious cases of precision telecom fraud. The recent case of Xu Yuyu telecom fraud by Shandong prospective college students is a follow-up fraud because criminals have mastered the leaked personal information of citizens in advance. Therefore, the situation brought by personal information disclosure is getting more and more serious, and more infringement cases related to it are also increasing. These new crimes not only violate citizens’ personal rights and property rights, but also are not conducive to social stability and security. In order to reduce the occurrence of accurate telecommunication fraud and other crimes from the source, criminal legal norms should play a preventive role in criminal law, regulate the protection of citizens’ personal information, and reduce the occurrence of derivative crimes. [1]
2. Determination of Crime of Infringement on Citizens' Personal Information

2.1. Crimes of Violating Citizens' Personal Information

The crime of infringing on citizens' personal information refers to the act of providing citizens' personal information to others, or selling citizens' personal information, and stealing or illegally obtaining citizens' personal information by other methods in violation of the relevant provisions of the state, if the circumstances are serious.

The criminal object of this crime is the personal information generated by the unspecified subject of social citizens in social relations. At present, the current criminal code of our country regulates the personal information of citizens mainly in articles 252 and 253. On the objective side, the perpetrator violated the state's laws and regulations on the protection of citizens' personal information, indicating the criminal illegality of the act. The criminal acts acting on citizens' personal information resulted in the disclosure of personal privacy information and were controlled by other perpetrators to carry out derivative criminal acts, resulting in certain criminal influence and social harmfulness. The result of this act is directly related to the perpetrator's violation of citizens' personal information. Accordingly, it has the characteristics of criminal law that should be punished. The subject of this crime refers to natural persons and units with criminal responsibility. The subjective aspect of this crime refers to the fact that the perpetrator intentionally sells or provides personal information of unspecified subjects. At the same time, Article 253 of the Criminal Law specifies the behavior of postal department staff to open, conceal, destroy and discard mails and telegrams without the consent of the other party. This also indicates that the subjective mentality of this crime can only be intentional.

2.2. The Connotation of Personal Information

At present, China's laws and regulations on the protection of citizens' personal information are scattered in the criminal law and the cyber security law, and there is no unified law to protect citizens' personal information. Therefore, in judicial practice, judges can only rely on the "cyber security law" and the "interpretation" issued by the two high schools, combined with the general evaluation standards in the society to identify, thus causing confusion in the identification of citizens' personal information. This has also created some loopholes that will be exploited by criminals. There are also three theories in the existing theoretical circle, namely "relevance theory", "privacy theory" and "identification theory".

First, the "relevance theory" covers the widest range of all theories. It is the personal information generated by individual citizens in the cooperation of social relations, which can clearly identify individuals and accurately locate the important information of individual citizens' social roles according to a single information. Second, the "identification theory" refers to the information embodiment that an unspecified social subject accurately identifies a specific citizen according to the presented personal information of citizens in the operation of social relations. This information is generally collected and presented by public authorities in a unified way. Third, the "privacy theory" privacy theory starts from the individual's right to privacy in the civil law. Only the information reflecting the individual's right to privacy belongs to the citizen's personal information, but this theory has great limitations. In judicial practice, various kinds of statements have been adopted by courts, but different standards will affect the identification of an act as a crime or a non-crime, thus failing to crack down on crime and protect human rights. Only a reasonable definition of the scope can fit the expectation of the people and the modesty of the criminal law. Judging from the combination of judicial practice and theory, the standard adopted in our country is "identity identification". I prefer to adopt the effective association theory, which is only applicable to identification theory or privacy theory. It only
focuses on some characteristics of personal information, while the only use of association theory will result in too wide a scope.

How to grasp and define the concept of "citizen's personal information" is a very important thing to protect citizen's personal information. Although the current criminal code of our country regulates the crime of infringing on citizens' personal information, there is no unified definition of the characteristics of citizens' personal information. However, China's "Cyber Security Law" and the "Several Interpretations on the Applicable Laws in Handling Criminal Cases of Infringement on Citizens' Personal Information" issued by the National People's Congress and the National People's Congress are of great help in defining the concept and scope of citizens' personal information.

2.3. The Difference Between Personal Information Right and Related Concepts

Although there are overlaps between personal privacy and personal information, there are many differences. First of all, in the scope of adjustment, personal privacy has no specific bearing object. At the same time, subject to the adjustment of civil laws and regulations, personal privacy has subjective characteristics of individual perception. Because personal information has specific bearing object and has certain objective physical attributes, it can be influenced by criminals. Secondly, there are differences in the content of rights. The right to privacy is an absolute right, which refers to the obligation of state units, social organizations and individuals not to spy on or disseminate personal private information. The right of the person who has the right to privacy is embodied in the right to legal remedy when his privacy is violated. The right to personal information has more power and can make better use of one's rights. Finally, there are differences in the subject of obligation. The obligation subject of the right to personal information points to the possessor of personal information. Only units specially engaged in collection, processing, dissemination and personal information are obligated to properly keep personal information. The subject of obligation for privacy right is the general social organizations and individuals, and there is no special limit, that is to say, anyone can become the subject of invasion of personal privacy. There are differences in conditions. Privacy right belongs to a subordinate branch of personality right. It is a right born to a natural person, and the generation of personal information right is valuable personal information.

Different from online privacy, online privacy is a natural extension of the traditional concept of privacy in the network environment. Although it is still within the scope of privacy in essence, it is similar to personal information due to its wide coverage, fast transmission speed, uniqueness of protection difficulties and its attachment to open, circulating and global network communication. However, the difference lies in that the generation of online privacy is mainly based on specific conditions. In the information age and the Internet age, online privacy is transformed from ordinary privacy. Therefore, personal information has a relatively broad form of expression.

3. Provisions on Personal Information Protection at Home and Abroad

3.1. Foreign Countries' Criminal Legislation on Personal Information Protection

Through consulting the regulations of foreign countries on criminal protection of personal information, nearly 20 countries have formulated unified legal norms for the protection of personal information of citizens. However, due to the different legal traditions and manifestations of each country, the normative adjustment of personal information of citizens also presents different legal relationships. [2]
The industrialization process in Britain and the United States was earlier than that in our country. Combined with religious theories with individualism as the core, there was a relatively perfect system for protecting the right to privacy. At present, the UK's regulations on personal information protection are mainly completed by the Data Protection Law, which accurately defines the types, presentation methods and specific provisions of citizens' personal information, providing a strong reference for the judiciary to accurately determine crimes against citizens. At the same time, the UK Criminal Law also provides criminal law protection for infringement of citizens' personal information. [3] For example, Article 5 of the Criminal Law prohibits the crime of possessing private information without registration permission. Britain is also a typical Anglo-American legal system country. In the protection of citizens' personal information, it has also continuously improved the current legal norms through the "judge-made law" to fill in the legal loopholes and issued a series of typical cases of infringement of citizens' personal information, providing practical reference for judges when applying such cases. Therefore, the British law on the protection of citizens' personal information presents the characteristics of "legislative guidance and case supplement".

The protection of personal information in the United States is mainly reflected in the expression of personal information as a kind of personality right and the enactment of the "Privacy Law" with criminal penalties. [4] Similarly, the United States also has a unified legal and normative form to regulate crimes against personal information. The protection of citizens' personal information is defined as the right to privacy, and the relief methods adopted are mostly remedial compensation measures afterwards. [5] For example, in the criminal punishment of the Privacy Law, it is clear that the individual's violation of other people's personal information is punishable by a fine of 5,000 US dollars in addition to minor crimes. Therefore, the protection of personal information is based on the relief mode of private social law. The definition of personality right crime is relatively vague. The United States has given full play to the discretion of judges in the application of individual cases, and has also created a large number of judicial precedents for judges' reference. Therefore, the United States' standard mode of personal information of citizens presents the legislative characteristics of "private law leading and public law covering the bottom".

The crimes against personal information regulated in Germany are mainly reflected in chapters 7 and 15 of the German Criminal Code. The main regulated targets are citizens' personal information and communication secrets. Germany has established a relatively complete legal punishment system, expanding the criminal object of personal information protection to the personal information carried by electronic data, increasing the object of criminal law adjustment, and stipulating a dual-track criminal law system of personal punishment and property punishment. Specifically, it can be expressed in Article 202 as follows: "Whoever illegally inquires for himself or others about data that do not belong to himself and that are specially protected shall be sentenced to imprisonment of not more than three years and a fine."

3.2. China's Current Laws and Regulations

Unlike most countries in the world, China has not yet enacted a special personal information protection law. Although there are many existing legal norms, they are scattered and not perfect. Early protection of personal dignity, personal privacy and related information security content cannot achieve the effect of comprehensive protection. However, in recent years, legislation has also concentrated on regulating the content of "personal information". First of all, the "Decision of the Standing Committee of the National People's Congress on Strengthening the Protection of Network Information" promulgated in 2012 is the only single law for personal information protection in China up to now, but only 12 articles are far from achieving full protection of personal information. Also, the Public Security Administration Punishment Law is only a punishment for sending spam messages. The promulgation of the "Cyber Security Law" shows
that the legislature and the power organs attach importance to this issue, although the relevant acts have been included in the legal regulation in the "Criminal Law Amendment (7)". In addition, the two high schools in 2017 issued relevant judicial interpretations. The first paragraph of Article 5 of the Interpretation clearly stipulates four kinds of "especially serious" circumstances, including personal injury, property damage, information damage and social damage.

The current legal norms only regulate and adjust the afterwards criminal acts that infringe upon citizens' personal information, but they do not accurately define the objects and objects of citizens' personal information infringement. The application of legal provisions cannot be separated from judicial interpretation. From the repeated revisions, the addition of relevant judicial interpretations of crimes against citizens' personal information and the amendment of the Criminal Law, we can see that the state has also attached more and more importance to the protection of citizens' personal information. Although the trend of centralized protection of personal information is becoming more and more obvious, there are still some jumbles at this stage, which have caused some obstacles to judicial practice.

3.3. Extraterritorial Reference to Violation of Citizens' Personal Information Norms

Although foreign citizens' personal information protection is advanced in legislation and transplantable, legal transplantation is an important tool to construct and perfect a country’s legal system. Legal transplantation is not completely copied. We should pay attention to the system agreement with the domestic legal value and perfect the localization of legal concepts. Proceed from the national conditions, take into account the actual differences in personal information protection, pay attention to the social tolerance and acceptability, and reduce the resistance of localization after legal transplantation. Based on the actual situation of our country, to solve our country’s practical problems and meet our country’s existing legal system as the purpose, to make a choice between the comparison, and finally form the best scheme conducive to the protection of our citizens' personal information. To avoid "borrowing doctrine" can also effectively make up for the defects and deficiencies of the current methods. Specifically, the criminal law protection of extraterritorial personal information has a lot to learn from: formally speaking, a special personal information protection law can be formulated. Although our country also has some related regulations at present, the regulations scattered in various departments still have some problems on the whole. For example, the scope of applicable subjects is limited, including only natural persons and units, or the coordination between laws is too poor and the implementation effect is not ideal. In terms of content, the relevant provisions of our country's crime of infringing on citizens' personal information also need to be improved. For example, "citizens' personal information" as the core of this crime needs to be further clarified.

4. Deficiencies in Laws Governing Violations of Citizens' Personal Information

4.1. The Concept of Personal Information Is Not Unified

"Citizen's Personal Information" is the target of this crime and should also be an important concept in the criminal law system. However, China's criminal law does not specifically define "personal information of citizens" and relies more on the discretion of front-line judicial personnel. Accurate definition of personal information is the premise for accurate conviction and sentencing of infringement of citizens' personal information; China's "cyber security law" stipulates that "personal information refers to all kinds of information recorded electronically or in other ways that can identify the personal identity of a natural person alone or in
combination with other information, including but not limited to the name, date of birth, identification number, personal biometric information, address, telephone number, etc. of a natural person", and adopts the traditional thinking of EU law. However, the problem in judicial practice is that this kind of definition is only defined by way of enumeration and does not exhaust the personal information generated by individuals in social relations. Because the personal information embodied in this regulation is the sign information of individuals and has the characteristics of popularization, the types of information generated by individuals in the cooperation of social relations are uncertain, and the personal information has the characteristics of extension in the expansion of social relations, thus there will be judicial problems of omission evaluation of personal information protection in strict accordance with the provisions of this law. From the legislative purpose of criminal law protection of personal information outside the territory, the balance between information protection and information sharing should be achieved. The vague definition of personal information not only hinders the protection of citizens’ privacy and legitimate rights and interests, but also severely restricts the development of data circulation and industrial innovation. Therefore, the accurate definition of the concept of "personal information" is the basis for the criminal law to play its preventive and striking role. [6]

4.2. The Standard for the Amount of Fines Is Vague

The severity of the penalty tends to lead to an unbalanced state of information protection and information sharing. The applicable standard of the fine can be clearly defined. The actor generally has the mentality of pursuing interests. The fine, a measure in property penalty, has stronger pertinence. The legal interests of citizens’ personal information guaranteed by the criminal law of our country are multiple. The legal interests involved involve all aspects of the existence and development of individuals. However, the legal punishment of additional penalty is adopted in setting the amount of fine. Moreover, in judicial practice, judicial personnel have greater discretion, and generally do not impose a large fine to compensate the victim for the loss. Such criminal law setting will cause sentencing imbalance and reduce the illegal cost of such criminal acts.

4.3. Objective Behavior Is Not Perfect Enough

In today's society, the disclosure of personal information has brought us some troubles to a certain extent and is becoming more and more rampant. Some people's behaviors are not subjective and malignant. According to the provisions in the "Criminal Law Amendment (IX)", this problem has been found. The definition of legal concept is vague. In view of the lack of legislation on harmful acts, simple and easily available information such as name and age should not be recognized as a crime. Is the regulation of "illegal use" too vague and the legal concept is not rigorous enough, is it determined according to the number of times or the consequences of the act? In reality, there is fraudulent use of other people’s identities, which is also illegal use of personal information, but our legislation is a blank state here. If these cannot have an accurate standard, it will cause great difficulties to the operability in judicial practice, and it is impossible to judge whether a crime or not. There is a certain practical urgency, which is also the result we do not want to see.

4.4. There Is No Provision for Negligent Crime of Infringing on Citizens’ Personal Information

At present, China’s criminal law only requires intentional subjective mentality to infringe upon citizens’ personal information, but in reality. The subjective state of the actor is not accurately defined, which is a defect in our protection of personal information. The act of negligently disclosing citizens’ personal information, although not in violation of laws and regulations, still violates citizens' right to personal information. Before the big data era, personal information
may not be as important as the right to health, but with the progress of society and technology, the right to personal information will become a new legal benefit.

From the theoretical level, there are many negligent crimes that adopt the principle of exceptional punishment when they are punished, which refers to the "negligent crime, which is subject to criminal responsibility only if the law has provisions" in the second paragraph of Article 15 of the Criminal Law. If other subjects hold personal information, then the holder has the obligation to protect the personal information. Those who can do this have a certain capacity of behavior and are able to realize the harmfulness brought about by the disclosure of personal information. Therefore, when they should have realized the harmfulness but did not avoid it, they have committed the crime of negligent infringement of citizens' personal information. For example, some enterprises will throw away the resumes of non-employed job seekers after the job fair is held. The contents of personal information contained in these resumes are very specific. If obtained by illegal elements, it will cause unpredictable harm. Moreover, the legislation has a certain lag, which is why some amendments are made every year. The reason for judicial interpretation is that new criminal acts have already appeared and the corresponding laws will only be issued. Therefore, there are still a lot of deficiencies in the provisions on this crime in the judicial practice stage, including judicial personnel who do not have clear reference standards when dealing with related issues.

5. Measures to Improve Crimes of Infringement on Citizens' Personal Information

5.1. Accurately Define the Scope of "Personal Information"

When perfecting legislation, it is necessary to issue guiding cases and judicial interpretations to clearly define "personal information". The key is whether it is used for the purpose of identifying specific individuals and whether it will bring unreasonable privacy risks to the parties concerned. Standards related to citizens' important personal and property should be adopted. In addition, considering the stability and conciseness of the criminal law provisions, I think the existing definitions can be integrated, and in international legislation and practice, most people prefer dynamic risks in scenes to static information types. We can define "citizen's personal information" by listing and summarizing.

With the progress of science and technology, our personal biological information can also be classified as our personal information to some extent. Now, there are stations that can enter the station through "face scanning" identification instead of the traditional identification through ID cards, and some applications on smart phones can unlock or complete other operations using input fingerprints. This is the use of our biological information, but there are no regulations in this regard. Personal biological information usually includes our fingerprints, facial features, genes and other information, and I think these also belong to the category of personal information. This system with fingerprints as its core is the only identification of natural persons. Even if other information can be counterfeited, personal biological information cannot be counterfeited. Moreover, unlike other types of information that can be stored in electronic or other media, such information will accompany us all our lives, even before we are born. Moreover, the identification rate of this information can be said to be 100%, and there is still a big feature that it cannot be changed, just as the police sometimes determine the suspects through fingerprints left over from the scene. These characteristics have inspired me that the utilization value of this information is higher than that of conventional personal information. However, the protection of this aspect is still in a blank state. If the protection of personal biological information can be added to the legislation, the protection of personal information can be realized in a longer term.
5.2. **Perfect Fine Penalty**

Personal information is a kind of intangible property, which makes the judgment of fine penalty lack of reference, the vague property attribute of personal information, coupled with the fact that there is no explicit provision in our country to calculate the property loss in the crime of violating citizens’ personal information. [7] before there was no specific limit of the fine system, coupled with the application standards are not uniform, the judicial practice process will be very difficult, according to these, can through legislation this way to determine the amount of fine range. In the process of legislation, we can learn from the foreign limited fine system. For example, Article 134 of Japan’s Criminal Code stipulates that "whoever commits this crime shall be punished with imprisonment for not more than six months or a fine of not more than 100,000 yuan". The use of legal or judicial interpretation to make a clear range of the amount, within this range, let the court combined with the specific circumstances of the case, make a discretion, and can better promote the judicial application.

5.3. **To Regulate "Illegal Use" Behavior**

In the "Interpretation" issued by the two high schools, illegal collection behavior is interpreted as "illegal acquisition by other methods", which is a kind of illegal acquisition behavior and lacks the norms of illegal utilization behavior. The implementation of the criminal law requires specific preconditions. Based on this, the "illegal use" is added to the objective behavior of the crime of violating citizens’ personal information in our country to better combine with the upstream behaviors of "selling, providing, illegally obtaining and stealing" to form a complete protection system. When making a specific ruling, "illegal use" is taken as a plot of the judgment. when the criminal law does not stipulate specific acts, it should be judged whether it is related to the person, property and other legal interests of the information subject. if it is within the scope of "individual citizen" stipulated by law, such illegal use of personal information of citizens can be added to the regulation of this crime. Of course, regulations must be made within a reasonable scope. With the advent of today’s information age, it is inevitable that there are certain contradictions with the rational and legal use of personal information, which makes it all the more necessary to clearly define how to use personal information.

5.4. **Provisions on Increasing Negligent Disclosure**

At present, there are many types of jobs that can access our personal information, and some of them are state workers. They are hard to avoid negligence in their work. As long as they appear, a large amount of personal information will be leaked. Our country can carry out appropriate legal transplantation. France will define the negligent infringement of personal information by the information archiving department as a crime, and our country can introduce subjective negligence into the official acts involving citizens’ personal information. Therefore, the negligent crime of postal department staff can be added to article 253 of the criminal code, including individuals and units, which is also a subject that cannot be ignored. in the legislation, it can be manifested as increasing unit negligence and causing personal information leakage and serious consequences. This is also the requirement that the criminal law should finally adapt to the social reality. In addition, by adding these regulations, it can play a guiding role and realize prevention in advance and punishment afterwards. It can urge the holder to exercise power reasonably and legally within the framework of the system.

6. **Summary**

Criminal law is the most severe intervention on citizens’ personal freedom and property rights. Its formulation and revision are lagging behind to some extent. It is a means of attack afterwards, but it can also play an indicative role and give us a warning. In order to perfect the legislation process, it is necessary to grasp the contradiction between the protection of personal
information and the sharing and utilization of social information. In this process, it is necessary to combine with the actual situation in our country, and some advanced experiences of foreign countries on the criminal law protection of personal information can be appropriately used for reference. With the continuous upgrading of information protection technology, there is still a long way to go to perfect the criminal law. This article only puts forward some opinions on the principle of legally prescribed punishment for a specified crime in the criminal law. It is suggested to increase illegal use of citizens' personal information and negligent crimes committed by units when improving legislation, hoping that they can fulfill their confidentiality obligations. With the challenges of new communication methods such as the Internet, strengthening the protection of personal information is now the consensus of most countries and people and has reached a very urgent point. As a representative of national and public interests, our government should take positive actions. The establishment of China's personal information protection system needs to fully protect the personal rights of information subjects and realize the legitimate use of information by information controllers on the basis of free values, and to establish a multi-element personal information rights protection system that is combined with the current legal value of China's society and the development laws of the future digital economy, so as to help realize the national industrial upgrading and the strategic power of the network.

References


