

Уголовно-правовая защита персональных данных граждан в сфере больших данных Criminal Law Protection of Citizens' Personal Information in the Big Data

Фу Сян Сян,
исследователь Института борьбы с преступностью
и уголовной политики
Хэнаньского университета,
г. Кайфэн, Китай
e-mail: fxyfxx@henu.edu.cn

Ван Гуанлун,
аспирант кафедры информационного права
и цифровых технологий,
Московский государственный юридический университет имени О.Е. Кутафина (МГЮА),
г. Москва, Россия
e-mail: guanglong95@163.com

Fu Xiang Xiang
Researcher,
Institute for Combating Crime and Criminal Policy,
Henan University,
Kaifeng, China
e-mail: fxyfxx@henu.edu.cn

Wang Guanglong,
Ph. D. Student, Department of Information Law
and Digital Technologies,
Institute of Postgraduate and Doctoral Studies,
Kutafin Moscow State Law University (MSAL)
Moscow, Russia
e-mail: guanglong95@163.com

© Фу Сян Сян, Ван Гуанлун, 2024

DOI: 10.17803/2587-9723.2024.7.131-142

Аннотация. В эпоху больших данных технологии обработки данных влияют на китайское общество, и сбор и анализ информации больше не являются случайным и непредсказуемым процессом. Персональные цифровые данные граждан представляют огромный интерес. Следовательно, необходимо рассмотреть взаимосвязь между социальным развитием на фоне больших данных и борьбой с преступлениями, связанными с использованием личной информации граждан. Путем анализа существующих в Китае норм уголовного права, касающихся личной информации граждан, и основываясь на трех аспектах концепции уголовного права, уголовно-правового законодательства и уголовного правосудия, авторы исследуют наказание и ответственность за нарушение прав на личную информацию граждан в Китае.

Исходя из модели двойной оценки качественных и количественных преступлений в Китае, кража личной информации граждан рассматривается как преступление при определенных обстоятельствах, и связанные с этим элементы обстоятельств непосредственно определяют вынесение приговора преступнику. Отсутствие толкования в китайских судебных документах и неполное установление обстоятельств приводят к расхождению результатов рассмотрения дел, что влечет вынесение уголовным судом различных судебных решений по одному и тому же делу.

Для всестороннего определения уголовно наказуемых обстоятельств посяательства на личную информацию граждан принята стратегия сосредоточения внимания на количественных

стандартах, дополненная неколичественными стандартами, чтобы обеспечить всестороннее определение и точную классификацию случаев и подчеркнуть ценность уголовного права.

Ключевые слова: большие данные; персональная информация гражданина; уголовное право

Abstract. In the Big Data, Chinese society is affected by data technology, and the collection and analysis of information is no longer a random and unpredictable process. Digital citizens' personal information contains huge interests. Therefore, it is necessary to deal with the relationship between social development under the background of Big Data and cracking down on citizens' personal information crimes. By sorting out the existing Chinese criminal law norms of citizens' personal information, and based on the three perspectives of criminal law concept, criminal law legislation and criminal justice, this paper analyzes the punishment and responsibility of infringing citizens' personal information in China. Finally, based on the dual evaluation model of qualitative and quantitative crime in China, the infringing of citizens' personal information is regarded as a circumstance crime, and the involved elements of circumstances directly determine the sentencing of the perpetrator. The lack of interpretation in Chinese judicial documents and the incomplete determination of circumstances lead to the discrepancy of case results, resulting in the criminal justice punishment of different judgments in the same case. For the comprehensive determination of the criminal circumstances of infringing on citizens' personal information, the strategy of focusing on quantitative standards and supplemented by non-quantitative standards is adopted to realize the comprehensive determination and accurate classification of cases and highlight the value of criminal law.

Keywords: Big Data; Citizen's personal information; Criminal law

Introduction

The concept of Big Data was first proposed by Viktor Mayer-Schönberger. Big Data refers to the technology with prediction function by acquiring all data without using random sample collection and analysis.¹ IBM (2016) describes Big Data as having the 5V characteristics of Volume, Velocity, Variety, Value and Veracity. Big Data makes citizens' personal information to be transmitted in cyberspace, and personal information thus uploaded to into the "cloud".

Citizens' personal information generally refers to all information about citizens' personal activities, including the citizens' identity information, property information, act information, etc. The citizens' personal information protected by criminal law should be a concept in the legal context with the attribute of legal interest, which is different from the citizens' personal information under the general semantics. It is a legal right or realistic urgency that needs to be protected by criminal law.²

Only those acts that are truly necessary to be prohibited can be defined as crimes in the criminal law and punished with criminal penalties.³ The protection of citizens' personal information in China is mainly to criminalize the acts infringing on citizens' personal information in the criminal code, so as to protect citizens' personal information rights, punish

crimes and maintain social order. Big Data is coming, and it is necessary for us to think about the protection of citizens' personal information at the criminal level. The importance of criminal law protection of citizens' personal information is self-evident.

I. Evolution of criminal law protection of China on citizens' personal information in Big Data

In recent years, the progress of Chinese network information technology has made the Big Data ecosystem increasingly mature. Meanwhile, crimes on citizens' personal information occur from time to time, which seriously threat citizens' personal and property security. The effective protection of citizens' personal information is not only related to the realization of the rights of social members, but also related to the strategic security of national data and the steady progress of social order. Therefore, Chinese criminal law continues to explore the effective protection of citizens' personal information and investigate the criminal responsibility for such criminal acts, which reflects the concern of the criminal law for the people's livelihood and society.

In 2009, Chinese criminal law legislation paid attention to citizens' personal information for the first time. Article 7 of the Criminal Law Amendment

¹ Viktor Mayer-Schönberger, Kenneth Cukier. 2013. Big Data: A Revolution That Will Transform How We Live, Work, and Think. 1st ed. London : John Murray. P. 9.

² Huang Zushuai. The Research of Criminal Law Legislation of Personal Information in China. Journal of Capital Normal University [Social sciences edition]. 2015 [05]. P. 65.

³ Chen Xingliang. Philosophy of criminal law. 1st ed. Beijing : China University of political science and Law Press, 2004. P. 6.

(VII) of the P.R.C. is inserted after Article 253 of the Criminal Law as Article 253-1. This article has become the core provision for the protection of Chinese citizens' personal information. There are three paragraphs in this article. The first paragraph⁴ is the charge of "selling or illegally providing citizens' personal information", the second paragraph⁵ is the charge of "illegally obtaining citizens' personal information", and the third paragraph⁶ stipulates the punishment provisions for unit crimes. Considering that Chinese basic laws on personal information protection and other relevant laws are not yet complete, the legislature has set a relatively light legal punishment in the Amendment(VII) to the Criminal Law of the P.R.C. , with a maximum of three years' imprisonment. Moreover, the criminal act of selling or illegally providing citizens' personal information has the preconditions of "special subject of crime" and "violation of national regulations".

In 2015, Chinese crime showed new characteristics. A large number of criminal acts were carried out through the medium of computers, and crimes are becoming cyberization. Aiming at the hot issues in social transformation, the Criminal Law Amendment (IX) of the P.R.C. further strengthens the protection of citizens' personal information. Citizens' personal information returns to the perspective of criminal law protection again. The "selling or illegally providing citizens' personal information" in the first paragraph of article 253-1 of the Chinese criminal law is revised to expand the scope of the criminal subject, change the special subject into a general subject, and remove the illegality requirement for the act of providing, as long as it is in violation of national regulations, sell or provide citizens' personal information to others, all constitute this crime.

If the perpetrator commits the crime in the process of performing duties or providing services, it shall be referred to as the second paragraph of the provisions as a condition for heavier punishment of the crime. After the original second paragraph "illegally obtaining citizens' personal information" was changed to the third paragraph, the number of paragraphs in article 253-1 of the Chinese criminal law was increased from three to four. In terms of statutory punishment, for those whose circumstances are particularly serious, sentencing

three to seven years and imposing a fine. The heavier punishment stipulated in the revised second paragraph shall also apply to the acts of stealing and illegally obtaining citizens' personal information in the third paragraph.

According to article 253-1 of current criminal Law, the charge of selling or illegally providing citizens' personal information and the charge of illegally obtaining citizens' personal information have been abolished, and it is uniformly called the charge of infringing citizens' personal information.

The first paragraph of article 253-1 stipulates: "Whoever sells or provides any citizen's personal information in violation of the relevant provisions of the state shall, if the circumstances are serious, be sentenced to imprisonment of not more than three years or criminal detention in addition to a fine or be sentenced to a fine only; or be sentenced to imprisonment of not less than three years but not more than seven years in addition to a fine if the circumstances are especially serious."

The second paragraph of article 253-1 stipulates: "Whoever sells or provides to any other person any citizen's personal information obtained in the course of performing functions or providing services in violation of any relevant provisions of the state shall be given a heavier penalty in accordance with the provisions of the preceding paragraph."

The third paragraph of article 253-1 stipulates: "Whoever illegally obtains any citizen's personal information by stealing or other methods shall be punished in accordance with the provisions of paragraph 1."

The fourth paragraph of article 253-1 stipulates: "Where an entity commits any crime as provided for in the preceding three paragraphs, the entity shall be sentenced to a fine, and its directly responsible person in charge and other directly liable persons shall be punished according to the provisions of the applicable paragraph."

In addition, legal interpretation can make up for the possible limitations of legislation and guide judicial practice. In 2011 & 2017, the Supreme People's court of China and the Supreme People's Procuratorate of China jointly issued the interpretation on Several Issues concerning the application of law in handling criminal

⁴ The first paragraph of article 253-1 stipulates: "Where any staff member of a state organ or an entity in such a field as finance, telecommunications, transportation, education or medical treatment, in violation of the state provisions, sells or illegally provides personal information on citizens, which is obtained during the organ's or entity's performance of duties or provision of services, to others shall, if the circumstances are serious, be sentenced to fixed-term imprisonment not more than three years or criminal detention, and/or be fined."

⁵ The second paragraph of article 253-1 stipulates: "Whoever illegally obtains the aforesaid information by stealing or any other means shall, if the circumstances are serious, be punished under the preceding paragraph."

⁶ The third paragraph of article 253-1 stipulates: "Where any entity commits either of the crimes as described in the preceding two paragraphs, it shall be fined, and the direct liable person in charge and other directly liable persons shall be punished under the applicable paragraph."

cases endangering the security of computer information systems⁷ (hereinafter referred to as the interpretation on handling computer criminal cases) and the interpretation on Several Issues concerning the application of law in handling criminal cases infringing on citizens' personal information⁸ (hereinafter referred to as the Interpretation on handling criminal cases of citizens' personal information) two Judicial Interpretations related to the protection of citizens' personal information.

The interpretation on handling computer criminal cases defines the identifying information from the perspective of property, and its protection mainly focuses on citizens' personal identity information in online financial services. The Interpretation on handling criminal cases of citizens' personal information expands the connotation of the protection of citizens' personal information and makes up for the insufficient protection of citizens' personal information in the criminal law. At the beginning of the Interpretation on handling criminal cases of citizens' personal information, it gives an enumerated definition of citizens' personal information, which details the concept of citizens' personal information for practical operation to a certain extent. In 2017, The interpretation of handling criminal cases of citizens' personal information has also achieved legal connection with other laws, but there are still some problems in the criminal protection of citizens' personal information.

II. Analysis on criminal law protection of Chinese citizens' personal information in Big Data environment

Everything has two sides. Big Data technology has brought immeasurable benefits to the management and services of the whole society, but there are also many risks in the application of citizens' personal data information in the Big Data era. Chinese "3.15

show"⁹ in 2021 exposed a series of problems involving citizens' personal information, for instance, the Online recruitment agency sold the resumes of job seekers to the black market,¹⁰ Malicious software Illegally obtained stored information in the mobile phone of the elderly.¹¹ The personal rights and interests of citizens are infringed, the property rights and interests are lost, and the current situation of "streaking" of citizens' personal information reflects the insufficient protection of China's criminal law.

A. The concept of criminal law has different understanding of personal information

As an important principle of criminal law, the legal interest protection shows that the core of criminal law is to protect the interests recognized by criminal law. "If the purpose of the criminal law is not to protect legal interests, then the charge is illegal or unconstitutional."¹² Due to the substantive intersection between the legal interests of citizens' personal information and the right content of relevant legal interests, the attribute boundary of legal interests is blurred, so there are different understandings, If other related legal interests cover the legal interests of citizens' personal information, the vague subjective understanding is not conducive to the development of criminal law. Based on this, the first is to clarify the boundaries, which mainly involves citizens' personal information, citizens' personal data and citizens' personal privacy.

As for the distinction between citizens' personal information and citizens' personal data, some scholars (Yu Chong, 2018) pointed out that "personal information can locate the identity of a specific individual. Compared with personal data, it is more controllable. Personal data is the data information database formed after computer retrieval of personal information."¹³ Some scholars (Shi Weimin, 2013) believe that the two are mainly different in the

⁷ Supreme People's Court website. Sept. 28, 2021 // URL: <http://www.court.gov.cn/fabu-xiangqing-3085.html> [URL: <https://perma.cc/gf5b-qtb1>].

⁸ Supreme People's Court website. Sept. 29, 2021 // URL: https://www.spp.gov.cn/xwfbh/wsfbt/201705/t20170509_190088.shtml [URL: <https://perma.cc/2sjm-457n>].

⁹ Supreme People's Court website. Sept. 29, 2021.

Some mobile phone management apps ostensibly manage mobile phones, but actually acquire a large amount of information in mobile phones. Through the stolen data information to the elderly user portrait, labeled as "easy to be misled and induced" group, and push vulgar, inferior, deceptive routine advertising and content, in order to defraud the elderly.

¹⁰ A public welfare show jointly hosted by China Media Group and government departments to safeguard consumers' rights and interests on the evening of March 15 every year and broadcast live.

¹¹ China Central Television website. Oct. 10, 2021 // URL: <http://315.cctv.com> [URL: <https://perma.cc/vq9w-yfgh>]. For just RMB 7, The suspect can get a resume of a job seeker in the network group of information transactions. The resume includes the applicant's name, gender, age, portrait, contact, Employment History, qualifications, etc.

¹² Yamaguchi. 2018. General theory of criminal law. 3rd ed. Beijing : China Renmin University Press. P. 18. Atsushi Yamaguchi. Criminal law. The general part. Translation: Fu Liqing. 3rd edition. Beijing : Publishing House of the Chinese People's University. 2018. P. 18.

¹³ Yu Chong. The Nature of Legal Interest of "Citizens' Personal Information" and the Criminalizing Boundary in the Crime of Infringing Citizens' Personal Information // Politics and law. 2018 [04]. P. 19.

field of discussion, "personal information is more focused on the legal field, while personal data is in the technical field."¹⁴ Other scholars (Yang Weiqin, 2016) argue that the two are consistent, "Citizens' personal information and citizen's personal data, the former is the substance, the latter is the form."¹⁵

The discussion of citizens' personal information and citizens' personal data shows that: personal data becomes the characterization of citizens' personal information in Big Data, citizens' personal information is transferred by data as the carrier, and citizen's personal data is the mapping of citizens' personal information in cyberspace. Thus, the identifiable characteristics of citizens' personal information are weakened, which decreases the legal distinction between citizens' personal information and citizens' personal data, and gradually converges with the influence of the Big Data.

The traditional informed consent mechanism can't effectively deal with the legal risks faced by citizens' personal information, and the data assimilation characteristics of citizens' personal information processed by Big Data is one of the issues that should be paid attention to in the current research on the basic theory of criminal law protection in China. The other is the legal interest boundary between citizens' personal information right and citizens' personal privacy right. *The Civil Code of China* stipulates the right to privacy and personal information right successively, and sets the legal rules applicable to the right to privacy for private personal information, which leads to the false attachment of citizens' rights and interests between citizens' personal information and citizens' personal privacy, and then blurs the boundary between citizens' personal information rights and citizens' individual privacy in subjective understanding.

Some scholars (Ling Pingping & Jiao Ye, 2017) point out that "citizens' personal information is objective, and only personal information that can identify and reflect specific acts or activities can enter the boundary of criminal law, while citizens' personal privacy is subjective, and the protection of personal privacy in criminal law requires certain subjective judgment."¹⁶ The criminal law actively protects citizens' personal information, while passively protects

citizens' privacy. With the deepening of Big Data, the understanding of rapid dynamic changes affects the protection of legal interests. Due to the compound interests of citizens' personal information, there is a "contradiction between supply and demand" between the timely intervention of criminal law and the demand for criminal law protection.

The cognition of legal interest attribute not only affects whether citizens' individual rights can be protected by criminal law, but also relates to the judgment of individual crime objects in criminal law. Chinese criminal law classifies infringing on citizens' personal information as a category of charges of citizens' personal and democratic rights, which indicates that Chinese legislation considers this to be the crime against the personal freedom and interests. Some scholars interpret it as "the legal interest of citizens' personal information is embodied in individual rights, not social order."¹⁷ this view directly equates the kindred object of crime with the direct object of crime, and holds that the legal interest of infringing on citizens' personal information is only a personal legal interest, which needs to be considered.

It is positive that the infringing citizens' personal information is to hinder the realization of the right of citizens' personal information, that is, the "legal interest self-determination right"¹⁸ of citizens' personal information. The core of legal interest self-determination of citizens' personal information is informed consent of the right holder.¹⁹ The general principle of informed consent is that the information acquirer has the obligation to inform the information provider and obtain its consent when collecting information.

In Big Data, the theory of informed consent is challenged by reality after the digitization of citizens' personal information, which is prone to the invalid of citizens' individual consent. In the data society, the right of informed consent became rigid, and some information providers have insufficient awareness of information risk, so they are vulnerable to a consent dilemma of the information providers' consent but understand, that is, the information acquirer is authorized by the information provider to collect and utilize citizens' personal information, but the

¹⁴ Shi Weimin. Personal Information Protection in Big Data Era: Predicament and Path Selection // Journal of Intelligence. 2013. 32 (12). P. 157.

¹⁵ Yang Weiqin. Study on the ownership model of personal information in value Dimension — From the perspective of benefit attribute analysis // Law Review. 2016. 34 (04). P. 69.

¹⁶ Ling Pingping, Jiao Ye. 2017. Reanalysis on the Legal interests of criminal Law for the Crime of Infringing citizens' Personal Information // Journal of Soochow University (Philosophy & Social Sciences Edition). 38 (06). P. 68.

¹⁷ Yu Chong. The Nature of Legal Interest of "Citizens' Personal Information" and the Criminalizing Boundary in the Crime of Infringing Citizens' Personal Information // Political Science and Law. 2018. (06). P. 21.

¹⁸ Ji Yang. Legal interest self-determination right and the judicial boundary of the crime of infringing on citizens' personal information // China Legal Science. 2019 (04). P. 73.

¹⁹ Zhang Yong. Criminal Law Protection of APP Personal Information: From the perspective of informed Consent // Law Science. 2020 (08). P. 117.

validity of this authorization is controversial. The illegal utilization of citizens' personal information has not yet been criminalized in China, citizens do not have fully informed consent to self-determination of personal information, so that the procedure for obtaining citizens' personal information is legal, which poses hidden risk for the protection of citizens' personal information, when citizens' personal information is infringed may lead to the security of citizens' personal information chain risk.

B. Act in criminal legislation are not comprehensive

Affected by the variety of Big Data, taking citizens' personal information as the object of crime is complex and changeable. Chinese criminal legislation on citizens' personal information has developed from scratch and from existence to amend, but the acts of infringing on citizens' personal information have not changed, and only stipulates the three types of acts such as illegally obtaining, selling and providing citizens' personal information. Chinese criminal law lacks a relatively complete criminal regulatory system about citizens' personal information. In the increasingly frequent cases of illegal utilization of citizens' personal information in Chinese society, such as the college application tampering case²⁰; Luo Caixia case²¹; 8·25 Deyang female doctor's suicide incident²², because the illegal utilization of citizens' personal information has not been regulated in China, and this act cannot be evaluated by other charges stipulated in Chinese criminal law, there is a legal

loophole in punishing the charge of infringing on citizens' personal information.

In the Big Data, criminal acts are hidden and difficult to detect. When citizens' personal information is illegally utilized, the vacancy in the criminal law may lead to the following results: firstly, the act is difficult to criminal punishment. Secondly, in the absence of the necessary protection of national public power, it is difficult for citizens to confront the infringer in civil or administrative litigation, so it is difficult for individuals to protect their rights. Finally, social order will also be negatively affected to a certain extent.

Another characteristic of the Big Data, value, is that people dig out great practical value based on the analysis of data information. The illegal utilization gradually become more frequent, the contradiction between normative blank and social reality forms the inadaptability of criminal law protection. Illegal utilization is an important part of the logic of the criminal act of infringing on citizens' personal information, if there is no illegal utilization of citizens' personal information, then the acquisition of citizens' personal information is less of the crime terminal link. Illegal utilization is the ultimate purpose of the crime. Illegal utilization makes the legal interests infringed in the previous criminal acts concrete and visual, and turns the possibility of legal interests infringement into the inevitability of legal interests infringement.²³

At present, Chinese criminal law has not criminalized the act of illegal utilization, which makes the judge will determine the case as other related charges when the act conforms the constructive elements of

²⁰ China Court website. Oct. 16, 2021 // URL: <https://www.chinacourt.org/article/detail/2017/01/id/2509078.shtml> [URL: <https://perma.cc/b5nc-haex>].

A middle school student in Shan County, Shandong Province, Chen Zuojia tampered with four classmates' college entrance examination applications, and the court charged that the act was a crime of "destroying the computer information system". However, the real victims of the case were multiple candidates, and the object of the crime should be the information stored in the computer system.

²¹ China Network Television website. Oct. 16, 2021 // URL: <http://news.cntv.cn/special/lanse/weiquan/> [URL: <https://perma.cc/88wg-nkge>]. Wang Jiajun of Hunan Province embezzled the identity information of classmate Luo Caixia and went to college under an assumed name. Wang was not criminally prosecuted.

²² Bai Du website. Oct. 16, 2021 // URL: <https://baike.baidu.com/item/8%c2%b725%e5%be%b7%e9%98%b3%e5%a5%b3%e5%8c%bb%e7%94%9f%e8%87%aa%e6%9d%80%e4%ba%8b%e4%bb%b6/22842202?fr=aladdin> [URL: <https://perma.cc/58k5-hvup>].

A female doctor in Deyang, Sichuan Province had a quarrel with two other swimmers during swimming. After her personal information was exposed, she was cyber manhunt and committed suicide under pressure. The court charged the two swimmers with insult.

²³ Liu Renwen. On the Criminalization of Illegal Use of Citizens' Personal Information // Legal forum. 2019. 34 (06), P. 119.

other crimes, such as the charge of illegal use of information network²⁴, the charge of destroying computer information system²⁵, the charge of insult²⁶, etc. To a certain extent, these charges realize the indirect protection of citizens' personal information rights and interests, but the judgment based on the formal conformity of constructive conditions is not quite appropriate. Firstly, other charges determined in the case are stipulated in other chapters of Chinese criminal law, which can not form a close legal logic system of charges. Secondly, from the legislative purpose, other crimes determined in the case are not set up based on the protection of citizens' personal information, but there is a cross and inclusive relationship in the facts or provisions, so as to achieve the protection of citizens' personal information. Finally, the other charges determined in the case do not directly fill in the legal interest damage of citizens' personal information, and affect the judgment of the actual protection object of the determined charges, affecting the existing criminal punishment system of Chinese criminal law.

C. Criminal judicial determination of circumstance elements is not comprehensive

The "proviso" of Article 13 of Chinese criminal law clarifies that Chinese determination of crime is a "dual" model of qualitative and quantitative analysis

combination, and the criminal acts and circumstances jointly determine the final evaluation of criminal justice. The criminal circumstances of the charge of infringing on citizens' personal information in China, which are divided into serious circumstance and particularly serious circumstance. The perpetrator of serious circumstances will be sentenced to fixed-term imprisonment of not more than three years or criminal detention and will also, or shall only, be fined. If the circumstances are particularly serious, the perpetrator will be sentenced to fixed-term imprisonment of not less than three years and not more than seven years, and a fine.

The judicial interpretation issued jointly by the Supreme People's Court of China and the Supreme People's Procuratorate of China further elaborates the two criminal circumstances of infringing on citizens' personal information. Articles 5 and 6 of the *interpretation of the Interpretation on handling criminal cases of citizens' personal information* quantify the determination standard of serious circumstances and particularly serious circumstance. The interpretation divides the infringing citizens' personal information into information quantity (type); The amount of illegal gains; Use of information; Subject identity; Subjective malice and other elements.²⁷

²⁴ The article 287-1 stipulates: "Whoever commits any of the following conducts by using the information network shall, if the circumstances are serious, be sentenced to imprisonment of not more than three years or criminal detention in addition to a fine or be sentenced to a fine only. (1) Establishing a website or a communication group mainly for committing fraud, teaching on how to commit a crime, producing or selling any prohibited or controlled article, or committing any other illegal or criminal activity. (2) Issuing any information on the production or sale of drugs, guns, obscene articles, or any other prohibited or controlled article or any other illegal or criminal conduct. (3) Issuing any information for committing fraud or any other illegal or criminal activity. Where an entity commits any crime as provided for in the preceding paragraph, the entity shall be sentenced to a fine, and its directly responsible person in charge and other directly liable persons shall be punished in accordance with the provisions of paragraph 1. Whoever commits any other crime while committing a crime as mentioned in the preceding two paragraphs shall be convicted and punished according to the provisions on the crime with the heavier penalty."

²⁵ The article 286 stipulates: "Whoever violates states regulations and deletes, alters, adds, and interferes in computer information systems, causing abnormal operations of the systems and grave consequences, is to be sentenced to not more than five years of fixed-term imprisonment or criminal detention; when the consequences are particularly serious, the sentence is to be not less than five years of fixed-term imprisonment. Whoever violates state regulations and deletes, alters, or adds the data or application programs installed in or processed and transmitted by the computer systems, and causes grave consequences, is to be punished according to the preceding paragraph. Whoever deliberately creates and propagates computer virus and other programs which sabotage the normal operation of the computer system and cause grave consequences is to be punished according to the first paragraph. Where an entity commits any crime as provided for in the preceding three paragraphs, the entity shall be sentenced to a fine, and its directly responsible person in charge and other directly liable persons shall be punished according to the provisions of paragraph 1."

²⁶ The article 246 stipulates: "Those openly insulting others using force or other methods or those fabricating stories to slander others, if the case is serious, are to be sentenced to three years or fewer in prison, put under criminal detention or surveillance, or deprived of their political rights. Those committing crimes mentioned above are to be investigated only if they are sued, with the exception of cases that seriously undermine social order or the state's interests. Where the victim files a complaint with the people's court on the commission of the conduct as provided for in paragraph 1 through the information network, but it is indeed difficult to provide evidence, the people's court may require the public security authority to provide assistance."

²⁷ Yu Haisong. Understanding and application of judicial interpretation of the crime of infringing upon citizens' personal information by the Supreme People's court and the Supreme People's Procuratorate. 1st ed. Beijing : China Legal Publishing House, 2018. P. 37—46.

Item (3) to Item (5) of paragraph 1 of Article 5 sets the determination standards for information quantity (type) and amount of illegal gains (as shown in Table 1). Combined with the data in the table, it shows that among the information quantity (types), the four types of track information, communication content, credit investigation information and property information have the lowest criminalization standards. If the number reaches 50, it will constitute the crime, while accommodation information, communication records, health and biological information and

transaction information need more than 500, or the illegal gains of the case is required to be more than RMB 5000. Such differentiation regulation on the quantity (type) of citizens' personal information and damage results is whether the perpetrator of the case is punished. Therefore, in judicial practice, whether the judiciary can comprehensively identify and accurately classify the quantity (type) of citizens' personal information and other circumstance elements when there is more information involved will ultimately affect the sentencing judgment of the case.

Table 1

Standard for determining the circumstances of different information

Types/circumstances	Serious circumstance	Particularly serious circumstance
Track information	Be used to crime, More than 50 pieces	More than 500 pieces
Communication content	More than 50 pieces	More than 500 pieces
Credit investigation information	More than 50 pieces	More than 500 pieces
Property information	More than 50 pieces	More than 500 pieces
Accommodation information	More than 500 pieces	More than 5000 pieces
Communication records	More than 500 pieces	More than 5000 pieces
Health and biological information	More than 500 pieces	More than 5000 pieces
Transaction information	More than 500 pieces	More than 5000 pieces
Other relevant information	More than 5000 pieces	More than 50000 pieces
Illegal gains	More than RMB 5000	More than RMB 50000

The criminal circumstances of infringing on citizens' personal information are divided into two types: serious circumstance and particularly serious circumstance. At the same time, the principle of heavier punishment is established for special subjects. From the perspective of determining the severity of the circumstances, Authors took the cases of China judgments online from February 28, 2009 (the effective date of criminal law amendment (VII)) to August 1, 2021 as the analysis object. According to statistics, there were 7857 criminal judgments involving citizens' personal information, of which 4411 were serious, accounting for 56.14 % of the total number of samples, and 3365

cases, accounting for 42.83 % of the total number of samples. (as shown in Figure 1) It can be seen that in judicial practice, 40 % of the Infringing citizens' personal information cases are particularly serious, and the Chinese judiciary has a higher determination of the "particularly serious circumstance" of the charge.

Among the 7 857 cases of infringing citizens' personal information collected, the cases can be divided into single circumstance element cases and compound circumstance elements cases according to the circumstance elements involved. After analysis, compound circumstance elements exist in a case, accounting for 83.92 % of the total sample. (as

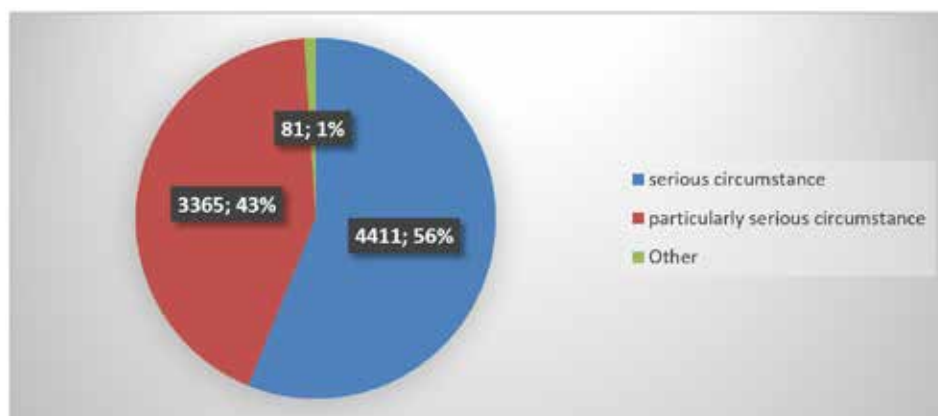


Figure 1. The determination of the seriousness of the circumstances

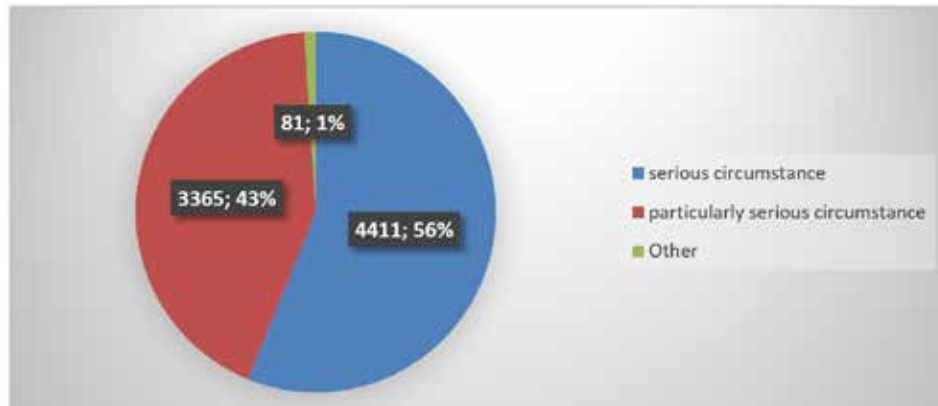


Figure 2. The circumstance elements of the case

shown in Figure 2) Usually, Chinese judicial organ needs to disassemble the compound circumstance elements cases, in order to select the most important factual circumstance as the basis for sentencing, or comprehensively identify various circumstance elements, so as to finally determine the judgment result.

The information type of a single circumstance element case is simple, and the amount of information or illegal gains is clear. The case handling in judicial practice is difficult to go out of control. And judicial organ can make detailed reasoning on the determination of the case in the judgment documents. Yet the charge of infringing citizens' personal information was aggregated with a variety of information elements, once the case involving compound circumstance elements, only a part of the judicial judges will select a variety of information elements, clarify the main plot and combine other elements involved in the case for comprehensive conviction and sentencing. More judicial judges will avoid this problem, directly choose quantity (type) and other elements of the case to unilaterally judge.

At the same time, the reasoning part of legal documents is often difficult to write fully. In addition to the insufficient reasoning of criminal judgment documents, the incomplete judicial determination of circumstance elements will lead to the discrepancy between the facts and results of the case, and the judicial situation of different judgments in the same case. Combined with the data of sentencing circumstances, the proportion of cases with particularly serious circumstances in judicial practice is larger. Its reason is that the judicial determination of compound circumstance elements is not comprehensive. In the process of adjudication, judicial personnel are easy to think simply and fear difficulties when facing the complex case facts, It is not conducive to the comprehensive judicial identification of circumstance elements in cases of infringement of citizens' personal information.

III. The proper path of criminal law protection of Chinese citizens' personal information in the background of Big Data

A. Proposal for criminal law theory

The criminal law takes the protection of legal interests as the core, defines the legal interest object of infringing citizens' personal information, and clarifies the legal interest connotation of the charge of infringing citizens' personal information, which is not only conducive to correctly judge the criminal attribute of infringing citizens' personal information, frame the scope of criminalization, but also serve the Teleology of criminal law, and provide a proper explanation for the constitutive elements of the crime. For both personal information and personal data, Authors think it is appropriated to pay attention to the structural relationship of personal information in the Big Data field. Form the hierarchical protection concept between the two²⁸, based on the isomorphism of citizens' personal information and citizens' personal data, taking the hierarchical and gradual understanding of criminal law, to build up the criminal law protection system: criminal law protection of network data — criminal law protection of personal data—criminal law protection of citizens' personal information.

For both personal information and personal privacy, Authors think it is reasonable to start from their own different characteristics, and take the recognizability of citizens' personal information and the privacy of citizens' personal privacy as the basis of understanding. Grasp the essence of citizens' personal information, accurately identify the connotation and denotation of relevant legal interests, and reflect the generation and exchange of citizens' personal information in the Big Data. Combined with the objective aspects of the acts in the case and the subjective intention of the perpetrators, I think it is justified to make a comprehensive judgment,

²⁸ Li Yuanli. Criminal Law Perfection for Cyber Security and Personal Information Protection // Journal of CUPL. 2015 (04). P. 78.

find different entry points for criminal protection of personal privacy, personal data and personal information, meet the needs of timely intervention of criminal law, and define the legal interests infringed by the criminal act from an all-round perspective.

To establish the concept of information standard and seek the reasonable position of information criminal law, I think it is conscionable to re-understand the connotation of citizens' personal information, break the traditional monistic protection of citizens' personal information, focus on the individual information itself, and take it as the object to establish the protection mode of information criminal law. The main purpose of the charge of infringing on citizens' personal information is to protect citizens' own personal rights and interests, which is indisputable.

However, in the Big Data, citizens' personal information is constantly used, which has produced great socio-economic impact. Under this interaction, the individual attribute of citizens' personal information decreases, while the social attribute becomes obvious. The protection of citizens' personal information in Chinese criminal law is the priority of personal legal interests, but it can not be simply understood as personal legal interests, and the super-personal legal interests such as social and public interests contained therein should be taken into account. It should not be limited to the cognitive level of individual rights and interests, but ignore the social and public rights and interests attribute of citizens' personal information in the Big Data.

To deal with the super-personal legal interest in the charge of infringing on citizens' personal information, I think it is reasonable to start from the system of information criminal law, pay attention to the criminal concept of risk prevention, and implement multi-dimensional and gradual criminal law response. In order to avoid undue damage to right of legal interest self-determination of citizens' personal information due to excessive pursuit of super personal legal interest protection.

Information generates value in the exchange. Under the characteristic of Volume of big data, citizens' personal information is constantly processed and shared. Citizens' informed consent right is affected, and the traditional principle of informed consent in the Big Data to a dead end. In order to deal with the invalid of general informed consent and protect the right of legal interest self-determination of information subject, this principle should be reconsidered. Dynamic consent can be regarded as a good solution. This model can make citizens' informed consent show certain dynamic changes in the process of personal information exposure, and break the dilemma of

one-time consent and formal consent. The flexibility, efficiency and timeliness of dynamic informed consent mechanism precisely correspond to the ever-changing data environment.

Citizens' personal information is in the social environment of the Big Data, it is a consensus to construct the legal system of personal information, to clarify the inner series of the interests of Big Data and criminal law, and theoretically to strive to interpret the relevant provisions of Chinese current criminal law, so as to build an integrated special legal protection integrated with the Big Data and a criminal law system protection of citizens' personal information. In the Big Data, aiming at the practical problems of the informationized society, the rationality of criminal law protection is studied, the security challenges of emerging risks are addressed, the concerns of the public about citizens' personal information rights and interests are responded to, and the orderly development of information criminal law circle is realized.

B. Proposals for criminal legislation

As a selective charge, the three criminal acts reflect the infringing citizens' personal information at different time nodes. In the Big Data, I think it is proper to pay attention to the act, which is seriously harmful to society but has not yet been regulated. Among the existing basic acts such as trading, illegal providing and stealing, it is appropriated to pay attention to focus on other typified act in the crime loop, especially the illegal utilization of citizens' personal information. At present, the criminal act of infringing on citizens' personal information has shifted from illegally obtaining and illegal providing to illegal utilizing as the criminal core.²⁹

Actively clarifying the criminal illegality of illegal utilization of citizens' personal information is conducive to solving the incompatibility of the original criminal law, such as "cyber manhunt", reducing costs of management and control, easing legal tension, and forming a comprehensive criminal protection of citizens' personal information. Consider criminalizing the illegal utilization of citizens' personal information. On the one hand, it can form a system of cracking down on the criminal act of "taking, utilizing and trading" of citizens' personal information; On the other hand, it can reduce the use of miscellaneous provision of infringing citizens' personal information in practice, so as to avoid improper discretion, or the distortion of text caused by the similar interpretation of the articles.

Whether an act needs to be punished by criminal law depends on and only depends on the constitutive elements of crime, but the analysis of the act cannot leave other legal departments. Whether a certain kind

²⁹ Pi Yong, Wang Suzhi. Legal Interests and Dangerous Acts in the Crime of Infringing Personal Information in a Big Data Environment. *Humanities & Social Sciences Journal of Hainan University*. 2017. 35 (05). P. 123.

of act is illegal or not, not only from the perspective of criminal law, but also from the perspective of legal order. The construction of illegal logic of utilization in civil law and administrative law should also be consistent in the criminal law department. The unified legal order requires that Constitution, criminal law, civil law and other legal departments do not conflict with each other, i.e., there should be no contradictory interpretations in the legal field.³⁰

Chinese civil law and some administrative laws have stipulated the utilization of citizens' personal information, which shows that illegal utilization has been ruled as an independent act by law in China. It is not an extension or evolution of other acts. To maintain the stability of the legal order, it is necessary to build the responsibility hierarchy of illegal utilization between different legal departments. The objective risk of information disclosure caused by illegal utilization of citizens' personal information already contains future crimes. Criminal law is the last line of defense for the protection of public or individual legal interests, and the continuous protection circle of legal norms should be the essential signification of criminal legislation. The criminal law protection of citizens' personal information should pay attention to the criminal evaluation of illegal utilization, and put the act of illegal utilization into the criminal circle when punishing the infringement of citizens' personal information. From indirect protection perspective, some criminal gangs of Internet computer crimes and criminal gangs of infringing on citizens' personal information often have substantial links, resulting in the infringement of citizens' personal information and network information security formed a legal connection. Protecting citizens' personal information in the big data is to ensure the information security of data networks.

As far as the specific ways of criminalizing the illegal utilization of citizens' personal information are concerned, there are two ways to criminalize a serious social act in China. One is to amend the law by criminal law amendment, and the other is to interpret the specific act through the existing articles by the competent interpretation organ. Authors believe that amendment can be adopted to determine the criminal illegality of the illegal utilization of citizens' personal information. Main rational reasons: on the one hand, as an independent act, illegal utilization has exceeded the appropriate range of legal interpretation; On the other hand, the legislative method of the amendment conforms to the principle of legally prescribed punishment for a specified crime, which is realized by the subject who holds the highest legislative power. The amendment procedure is rigorous and

legitimate, which is not easy to cause the instability of criminal law. Criminalizing illegal utilization of citizens' personal information will undoubtedly play a positive role in judicial practice. Therefore, taking illegal utilization as a selective charge can cover the act of infringing on citizens' personal information, integrate the internal protection of criminal law, and greatly realize the criminal protection and the public trust and stability of criminal law.

C. Proposals for criminal Justice

Crime as a social phenomenon, circumstances refer to the existence and change of criminal conditions and links.³¹ In order to comprehensively identify the facts of the case and comprehensively evaluate the circumstance elements of the charge of infringing on citizens' personal information, the quantitative standard should be the first. In the process of conviction and sentencing, quantitative standards and non-quantitative standards work together to break the judicial situation of inconsistent information identification and incomplete identification of circumstance elements, realize the accurate classification of circumstance elements, reflect the existence and changes of crimes, and achieve the judicial goal of simultaneous sentencing in the same case. Authors refer to *the Guidance on Sentencing of Common Crimes (Trial) by the Supreme People's Court Supreme People's Procuratorate* came into effect on July 1, 2021,³² and put forward the steps for judicial determination of the charge of infringing on citizens' personal information:

For the case of a single circumstance element infringing on one or more types of citizens' personal information, the quantity (type) of information should be taken as the main basis for circumstance judgment, and the quantitative standard should be taken as the first standard. For the illegal gains in specific cases, the standard of the amount of illegal gains should be taken into account to supplement.

For compound circumstance elements cases, it can be divided into two cases: infringement of a large number of citizens' personal information and infringement of a small number of citizens' personal information. In cases involving a large number of citizens' personal information and with relatively comprehensive circumstance elements, both quantitative and non-quantitative circumstance elements evaluation standard should be taken into account on the premise of taking as the determination basis.

Firstly, according to the quantity (type) elements of information to determine the basic criminal facts,

³⁰ Wang Jun. Must illegality judgment be Monistically Conducted? — In the perspective of Substantive Relationship Between the Criminal Law and the Civil Law. *The Jurist*. 2013 (05). P. 132.

³¹ Gao Mingxuan. *Principles of Criminal Law*. 1st ed. Beijing: China Renmin University Press, 1994. P. 244.

³² Supreme People's Court. Oct. 31, 2021 // URL: https://m.thepaper.cn/baijiahao_13435809 [URL: <https://perma.cc/uh87-e77n>].

and determine the sentencing basis point in the corresponding statutory range of punishment. If the circumstances are unascertainable or difficult to prove, the amount of illegal gains of the case is given priority as the replacement standard, so as to determine whether the case is a crime and the criminal circumstances and sentencing basis point.

Secondly, on the sentencing base point, other elements of the case are integrated to determine the benchmark punishment and increase punishment. The quantity (type) of information should be taken as the keynote, and non-quantitative elements such as the amount of illegal gains, the use of information, subject identity and subjective malignancy should be integrated for criminal judicial determination, and the method of "adding in the same elements and subtracting in the opposite elements" should be adopted to ensure that the judicial determination of compound circumstance elements cases is logical and orderly and the results are fair.

Thirdly, according to the general provisions of criminal law in the statutory sentencing circumstances, and then according to the specific provisions of criminal law of sentencing circumstances for the adjustment of the sentencing basis point.

Finally, the announcement punishment shall be determined according to the law based on the whole case. If a case imposes a fine, the amount of the fine shall be determined according to law on the basis of the criminal circumstances and taking into account the defendant's ability to pay the fine.

In cases involving a small number of citizens' personal information, it shall be quickly ascertained whether the case has resulted in serious consequences such as death, serious injury, mental disorder or kidnapping of the victim, and whether there have been major economic losses or adverse social impacts. If the case has such circumstances, it will directly apply the provisions of the second paragraph of article 5 of the interpretation of the Interpretation on handling criminal cases of citizens' personal information, and the circumstances of the case shall be deemed to be particularly serious. In cases where a few citizens' personal information is infringed, the seriousness of the infringement of the victim's legal interests should be regarded as the core of circumstances, while other circumstance

should be identified as supplementary standard of the circumstances, and then reflected in the main sentence and fine.

To sum up, in the judicial determination of the charge of infringing on citizens' personal information in China, the mode of comprehensive evaluation of circumstance elements should be determined according to the actual fact of the case, and the circumstance elements involved should be comprehensively evaluated, so as not to omit circumstance elements, and different circumstance elements reflect different severity of the circumstances. The judicial organ not only considers the social harmfulness of the defendant, but also considers the defendant's criminal responsibility, so as to adhere to the principle of suiting punishment to crime, and realize the purpose of punishment and crime prevention.

Conclusion

Criminal law is a last resort. When properly used, both individuals and society benefit from it; When used improperly, both individuals and society will suffer from it.³³ The protection of criminal law is not the only, nor the first choice. The criminal protection of citizens' personal information is backward, and specialized legislation fills a certain gap in Chinese law, so that the strike of criminal law tends to be reasonable.

Actively extend the criminal protection of citizens' personal information, actively avoid risks through legal guidance, and create a protection chain between norms. Improve the market access threshold of key industries involving citizens' personal information, strengthen the law enforcement of administrative compulsion and the administrative punishment, enrich the civil remedy, and set up punitive compensation. Big Data is like the sword of Damocles suspended on citizens' personal information.

The new form of crime is just a symbiotic product of the development of Big Data. Maintaining the Criminal Modesty at same time, criminal law should take action when the legal interests of citizens' personal information are infringed, adhere to zero tolerance for crimes, implement the criminal policy thinking of cracking down early and cracking down small, refine the crack down on crimes, and do a good job in criminal law protection.

³³ *Chen Xingliang*. The Value Structure of Criminal Law. 1st ed. Beijing : China Renmin University Press, 1998. P. 10.