WEP Warwick Evans Publishing

Transactions on Social Science, Education and Humanities Research
ISSN: 2960-1770, eISSN: 2960-2262 | Volume 7
ADCS 2024

Criminal Protection of Public Personal Information in the Digital Era

Yuxuan Zhong *

Hefei University of Technology, Hefei, China

* Corresponding Author Email: 2050158285@qq.com

Abstract. The digital era has accelerated the speed and breadth of information dissemination. While enjoying the information dividend, the security of personal information has hidden dangers of leakage. For public personal information, this concern is even worse. On the theoretical level, the secondary authorization theory, the purposiveness theory, and the objective openness standard theory cannot fully respond to the reality and urgency of repeated violations of public personal information. On the level of judicial practices, the guiding cases of personal information protection issued by the Supreme People's Court enlighten us that we should give classified protection to public personal information. Typed protection mode classifies the public personal information from the perspectives of voluntary disclosure, compulsory disclosure, and illegal disclosure, and considers whether it is convicted or not from three aspects: the subjective illegality of the doer, the scope of information control of the information subject and the measurement of public and private interests, which strengthens the protection of the public personal information.

Keywords: Public Personal Information; Crime of Infringing Citizens' Personal Information; Personal Information Protection; Criminal Law Regulation.

1. Raise of the Question

With the rapid evolution of cutting-edge technologies such as big data, the Internet of Things, cloud computing, and artificial intelligence, digitalization has penetrated into all levels of social life, leading us into a new era of "empowerment". [1] The digital economy era shows the characteristic that "The myriad things all count. The myriad numbers all connect." Data has become a key element of social development and one of the main carriers of information. With the rapid progress of information technology and the gradual establishment of information disclosure systems in China, personal information can be widely circulated and utilized. Public personal information refers to the personal information released to unspecified people and obtained directly and legally from public channels. [2] At present, the protection of public personal information in China is relatively weak as a whole. Although Article 253 of the Criminal Law stipulates the crime of infringing citizens' personal information, the criminal law and its related judicial interpretation have no clear provisions on whether the object of the crime includes public personal information. In the academic realm, there are heated discussions among the secondary authorization theorists, the purposiveness theorists, and the objective openness standard theorists. [3] The secondary authorization theorists believe that the re-provision of public personal information should be effectively authorized by the oblige. The purposiveness theorists believe that the use of public personal information should always conform to the original purpose and usage of information disclosure. The theorists of objective openness standard believe that the degree of information openness should be taken as the standard to protect the public personal information. However, all the above theories have certain limitations, and it is difficult to provide comprehensive guidance on the law theory level for the protection of the public personal information. The imperfection of the normative level and the inconsistency of the theoretical level further lead to the different comprehension of judicial personnel in judicial practice about whether the public personal information can be used as the protection object of the crime of infringing citizens' personal information. Some courts believe that the harm of infringing on public personal information is limited, and the consequences of this behavior should be foreseen by the information owner, so it is not appropriate to convict. However, some courts hold that after the defendant collected the public

personal information without the consent of the information holder, the act of illegally providing it to others exceeded the expectation of the information holder for releasing personal information, which is an act of infringing on citizens' personal information and has social harm, and the crime of infringing citizens' personal information should be established. [4]

The deficiency of the above theoretical level and the controversy of related theories make it difficult to effectively protect public personal information, which damages the legitimate rights and interests of information owners and social public interests. Therefore, it is necessary to clarify the theoretical disputes about public personal information. In addition, based on this, this study also explores the normative boundaries of criminal law to protect the public personal information and provides some considerations for judicial practice.

2. The Theoretical Analysis of the Criminal Protection of Public Personal Information

In the current era of big data, citizens' personal information is frequently made public, which has developed into a readily available resource for the public, and the criminal protection of public personal information is facing arduous tests. Therefore, at the level of criminal legislation, academia began to explore the path of criminal protection of public personal information and put forward new theoretical viewpoints to bring public personal information into the scope of criminal protection. However, subject to different positions, the academia has not yet reached a consensus on whether the illegal handling of public personal information should be criminalized and under what circumstances it constitutes a crime. The following lists several representative theories:

2.1. The Secondary Authorization Theory

The legal basis of the secondary authorization theory comes from the second paragraph of Article 3 of the *Interpretation of the Supreme People's Court and the Supreme People's Procuratorate on Several Issues Concerning the Application of Laws in Handling Criminal Cases of Infringement on* Citizens' *Personal Information* (hereinafter referred to as the *Interpretation*). This Article stipulates that the act of providing citizens' personal information legally collected to others without the consent of the collected person belongs to the act of "providing citizens' personal information" as stipulated in Article 253 of the Criminal Law, except that a specific individual cannot be identified and cannot be recovered after processing. Scholars who hold the view of secondary authorization believe that to judge whether the act of providing the obtained public personal information again is punishable, we should consider the will of the information holder and divide it into voluntary and involuntary public personal information. The former should not be considered a crime, while the latter may be punished as a crime of infringing citizens' personal information. [5] Another scholar believes that in terms of the personal information that the obligee has agreed to be public on the website, it is advisable to infer the existence of general consent except that the relevant obligee explicitly requests "secondary authorization", thus preventing the illegality of providing behavior. [6] In other words, the obligee has the right to request a secondary authorization for the public personal information. If the obligee does not request re-authorization, it is legal to provide information without authorization. The theory of secondary authorization reflects that in judicial practice, there are cases in which it is judged that the doer has not obtained the authorization consent of the information holder, which constitutes a crime of infringing citizens' personal information. [7]

In the era of information explosion, information dissemination is fast and wide. If the reuse of information still needs to be authorized by the obligee, it will inevitably increase the difficulty and time for information to be obtained and used, thus slowing down the speed of information circulation, increasing the cost of information circulation, and affecting the value of information circulation, which undoubtedly violates the original intention of the information disclosure system. In addition, Article 27 of the *Personal Information Protection Law* and the second paragraph of Article 1036 of the *Civil Code* deny the secondary authorization rule from the normative level. They stipulate that unless the information obligee explicitly refuses or provides relevant information, which infringes on

the major rights and interests of the obligee, as long as the behavior of the actor providing public personal information is within the reasonable limit, it should not be considered as a crime. [8] From this point of view, the secondary authorization theory cannot play its due role in protecting the public personal information.

2.2. The Purposiveness Theory

The purposiveness theory holds that the use of public personal information should be consistent with the purpose it wants to achieve at the beginning of publicity, and this principle is taken as a restriction. Some scholars believe that the behavior of obtaining citizens' personal information from public enterprise information should not be treated as innocent for the following reasons: if the information processing behavior is consistent with the original intention of disclosing personal information, and there is no fundamental conflict, it should not be considered as a crime. [9] On the other hand, if the act of dealing with personal information significantly deviates from the purpose and usage set by the information owner when disclosing information, then the act may be regarded as a crime of infringing citizens' personal information. In other words, the nature of the act of obtaining and using citizens' personal information again from the public information should be comprehensively analyzed in combination with the purpose and usage of the obligee when he or she first disclosed the information. Another scholar believes that if the behavior of collecting, selling, and supplying public personal information can be evaluated as flowing in the same scene, it should be regarded as "reasonable handling" within the scope permitted by law. [10] In fact, the author believes that the usage scenario of personal information corresponds to the use of personal information, and the above-mentioned scenario view is essentially consistent with the purposiveness theory.

The purposiveness theory can judge the nature of subsequent behavior from a macro perspective by considering the purpose and usage of disclosing personal information, which makes the criteria for judging whether subsequent behavior is guilty more substantial and clear. [11] In addition, the purpose of processing is objectively consistent with the purpose of publicity, and such standards can promote the more convenient circulation of information and give full play to the altruistic benefits of information. [12] However, the rationality of the purposiveness theory is still debatable. First of all, the purpose and usage of disclosing personal information are diverse, complex, and vague. [13] Taking it as a condition of conviction will easily lead to subjectivization of the criteria for conviction. In addition, the theory of purposiveness needs to consider the degree of information control by the information obligee when disclosing information. The increase in the speed and breadth of information circulation will make the reuse of information beyond the obligee's control, but the obligee cannot make an accurate judgment on the use of information in advance. At the same time, the information collector cannot tell the obligee accurately when collecting information. [14] Therefore, it is difficult for information owners to determine whether the purpose and usage of processing are consistent with the purpose and usage of disclosure when processing information.

2.3. The Theory of Objective Openness Standard

Public personal information belongs to the lower concept of personal information, and what kind of information can be judged as public personal information under what circumstances involves the determination of the openness of personal information. The objective openness standard theory focuses on evaluating the degree of objective openness of information and uniformly dividing the criminal responsibility of those who disclose personal information. [15] Scholars who hold the view of this theory believe that personal information can only be called public personal information if its openness reaches a fixed objective standard, and meanwhile, it should be divided into three categories according to its openness: complete disclosure, restricted disclosure, and illegal disclosure. [16] For the completely public personal information, the public behavior has actually obtained the general authorization based on the consent of the information holder or the presumption of laws and regulations, which is in principle in line with the provisions of the second paragraph of Article 1036 of the *Civil Code* and the exemption clause of Article 27 of the *Personal Information Protection Law*,

and usually does not infringe on the personal information right, so there is no need for excessive intervention by the Criminal Law. Restricted public personal information is conditionally open to specific subjects. Therefore, the doer has no legitimate reason to deal with such information without authorization or legal presumption. In addition, if personal information is illegally disclosed by others, the information processing behavior should be regulated by Criminal Law, whether it is completely open or restricted. [17]

In this theory, there is still uncertainty about the "judgment condition of objective openness", which is not completely consistent with the handling of cases of public personal information. Furthermore, restricted disclosure of personal information refers to personal information that is public to a specific subject under certain conditions, but the criteria for judging "specific subject" and "conditional disclosure" are vague. In addition, under what circumstances the public personal information constitute illegal disclosure, and there is still great controversy in academia. Therefore, the theory of objective openness standard is not easy to operate in judicial practice, which leads to its failure to effectively play the targeted attack value of Criminal Law.

To sum up, although the above theories are reasonable to some extent, there is a general lack of typological and scene-based thinking in the choice of case-handling mode, which ignores the differences in the infringement of legal interests due to different usage scenarios. Because different types of public personal information reflect the exercise of personal information rights by information owners to different degrees, it is decided that corresponding protection measures should be taken for different types of public personal information. Therefore, the criminal protection of public personal information should be based on typology.

3. The Judicial Analysis of the Criminal Protection of Public Personal Information

At the level of criminal law, there are still differences in theoretical understanding of the protection of public personal information, which is further reflected in practice. After analyzing the 35th batch of *Criminal Guiding Cases on the Protection of Citizens' Personal Information* issued by the Supreme People's Court, the author finds that the above theory not only plays a guiding role in protecting citizens' personal information in practices but also helps to clarify the legal application of such cases and plays an important role in safeguarding citizens' legitimate rights and interests in disclosing personal information. At the same time, the author also analyzes the possible problems in guiding cases and puts forward relevant suggestions, in order to provide some reference for improving the criminal protection of public personal information.

3.1. The Criminal Protection Mode of Public Personal Information in Judicial Practices

On the protection level of personal information with traditional forms (such as identity cards, mobile phone numbers, etc.), the guiding cases show new highlights, mainly as follows:

First of all, Guiding Case No.193 has a high reference value for sentencing in cases of personal information infringement. In this case, the defendant's defender suggested that the citizen information alleged in this case belonged to the general information in Item 5 of Paragraph 1 of Article 5 of the *Interpretation*, not the specific information in Item 4 of Paragraph 1 of Article 5, so according to the amount of information seized in the case, the defendant's behavior has not yet constituted a particularly serious case. After the trial, the court of the first trial held that the importance of the address on the identity card and the necessity of protecting it according to law should be higher than the "accommodation information" as a temporary and past residence of citizens, so it should be recognized as specific information. The court of the second trial held that the household registration address, name, face, and identity number on the resident identity card are highly unique and identifiable, which can accurately correspond to natural persons, and can further induce the leakage of other personal information of citizens, which greatly infringes on the rights and interests of citizens' personal information. Therefore, the information on the resident identity card should be recognized as information related to the personal and property safety of citizens as a whole. The *Interpretation*

stipulates that the determination of "serious circumstances" of infringing personal information should adopt a comprehensive determination method, which is of great significance to reduce the "quantity-only theory" mode that appears in practice. [19] In terms of the protection of the public personal information, when evaluating the legal element of "serious circumstances" in sentencing, we should fully consider the nature, scale, illegal profit amount, and harmful consequences of the information involved in the act, and make clear the specific standards of these factors. This is conducive to accurately reflecting the actual situation of the case, effectively solving the problem of different evaluation scales in judicial practice, and ensuring the fairness and fairness of case handling. [20]

Table 1. Cases of protecting traditional personal information such as identity card and mobile phone number

Case number and case name	Brief introduction of the case	Focus of controversy	Referee points
Guiding case No.193: Wen Wei and others infringed on citizens' personal information. (2020) Shanghai No.0109 No.957 The first trial procedure of criminal prosecution; (2021) Shanghai No.02 No.1055, The final trial procedure of criminal prosecution	The defendant Mr. Wen and others registered and activated the personal information of citizens, such as photos of purchased identity cards in batches.	Whether the resident identity card information belongs to the fourth item of the first paragraph of Article 5 of the *Interpretation*. [18]	The information on the resident identity card includes a variety of personal information, such as name, face photo, identity number, and household registration address, which belongs to the personal information stipulated in item 4 of paragraph 1 of Article 5 of the *Interpretation*.
Guiding case No.195: Luo Wenjun and Qu Xiaozhen's criminal incidental civil public interest litigation case of infringing citizens' personal information. (2021) Hunan 0212 No.149 The first trial procedure of criminal prosecution	The defendant Mr. Luo and others illegally obtained and sold the personal mobile phone number and verification code of citizens.	Whether the mobile phone number and verification code belong to citizens' personal information	The verification code received by a specific mobile phone number is unique and confidential and can reveal the identity of a specific individual or the details of his life activities, which belongs to the personal information of citizens stipulated in the Criminal Law.

Secondly, in daily life, citizens usually do not associate the value of digital information such as mobile phone numbers and verification codes with their personal identity. Therefore, this kind of information is more likely to be easily disclosed by itself, and then used by offenders, resulting in the failure to fully and effectively protect citizens' personal information rights. Guiding Case No.195 reflects citizens' awareness of the risks of disclosing personal information, which is conducive to strengthening the protection of personal public information in the communication field at the criminal law level. In addition, public interest litigation, a relatively new litigation mode, can effectively protect the rights of citizens' personal information, and combine similar cases for trial, which can effectively improve the handling efficiency of judicial organs and the social influence of related cases, thus enhancing citizens' awareness of the right to safeguard their personal information by judicial means.

The above two cases show that with the progress of information technology, the provisions of Criminal Law concerning personal information protection should also be updated in time. Guiding case No.192 brings face information into the protection scope of Criminal Law, which enlightens us that we should further improve the criminal protection system of biometric information in the field

of criminal regulation, optimize the criminal regulation boundary of biometric technology, and improve the special level protection system of biometric information. [21] Face recognition technology has the technical characteristics of zero contact, non-mandatory, and natural recognition. On daily occasions, any medium that can be equipped with ordinary cameras can be used as an interface to capture face data, and combined with face recognition programs and calculation methods, relevant information can be captured and recorded from a distance. [22] Therefore, face information is more likely to be openly and illegally used, and the related violation of personal information is more harmful to society. Biometric information is more closely related to personal identity, and its personality attribute is significantly higher than that of general personal information. Moreover, the Personal Information Security Code also includes it in the category of personal sensitive information and gives it special protection. Therefore, Criminal Law should adopt the above-mentioned type of protection mode for public personal information, so as to protect citizens' personal biometric information to a higher degree.

Table 2. Cases of protecting personal information in high-tech fields

Case number and case name	Brief introduction of the case	Focus of controversy	Referee points
Guiding case No.192: Li Kaixiang's criminal incidental civil public interest litigation case of infringing citizens' personal information. (2021) Shanghai No.0120 No.828, The first trial procedure of criminal prosecution	Defendant Mr. Li illegally used mobile phone software to steal and sell user album photos.	Whether "face information" belongs to citizen's personal information in the scope of criminal law regulation.	Face information can be used alone or in combination with other information to confirm the identity of a specific individual or track the behavior of an individual, which belongs to the personal information of citizens stipulated in the criminal law.
Guiding Case No.194: Xiong Changheng and others' infringement of citizens' personal information (2021) Jiangxi No.0981 No.376, The first trial procedure of criminal prosecution	Defendant Xiong and others illegally used mobile phone software to obtain and sell social media accounts such as WeChat numbers.	Whether the WeChat number belongs to the citizen's personal information should be protected by criminal law.	Buying, illegally making, selling, or providing social media accounts with citizens' personal information in violation of state regulations. If the circumstances are serious, it constitutes a crime of infringing citizens' personal information.

Guiding Case No.194 takes the characteristics of identifiability as the criterion for judging whether it constitutes personal information, and brings social media account information widely used in life, such as WeChat number, into the scope of criminal law regulation, which makes up for the lack of existing legal provisions and highlights the protection of personal information widely used in modern virtual social scenes. In addition, Criminal Law in China has not clearly stipulated whether to protect the public personal information and to what extent. In this case, the referee's opinion pointed out that obtaining public personal information by means of purchase, acceptance, exchange, and other means without the consent of the citizens themselves or legal authorization and illegally using it violated the original intention and restrictions of citizens when they disclosed personal information, and did not constitute a proper way of handling it recognized by law. If the circumstances were serious, it would constitute a crime of infringing on citizens' personal information. [23] This shows that in judicial practice, public personal information has been brought into the field of criminal law regulation with the theory of purposiveness.

3.2. The Insufficient Protection of the Criminal Law for Public Personal Information in Judicial Practices

"Legislation lags behind, practice comes before that." The above guiding cases keep pace with the times, which has strong practical reference value for improving the criminal protection of public personal information. In addition, in practice, new behavior forms of infringing citizens' personal information have emerged, and it is urgent to amend the Criminal Law from the normative level to make up for the loophole of "everything can be done without prohibition". The specific analysis is as follows:

3.2.1. Increasing the Types of Behaviors Regulated by Law

The above four guiding cases are all based on Article 253 of the Criminal Law, and the illegal selling or providing behavior stipulated in this article is the basis for the defendant to constitute the crime of infringing citizens' personal information. In addition to the above two modes of behavior, the Criminal Law also stipulates the act of illegally stealing or obtaining citizens' personal information by other illegal means. However, the current Criminal Law does not comprehensively summarize the types of such criminal acts and does not list illegal use among them, which cannot give full play to the normative, punitive, and preventive functions of the law. Because the core feature of citizens' personal information is that they can identify the identity of specific natural persons, illegal use of personal information is more accurate than selling, providing, and stealing, and can directly infringe on the personality and property of the information subject. [24] With respect to public personal information, illegal use is consistent with other typical violations at the subject and object levels. The subjective level is intentional, and the doer of the objective level has not been authorized by the information subject or exceeded the scope of authorization, and then used the public personal information for profit, illegal crime, or other improper purposes without authorization, causing serious damage to citizens or society. [25] Therefore, the Criminal Law should be revised and improved in time, and illegal use should be stipulated as an act of infringing citizens' personal information.

3.2.2. Expanding the Subjective Level of Crime

In the guiding cases, the doer is intentional at the subjective level. The Criminal Law in China and related judicial interpretations also believe that the behavior types stipulated in the crime of infringing citizens' personal information usually require the doer to take the initiative, that is, the doer should be intentional at the subjective level, but there is no relevant statement about the negligent crime. [26] However, in practice, it is common that citizens' personal information is infringed due to negligence. Especially in the extensive and high-speed information flow at present, many public and private institutions with personal information sometimes have information leakage problems caused by poor management. This situation not only brings losses of body, mind, and property to individual citizens but also may trigger a crisis of trust among the public. [27] The degree of harm is no less than that of intentional selling, offering, and stealing as stipulated in the Criminal Law. Based on the above reasons, for those who have mastered public personal information, if they illegally sell, provide, or use citizens' personal information because of their carelessness or negligence, causing serious losses to citizens and society, they should bear the corresponding legal consequences. Through the above analysis, it can be seen that the Criminal Law should reasonably expand the subjective level of the crime of infringing citizens' personal information. This can not only effectively improve the vigilance of the subjects who obtain public information when collecting, saving, and using personal information of citizens, but also achieve the purpose of pre-prevention. Moreover, it can urge them to assume the responsibility of rational use and public personal information and ensure the effective protection of citizens' personal information security.

3.2.3. Strengthening the Criminal Responsibility of the Doer

In addition, the protection of personal information in the scene from "relatively public" to "completely public" in life should also be strengthened. Common private enterprises such as Meituan

and Alipay protect the public personal information. The public obtains corresponding services by providing personal information to this type of enterprise and enterprises often have much personal information such as user names, faces, mobile phone numbers, and home addresses. At this time, citizens' personal information is in a relatively open state within enterprises. Under the double inducement of economic interests and unfair market competition, people who have access to the above information within the enterprise are likely to resell such information, making the relatively open information completely public and causing adverse consequences to the information subject. In addition to subjective intention, enterprises may also make the stored personal information used by criminals because of loopholes in program settings and other reasons, resulting in much user information being made public and causing hidden dangers of information security. Enterprises that provide services by obtaining information have the obligation to protect users' personal information, and the Criminal Law should strengthen the criminal responsibility of the person in charge or the person directly responsible for intentionally leaking personal information. At the same time, enterprises should constantly improve their own algorithms and program settings to prevent problems before they happen. If the user information is made public due to the lack of the program, then the enterprise should also bear the corresponding criminal responsibility.

4. The Typed Criminal Protection Mode of Public Personal Information

From the judicial practice, we can see that it is necessary to adopt a type of protection mode for public personal information, and fully consider the subjective psychological state of the doer's intention and negligence and the degree of information disclosure, so as to give full play to the value of information circulation and effectively protect the rights and interests of personal information. Typed thinking can find a balance between abstraction and concreteness, thus better taking into account individual justice. [28] Typing is to divide the types and attributes of research objects based on the fundamental characteristics of things. [29] To a certain extent, the act of disclosing personal information can be regarded as a game between personal information rights and social public interests. Due to the differences in the weight of protection between the two in different scenarios, and the obvious differences in the subject, object, purpose, and basis of the act of disclosing personal information, it is necessary to adopt a typed protection model for the disclosed personal information, and protect it differently according to the standards of voluntary disclosure, compulsory disclosure, and illegal disclosure. [30] The subject of voluntary disclosure is usually the right holder of information, which reflects the exercise of personal information rights, such as individuals posting dynamics on social media, and this behavior has nothing to do with the value of public interest. Compulsory disclosure is mostly made by state organs according to the results of mutual comparison, measurement, and compromise between public interests and personal information legal interests. This kind of publicity involves the dual consideration of public interest and individual rights, and in most cases, public interest is the most important (for example, state organs disclose the information of untrustworthy personnel, with the aim of strengthening the disciplinary function). However, the subject types of illegal disclosure are more diverse, including individuals other than the information subject, as well as government departments and other state organs. This kind of publicity lacks legal basis, and the public behavior infringes on the legitimate rights and interests of the information subject. The illegality awareness of the information processor is the key to the characterization of this kind of scene publicity.

4.1. Voluntary Disclosure

With the development of network technology and the arrival of the information age, the Internet has become an indispensable part of people's lives. Individuals have a higher demand for the dissemination and utilization of information, and the enthusiasm for using social media to disclose information and share life is constantly rising. In the case of voluntary disclosure, the information subject can decide the scope, purpose, and use of personal information independently. Personal information disclosed under this "strong control", embodies the principle of autonomy of private will

stipulated in civil law. Therefore, criminal law should take a cautious intervention attitude to protect it. If this kind of public personal information is disseminated and used again, and it does not cause serious personal injury or property loss, it should not be characterized as the crime of infringing citizens' personal information. Even if this kind of behavior has a negative impact on social public interests, civil law or administrative law should be given priority to regulate and stop it. Criminal law should intervene and regulate only if the behavior brings serious damage to the relevant right holders or social public interests and it is necessary to convict. What needs to be emphasized here is that in real life, the situation which personal information voluntarily disclosed by the information owner is used by a third party is often complicated, such as in the following cases. When using a search engine, the court found that Baidu's collection and storage of the plaintiff's photo did not violate the general duty of care as a search engine. However, when the plaintiff explicitly requests to delete the relevant photos, Baidu is obliged to remove the photo of the certificate according to the user's request. [31] That is, personal information that is voluntarily disclosed should also be used within a certain range. Third-party entities such as relevant platforms still have to fulfill their reasonable duty of care for information that is voluntarily disclosed by individuals and share the risks of some information disclosure. When the third party fails to fulfill its corresponding obligations and damages the interests of the information obligee or social public interests, it should also bear corresponding civil and even criminal responsibilities.

4.2. Compulsory Disclosure

Compared with voluntary disclosure, the scene of compulsory disclosure is more special, and its purpose of disclosure stems from the fact that the protection of public interests should take precedence over personal interests when there is a conflict between individual rights and public interests. This kind of publicity is common in the public release of personal information by state organs, such as the following two situations: the enterprise information disclosed by the enterprise information publicity website, so as to strengthen credit constraints, maintain transaction security, and improve supervision efficiency [32]. The judgment documents published by China Judgment Document Network are convenient for implementing the principle of open trial and promoting judicial justice [33]. Compulsory disclosure focuses on the protection of public interests, which may go against the will of the obligee. Therefore, the protection of this kind of information should be considered from the perspective of interest balance and purposefulness:

First of all, it is necessary to make clear the connotation and extension of legal utilization. The act of simply inquiring and obtaining information that is forced to be disclosed on relevant websites should be regarded as legal use and should not be considered a crime. This is related to the purpose of compulsory disclosing information: (1) to facilitate citizens to supervise administrative or judicial acts; (2) to integrate all kinds of relevant information to facilitate citizens to find and learn; (3) to punish those who violate relevant regulations is closely related to warning other public. In this case, the value of providing information convenience for the public by the government and other public authorities is far greater than the value of protecting the personal information of the information subject. Therefore, the act of searching and using information from public websites should not be punished as an illegal act.

Secondly, the government should determine the connotation and extension of information reuse beyond the original purpose of public authorities to disclose information. The nature of the act of reusing information beyond the original purpose of public authorities should be considered in combination with the purpose of the subsequent use of information by the doer and the degree of losses caused by the act. If obtaining personal information from public websites and then selling it to others for profit, the widespread dissemination and identifiability of the information will cause damage to the information subject beyond the original public purpose. If the damage is serious, the behavior constitutes a crime. Therefore, criminal law should be used to regulate this behavior. In this case, the public authorities have not reached a consensus on how to weigh and choose personal information rights and social public interests. Therefore, at present, there is no consensus in criminal

law circles on how to identify and punish compulsory disclosure. For example, enterprises download, disseminate, and use judicial judgment documents published by China Judgment Document Network for business needs, and two plaintiffs involved in similar cases filed lawsuits in Suzhou and Beijing respectively, demanding the defendant enterprises remove the judgment documents containing their personal information. Although the facts of the cases are roughly the same, the courts in the two places have made different judgments: the former focuses more on protecting citizens' right to control personal information, while the latter emphasizes the importance of judicial transparency and tends to protect public interests such as public supervision and right to know. [34] In view of the above-mentioned types of cases, some scholars believe that the behavior of individual citizens downloading data from the platform and then providing it to others should generally not be considered as a crime, because these data have been made public in nature. Even if there is no special service to promote the circulation of these data, users can still obtain this information by themselves, but it may take more time and energy. Therefore, such services mainly improve the efficiency of data access, rather than creating new data sources. [35] The author believes that the nature, purpose, and use of the re-offering behavior should be considered when determining the criminal responsibility of the behavior that meets this situation, and at the same time, the damage degree of the behavior to the information obligee should be considered. If the purpose of the act is obviously illegal or improper, and the damage to the information subject has exceeded the punishment range of the initial public authority to disclose information, the actor should bear adverse legal consequences.

To summarize, due to the nature of compulsory disclosure, the information subject's control over personal information and subjective initiative to protect personal information are relatively weak. Therefore, in the process of compulsory disclosure, public authorities should be more cautious in protecting personal information and share the pressure that information subjects may face because of public behavior. For example, the personal information to be disclosed is classified into general personal information and sensitive personal information for the second time. Due to the uniqueness and irreplaceability of sensitive personal information, once it is forced to be made public, it will have a greater impact on the information subject. Therefore, public authorities should pay more attention to and protect biological information such as faces, fingerprints, genes, or other sensitive information. [36] To some extent, it will "kill" the adverse risks to individuals.

4.3. Illegal Disclosure

Illegal disclosure means that personal information is placed in a public state without the consent of the right holder. This behavior itself will make personal information beyond the effective control of the information owner, so the disclosure behavior itself is illegal. [37] The author believes that the situation of information being illegally disclosed includes two situations: "illegal disclosure + illegal acquisition and use" and "illegal disclosure + legal acquisition and use". In view of the former combination behavior, the acquisition and use behavior of the post-processor itself is illegal and increases the burden of the information subject, which should constitute a crime. When determining the latter combination behavior in *Criminal Law*, the subjective attitude of the post-processor should be considered first. Specifically, if the information processor realizes that the information he has obtained and used is in the state of illegal disclosure, he will still carry out reprocessing based on this objective state, and the doer should bear the corresponding legal responsibility together with the doer who illegally disclosed the information because he increased the burden of the information subject and acted as an "accomplice" to its damage expansion.

On the other hand, if the information processor has evidence to demonstrate that he did not know or should not have known that the information obtained and used was illegally disclosed, the information reprocessing behavior he carried out may not be considered a crime because he did not know, that is, the adverse consequences brought to the information subject by illegal disclosure and legal use should not be borne by the information processor. In addition to considering subjective fault, the court also needs to consider the behavior of the post-processor when convicting and sentencing the post-processor. This is because, with the development of the Internet, the use of emerging Internet and

automation technology is more harmful to information owners, and should be strictly regulated by criminal law. For example, "big data discriminatory pricing" is a technical means to formulate price strategies by using automated decision-making procedures and unauthorized use of consumer personal information. Compared with the traditional means of information processing, this technology significantly improves the efficiency of information processing, but puts the safety of citizens' public personal information in a more unfavorable position, and may lead to additional economic burden for citizens. [38] However, it should be noted that in the crime of infringing citizens' personal information stipulated in the current *Criminal Law*, the word "infringement" is narrowly understood as "illegal sale, illegal provision, and illegal acquisition". Because the Criminal Law does not include the illegal use of personal information in the scope of this crime, the court cannot investigate the criminal responsibility of the perpetrator of the illegal use of personal information according to the law. [39] Because the illegal use of citizen's personal information is more harmful to society, the author suggests that the *Criminal Law* in China should be revised in time to achieve the purpose of comprehensive and systematic protection of public personal information.

5. Conclusion

The main function and value of information lies in information circulation. The rapid development of digital information technology makes the speed of information circulation show a geometric growth, which leads to the huge economic value contained in citizens' personal information gradually salient. Lured by economic interests, further violations of citizens' personal and property safety by infringing on public personal information occur from time to time. How to protect citizens' personal information at the criminal law level is facing certain difficulties. At present, the *Criminal Law* in China has not clearly stipulated the protection of public personal information, and there are also great disputes in academia about the protection of public personal information, which makes it difficult to deal with the new technologies and new forms of crimes against personal information. Public personal information is an important part of citizens' personal information. It is of unique value to protect public personal information in criminal law so that personal information can find a reasonable balance between free circulation and orderly circulation and better release the dividend of information. In the future, it is suggested to adopt a type of protection mode, combine the problems existing in judicial practices, modify and improve the relevant provisions of the current *Criminal Law* on personal information protection, and bring public personal information into the framework of criminal protection, so as to protect citizens' personal information more comprehensively and promote the construction of information society.

References

[1] Refer to Nicola Negroponte: *Digital Survival*, Electronic Industry Press, 2017, p. 232; Liu Shuangyang, Li Chuan: The Necessary Turn of Criminal Law Protection of Personal Information in the Age of Big Data -- Focusing on Regulating the Illegal Use of Personal Information, *Journal of Chongqing University (Social Science Edition)*, No.6, 2022, 6, p. 232.

[2] See Ma Xinyan, Liu Ruijia: Interpretation Correction of Weakening Protection of Public Personal Information, Jilin University Journal Social Sciences Edition, No.3, 2022, p.63.

[3] See Yu Haisong: A Case Solution of Judicial Difficulties in the Crime of Infringing Citizens' Personal Information, *People's Judicature*, No.32, 2018, p. 14.

[4] See criminal judgment (2018) Jiangsu 0302, No.43, The first trial procedure of criminal prosecution, Gulou District People's Court, Xuzhou City, Jiangsu Province.

[5] See Yu Haisong: A Case Solution of Judicial Difficulties in the Crime of Infringing Citizens' Personal Information, *People's Judicature*, No.32, 2018, p. 14; See also Yu Haisong: Analysis on the judicial application situation and controversial focus of the crime of infringing citizens' personal information, *Journal of Law Application*, No.7, 2018, p. 12.

[6] See Song Weiwei: The Boundary of Criminal Law in Handling Public Personal Information, *Jilin University Journal Social* Sciences *Edition*, No.6, 2022, p. 73.

[7] See Fengcheng city People's Court of Jiangxi Province (2021) No.0981, the first trial procedure of criminal prosecution, No.376 criminal judgment.

[8] See Yu Haisong: Judicial Application of the Crime of Infringing Citizens' Personal Information from the Perspective of Civil Code, *Journal of Beijing University of Aeronautics and Astronautics (Social Sciences Edition)*, No.6, 2020, p.7.

[9] See Zhou Guangquan: The object of the crime of infringing citizens' personal information, *Tsinghua University Law Journal*, No.3, 2021, p. 37, p. 40; Cheng Xiao: On the Legal Regulation of Open Personal Information Processing, *China Legal Science*, No.3, 2022, p. 92.

[10] See Li Yu: Principles and Rules of Criminal Law Protection of Public Personal Information, *People's Procuratorate*, No.8, 2022, p.65.

[11] See Jiang Tao, Guo Xinyi: The Boundaries of Criminal Law Regulation of Public Personal Information, *Academic World*, No.3, 2023, p. 105.

[12] See Ning Yuan: Legal Basis and Rule Application of "Personal Information has been made public", *Global Law Review*, No.2, 2022, p. 73.

[13] See Wang Huawei: Criminal Law Protection of Public Personal Information, *Law Research*, No.2, 2022, p. 195.

[14] See Gao Fuping: Personal Information Protection: From Personal Control to Social Control, *Law Research*, No.3, 2018, p. 98.

[15] See Jiang Tao, Guo Xinyi: The Boundaries of Criminal Law Regulation of Public Personal Information, *Academic World*, No.3, 2023, p. 100.

[16] See Wang Huawei: Criminal Law Protection of Public Personal Information, *Law Research*, No.2, 2022, p.204.

[17] See Wang Huawei: Criminal Law Protection of Public Personal Information, *Law Research*, No.2, 2022, p.206.

[18] See Article 5, paragraph 1 of the *Interpretation of the Supreme People's Court and the Supreme People's Procuratorate on Several Issues Concerning the Application of Laws in Handling Criminal Cases of Infringement on Citizens' Personal Information*: "Illegal acquisition, sale or provision of citizens' personal information shall be deemed as serious circumstances" as stipulated in Article 253-1 of the Criminal Law: (1) selling or providing information on whereabouts and tracks, which is used by others to commit crimes; (2) knowing or should know that others use citizens' personal information to commit crimes, and selling or providing them; (3) illegally obtaining, selling or providing more than 50 pieces of track information, communication content, credit information and property information; (4) illegally obtaining, selling or providing more than 500 pieces of personal information of citizens, such as accommodation information, communication records, health and physiological information and transaction information, which may affect personal and property safety; (5) illegally obtaining, selling or providing more than 5,000 pieces of personal information of citizens other than those specified in Items 3 and 4; (6) the quantity does not meet the standards stipulated in items 3 to 5, but it reaches the relevant quantity standards in a corresponding proportion; (7) the illegal income of more than five thousand yuan; (8) Selling or providing citizens' personal information obtained in the course of performing their duties or providing services to others, with the quantity or amount reaching more than half of the standards specified in Items 3 to 7; (9) Having received criminal punishment or administrative punishment within two years for infringing citizens' personal information, and illegally obtaining, selling or providing citizens' personal information; (10) Other serious circumstances."

[19] See Zhao Jingwu and Tang Haolong: Orientation and Application of Procuratorial Public Interest Litigation under the Framework of Personal Information Protection, *People's Procuratorate*, No.14, 2022, p. 58.

[20] See Zhao Zubin: From Static to Dynamic: Personal Information Protection under Scene Theory, *Science and Society*, No.4, 2021, p. 105.

[21] See Du Jiawen and Pi Yong: The International Vision of Criminal Law Protection of Biometric Information in the Age of Artificial Intelligence and China's Position -- From the Problem of Information Abuse under the Application of Face Recognition Technology, *Hebei Law*, No.1, 2022, p. 144.

[22] See Yang Jian: Legal Regulation on the Application of Face Recognition Technology, *China Social Sciences Journal*, 6th edition, March 25th, 2020.

[23] See Fengcheng city People's Court of Jiangxi Province (2021) No.0981, the first trial procedure of criminal prosecution, No.376 criminal judgment.

[24] See Wang Yuanyuan: Thoughts on Strengthening Criminal Law Protection of Citizens' Personal Information, *Journal of Chengdu University (Social Science Edition)*, No.4, 2022, p. 126.

[25] See Liu Shuangyang, Li Chuan: The Necessary Turn of Criminal Law Protection of Personal Information in the Age of Big Data -- Focusing on Regulating the Illegal Use of Personal Information, *Journal of Chongqing University (Social Science Edition)*, No.6, 2022, p.238.

[26] See Wang Yuanyuan: Thoughts on Strengthening Criminal Law Protection of Citizens' Personal Information, *Journal of Chengdu University (Social Science Edition)*, No.4, 2022, p. 127.

[27] See Liu Guohua, Luo Xin and Zhang Lizhi: On the Criminal Law Protection of Chinese Citizens' Personal Information, *Heilongjiang Social Sciences*, No.4, 2020, pp. 108-113.

[28] See Li Ke: Typological Thinking and Its Significance of Legal Methodology -- Taking Traditional Abstract Thinking as Reference, *Jinling Law Review*, Autumn 2003 (No.2), p. 105.

[29] See Li Ke: Typological Thinking and Its Significance of Legal Methodology -- Taking Traditional Abstract Thinking as Reference, *Jinling Law* Review, Autumn 2003 (No.2), p. 112.

[30] See Ning Yuan: Legal Basis and Rule Application of "Personal Information has been made public", *Global Law Review*, No.2, 2022, p. 71.

[31] See Mr. Sun and Beijing Sohu Internet Information Service Co., Ltd. and other personal rights disputes, Beijing Internet Court (2019) Jing 0491 The first trial procedure of civil dispute prosecution No.10989 civil judgment.

[32] On August 7th, 2014, the State Council issued the Provisional Regulations on Enterprise Information Publicity (Order No.654 of the State Council of the People's Republic of China).

[33] On August 29th, 2016, the Supreme People's Court issued the Provisions on People's Courts Publishing Judgment Documents on the Internet (Fa Shi [2016] No.19).

[34] See the case of dispute over personality right between Mr. Yi and Suzhou Beltas Data Technology Co., Ltd., the civil judgment of Suzhou Intermediate People's Court (2019) Jiangsu 05 The final trial procedure of criminal prosecution No.4745; The dispute between Mr. Liang and Beijing Huifa Zhengxin Technology Co., Ltd. over the liability for network infringement, the civil judgment of Beijing No.4 Intermediate People's Court (2021) No.71, Jing 04 The final trial procedure of criminal prosecution.

[35] See Wang Huawei: Criminal Law Protection of Public Personal Information, *Law Research*, No.2, 2022, p.205.

[36] See Lao Dongyan: Criminal Law Protection Mode of Personal Data, Comparative *Law Research*, No.5, 2020, p. 49.

[37] See Jiang Tao, Guo Xinyi: The Boundaries of Criminal Law Regulation of Public Personal Information, *Academic World*, No.3, 2023, p. 107.

[38] See Liu Xianquan: Adjustment of Elements of Crime of Infringing Citizens' Personal Information from the Perspective of Personal Information Protection Law, *Journal of South China Normal University (Social Science Edition)*, No.1, 2022, p. 148.

[39] See Wang Yuanyuan: Thoughts on Strengthening Criminal Law Protection of Citizens' Personal Information, *Journal of Chengdu University (Social Science Edition)*, No.4, 2022, p. 125.