Research on the restriction of "new" pocket crime under the background of the Internet- from the Amendment of Criminal Law (IX)

Yixiao Hao [1, *, †], Keying Li [2, †]

[1] Law School, Northwest University, Xi 'an, Shaanxi Province, China.

[2] Law School, Henan University of Technology, Zhengzhou, Henan Province, China.

* Corresponding Author Email: 2019107044@stumail.nwu.edu.cn

†These authors countribute equally.

Abstract. With the release of the criminal law amendment (9), refusing to fulfill the obligation of network security crime and helping information network crime, as two important new charges, have improved the criminal law because the responsibility of "network service provider" was introduced for the first time in the field of criminal responsibility. However, in the implementation of relevant charges, due to its limitations in legislation and the similar problems in judicial practice, the scope of related crimes is improperly expanded forming the so-called "new pocket crime". Based on this situation and the legislation in Germany, combined with our own judicial practice, the systematization of related charges should be promoted in network service providers on the legislative level of special legislation. In the judicial level, specification of "knowing" standard and expanding the application of interpretation should be adopted. These two ways can realize the reduction of pocket crime and produce positive effect on the disadvantages of the rule of law construction in China. This paper proposes the method to solve the restriction of pocket crime from two aspects. At the legislative level there are three initiatives. Firstly, special legislation network service providers should be implemented. Secondly, the criminal law charges should be set systematically based on the typing of network service providers. Lastly, the criminal responsibility should be apportioned hierarchically based on the typing of network service providers. As for the judicial level, the identification standard of "knowing" should be clarified in judicial practice. In the process of applying the extended interpretation, it is important to adhere to the same kind of interpretation. In addition, the judicial authorities should organically combine the crackdown on crime with the development of the Internet in the process of cracking down on cybercrimes.

Keywords: New pocket crime, justice, network service provider.

1. Introduction

The pocket problem has a long history in China. In recent years, with the increase of Internet-related cybercrimes, traditional behaviors in public places appear in the network field and the new charges in legislation also show the tendency of pocket. Since the two charges in the Ninth Amendment of the Criminal Law has been published, scholars' discussion has focused on the specific issues of limiting the application of the two charges. Zhang Mingkai denied the legalization of accomplice behavior in the crime of aiding trust and Wuchuanyang believed that it should be judged as a crime from the perspective of neutral behavior. [1] This paper comprehensively reexamines the current situation and harm of pocket crime and puts forward the solution by referring to the German legislation and combining the practice of our country.

This paper analyzes the characteristics of pocket crime from three aspects of legislation, judicial interpretation and judicial practice. At the legislative level, pocket crime is vague in the setting of crime. In terms of judicial interpretation, pocket crime has the phenomenon of expansion explanation or even similar explanation. At the level of judicial practice, the threshold of pocket crime is low and there is a tendency to enter the crime. In the context of the Internet, the specific characteristics of pocket crimes mainly include the vague and abstract provisions of the crime at the legislative level,

the lack of typological standards for the identification of responsibility subjects, the chaotic criminal policy of "cracking down on" cybercrime and "knowing" identification in China at the judicial level.

Then the article analyzes the disadvantages of pocket crime including violating the public interest, causing judicial injustice, destroying the principle of legal punishment, destroying the scientific character of the legislative system, affecting the predictability of the law, and dislocation with the guarantee function of criminal law, so the pocket crime must be limited.

2. The definition and characteristics of the criminal law of pocket crime

2.1 The definition of pocket crime

After the promulgation of the Criminal Law, people joked that hooliganism (crime of speculation) is a basket into which you can put anything. The academic circle also gradually adopted this saying and pocket crime formed a fixed criminal jurisprudence term. [2] Some scholars define the crime as follows. The so-called "pocket crime " refers to the situation that a crime includes too much content or the content is not specific, thus the related behavior can be put in. These two statements point out the manifestations of oral crime, but they are too vague to generalize the characteristics of pocket crime. Some scholars argue that phenomenon of filling in all blanks of incomplete enumeration through uncertain and vague provisions in legislation in order to exhaust the effect of enumeration is called "pocketing in legislation". [3] This statement explains the purpose of the pocket crime. Therefore, it can be said that the phenomenon of using vague law or expanding interpretation in legislation and applying law for conviction in judicature is called the crime of mouth. Nowadays, Except for the inherent pocket crime including the crime of illegal business operation as well as crime of picking quarrels and provoking troubles, since the society the Network times has arrived, help information network criminal activity crime and other crimes also appear a pocketing trend.

2.2 The character of pocket crime

The pocket crime has distinct external signs and formal characteristics, which make it enough to become a typed and regular alienation phenomenon of criminal law At the legislative level, the pocket crime is vague in the crime setting, which includes the use of words involving value judgment, such as arbitrary, serious circumstances, bad circumstances and a list of a wide range of behavior methods.[4] For example, the statement, violating state regulations, is stipulated in the crime of illegal business operation. Meanwhile, the crime of picking quarrels and provoking troubles referred to the phrase" destroy social order" need value judgment.

From the perspective of judicial interpretation, judicial interpretation shows the phenomenon of expansion and even analogy. This point is most obvious in the Internet era of new network crimes. The Explanation of Defamation information completes the expansion of the network of illegal business crime by interpreting the behavior of paid deletion of posts on the Internet as the type of behavior that is covered by the bottom clause of illegal business crime. In addition, the judicial interpretation expands the interpretation of "other methods" in the behavior mode of helping the crime of information network crime, so as to click farming become a crime.

As far as judicial practice is concerned, the pocket crime reflects the tendency of criminalization. The pocket crime solves the conviction needs of the perpetrator, and the pursuit of simple "evil can punish", ignoring the modesty of the criminal law. A case of picking quarrels and provoking troubles, which is known as Zhaoqing graffiti incident, reflect this trend. In Guangdong province, the identification standard for the crime of intentionally damaging property is 5,000 yuan, while the identification standard for the crime of picking quarrels and provoking troubles is 2,000 yuan. The lawyer put forward that the amount of property loss was more than the actual loss and the crime of intentionally damaging property was not established. Besides, the inspection authority changed the initial charge to the crime of picking quarrels and provoking trouble.

3. Pocket of related charges in the Criminal Law Amendment (IX) under the background of the Internet

The Amendment (IX) to the Criminal Law, adopted in 2015, has added two crimes of refusing to fulfill the obligations of information network security management and helping them in the field of cybercrimes.

Paragraph 1 of Article 28 stipulates that a network service bear legal liability under the following circumstances. Firstly, the Internet service provider causes the mass dissemination of illegal information. Secondly, they cause the disclosure of user information, resulting in serious consequences. Thirdly, they cause the loss of evidence in a criminal case to a serious extent. Fourthly, there are other serious circumstances involved. It also stipulates the conditions of punishment, that is to say, the Internet service providers do not perform the information network security management obligations stipulated by laws and administrative regulations. Meanwhile, they refuse to correct after being ordered to take corrective measures by the regulatory authorities. The 5th paragraph of article 29 stipulates the circumstances under which Internet service providers provide support for others to carry out cybercrime activities.

The amendment is the first time to introduce criminal punishment into the field of network service providers, stipulating the criminal responsibility for providing network help for illegal or criminal acts. However, the specific provisions do not make a clear definition of Internet service providers. At the same time, the expression of incrimination circumstances and degree of harm is vague, abstract and applied flexibly, showing a low threshold of incrimination and the tendency to pursue incrimination. As a result, the above two charges show a "pocket" tendency.

3.1 Legislative level of the pocket

The provisions of the crime are relatively vague and abstract, and the identification of the responsibility subject lacks typing standards.

According to the tradition of China's statutory law and the requirements of the principle of legal punishment, the provisions of the criminal law should pursue detail and accuracy, and reach the degree of accuracy in the circumstances of the crime. [5] However, in the criminal circumstances of Article 28 of the Criminal Law Amendment (IX), the vague expressions such as "mass dissemination", "serious consequences" and "serious circumstances" are used for many times. This kind of expression has a certain flexibility in the process of application, which makes it difficult to clarify the standard of this crime entry, and the application space is further expanded, so that the article inevitably has abstract characteristics and the risk of being arbitrarily applied and arbitrarily interpreted. At the same time, since article 28, paragraph 1 of Article 29 and Article 29, paragraph 5 of the Amendment to the Criminal Law do not specify the type of network service providers, the general provision of criminal liability further expands the ambiguity of the standard of such crimes. In practice, different types of network service providers often play different functions in the process of providing network services according to the services and different technology. It should bear the duty of care for criminal behavior should be different, so theoretically should be according to different degrees of duty of care to determine different types of network service providers should bear criminal responsibility. However, in the provisions of the criminal law only generally stipulated that the network service provider should bear criminal responsibility, but do not classify them. Therefore, the determination of criminal responsibility can only be based on vague duty of care, and the criminal responsibility of ISPs with low duty of care is aggravated, which leads to the trend of pocketing of these two charges. Based on the above reasons, the crime of refusing to fulfill the obligation of network security management, and the crime at the beginning of the establishment, and the crime standard was improperly expanded.

3.2 Judicial level of the pocket

3.2.1 Expanding interpretation alienation is analogy interpretation

"Expanding interpretation" is one of the commonly used interpretation methods in the current judicial system in China. By expanding the literal meaning of criminal law provisions, the accurate application of criminal law is realized on the basis of logic. However, based on the vague characteristics of the crime of refusing to fulfill the information network security management obligation and helping the information network crime, this interpretation method is easy to alienate into analogy in the application process, resulting in the improper expansion of the scope of these two crimes. According to the requirements of "expanded interpretation", the expansion of the semantics of criminal law should be within its possible scope and conform to the legislative purpose. At the same time, "ordinary people" can also rationally predict whether their behavior is a criminal behavior. However, in the process of expanding the above two charges, due to "other serious circumstances" out of specific provisions, it is easy to conform the crime whether is not fit the specification as a crime and what is beyond the legislative purpose. Therefore, it can be thought as an alienation of "analogy rather than an" expand interpretation". The application of "analogy interpretation" leads to the improper expansion of the application of the relevant charges, showing a tendency to pocket.

3.2.2China's criminal policy of "cracking down hard" on cyber crimes

With the rapid development of China's Internet industry, the number of information network crimes increases rapidly, which not only causes great losses to China's social economy, but also poses a serious threat to China's national security and other important legal interests. [6] On this background, in order to effectively deal with information network crimes, China follows the basic criminal policy of balancing justice with mercy, and increases the fight against information network crimes. At the same time, by broadening the scope of cybercrime, judicial intervention in advance, aggravating punishment and other ways, China has realized the "strike hard" on cybercrime. Although this criminal policy has a significant effect on cracking down on crimes, the strong tendency to crimes improperly expands the scope of helping information crimes to some extent. At the same time, it causes heavy punishment, aggravating the "pocket" trend of such crimes.

3.2.3 The "knowing" confusion expands the scope of the relevant charges

In China's current judicial practice, in view of the criminal law amendment (9), the criteria of knowing " is confusing. It requires that network service providers have joint intention and criminal perpetrators have clear contact network service providers know a criminal behavior. However, it hasn’t mentioned whether there are specific helpers and whether there are contact between the helpers. In the absence of clear contact requirements, the scope of the crime will be far greater than the requirement of clear contact circumstances. [7] In view of the reality of China's high-pressure crackdown on cybercrimes and the strong tendency of the judicial organs to commit crimes, lowering the entry threshold of the crime has gradually become the main trend. The identification that does not require a clear meaning of contact is more and more adopted by the judicial institutions. In the absence of a unified identification standard, as long as they know that the crime has occurred and provide help, they will be identified as a crime regardless of how harmful the behavior is or whether the upstream crime is effectively controlled. This phenomenon is undoubtedly an improper expansion of the scope of the relevant charges, deepening its character of pocketing.

4. The disadvantages of pocket crime expansion

4.1 Harm judicial justice, reduce judicial credibility

In judicial practice, judicial staff in different regions and at different levels have different degrees of mastery of legal knowledge, and there are certain differences in relevant work experience. In addition, some judicial staff have insufficient professional ability. Meanwhile, there are arbitrary

understanding and selective application of relevant laws. As a result, " the court treats similar cases unequally" will appear in the application of the abstract law, which lacks a clear crime.

In the case of Zhang and Liu opening a casino, the court judge based on the same grounds made such a judgment that Zhang constituted the crime of opening casinos and Liu constituted the crime of helping information network crime. Such cases tend to arouse the public's psychology of disagreeing with the judgment and questioning the impartiality of the judiciary, which seriously undermines the judicial authority and reduces the credibility of the judiciary.

4.2 Undermining the principle of legality

Principle of legality requires that the content of a crime and punishment must be proper. Meanwhile, the punishment scope and degree of punishment must be reasonable. Moreover, only the behavior that has the basis of punishment or deserves punishment can be defined as a crime. China's current criminal law has clearly stipulated the principle of legality in the general provisions. It is not a crime without explicit provisions in the law, and it is not punished without explicit provisions in the law. However, in the crime of refusing to perform the information network security management obligation and the crime of helping information network criminal activities, the listed harmful behavior is unknown and the content is too abstract to accurately apply. Besides, there is no unified and stable value scale for incriminating and incriminating standards. This results in excessive subjective arbitrariness of the judicial organs in the judgment, which also fundamentally violates the statutory requirements of the crime. In addition, the principle of legality also requires that the norms of crime and punishment must be clear, so that the people can accurately understand the constitutive elements of criminal law and the legal consequences of the crime, and reject vague and vague norms of criminal law. The two charges mentioned above make it difficult for the public to predict whether their behavior constitutes a crime, which is not conducive to their compliance with the law and affects the predictability of the law. In judicial practice, this kind of malpractice is mainly manifested in the influence of public opinion on judicature and restriction of citizens' legitimate exercise of rights.

4.3 Dislocation with the protection function of criminal law

As the most severe law in the legal system, criminal law is the last line of defense to protect civil rights and adjust social norms, so it should be modest. Criminal law can only be applied when civil law and administrative law cannot regulate it. Even if some behaviors are harmful to society, criminal law cannot be directly applied. However, in judicial practice, the application of preposition law is overlaid. In order to respond to public opinion or conform to criminal justice policy, some cases that should be handled by administrative law are regulated by criminal law. In addition, the ambiguity and uncertainty of the law itself leads to the concurring of criminal charges, which makes non-criminal charges enter into the crime and this crime is identified as another crime. Thus, it increases the possibility of incrimination and the possibility of applying more serious charges. Under the view of active legislation, the modesty of criminal law is impacted, which is not conducive to the better role of criminal law in social governance.

5. the restriction of "new" pocket crime under the background of the Internet

5.1 Legislative restrictions

5.1.1 Implementing special legislation for network service providers

Special legislation is implemented for network service providers. The administrative legal regulations which conducted on the harmful acts of different types should be applied especially for the network service providers whose behavior do not constitute a crime but the mode conforms to the provisions of the above charges.

Germany, the United States and other Internet developed countries have set up special legislation for network service providers. For example, on March 1,2007, the German Bundestag passed the

remote media law. The law has clearly defined the definition of Internet service providers. that is every natural person or legal person who provide use or the use method of the natural person. At the same time, in the form of typing, the content service providers, information channel providers, information storage providers and cache service providers are not responsible respectively. Meanwhile, the criminal responsibility required by the network service providers is determined in combination with the joint criminal crime theory. [8]

This kind of special legislation is often one of the important bases for determining the criminal responsibility of network service providers. Through the typed analysis of network service providers and the establishment of corresponding exemption clauses, combined with the relevant provisions of criminal law, the systematization and hierarchy of network service providers in the way of crime can be realized.

The laws and regulations on the Internet, including the Decision on Strengthening the Protection of Network Information and the addition of the Criminal Law Amendment (9), are in the absence of a clear definition of the subject, the vague criteria, excessive scope, sentencing severity and judicial injustice, which destroy the legal principle of the crime.

The above problems can be solved according to the current laws and regulations, combined with the tradition of written law in China and the legislation status of Internet service providers in Germany and the United States. First of all, effective laws and regulations can be integrated including Internet Information Service Management Measures and Provisions on Internet Security protection Technical Measures etc. Then set up special administrative law for Internet service providers on the basis of integration. The content should include a clear definition and typing of ISPs. Categories can include content service providers, storage service providers, caching service providers, and Internet access service providers. At the same time, hierarchical liability clauses should be set up for different types of Internet service providers, which means that responsibilities should be allocated according to the level of duty of care. Content service providers should have the highest duty of care and storage service providers should have a higher duty of care. Meanwhile, caching service providers should have a lower duty of care and Internet access service providers should have the lowest duty of care. [9]

Through the establishment of special administrative regulations, the typing of network service providers and their responsibilities are hierarchical. Their responsibilities are pre-reviewed. The corresponding administrative illegal acts should be stipulated referring to the contents of the two crimes of "crime of helping information network crimes" and "crime of refusing to fulfill network security management obligations". Thus, such illegal acts are regulated through administrative punishment. At the same time, under the corresponding liability provisions, it stipulates that "if a crime is constituted, the criminal responsibility shall be borne according to law", and the criminal responsibility of different types of network service providers is determined respectively according to the nature of their behavior and the size of their harm. When the behavior of the network service provider causes serious harm to the society, the administrative institutions that are responsible for supervision shall transfer the case to the criminal judicial organ and impose sanctions through criminal procedures, so as to realize the connection between the law and the criminal law.

5.1.2 Systematic of criminal law charges based on the typing of network service providers

The content of the crime of refusing to fulfill the network security management obligation is set systematically, and different types of network service providers assume responsibility for different criminal acts based on different obligations of care. [10]

In the case of paragraph 1 of Article 28, different types of network service providers shall be set up for the criminal liability responsibility.

The criminal responsibility in the case of "causing the large dissemination of illegal information" shall be attributed only to the content service provider and the storage service provider. Based on the characteristics of the Internet rapid transmission, the result of the mass dissemination of illegal information may occur quickly in a short time. However, its stay in the access service is too short and related service providers are difficult to achieve supervision to the illegal information in this period

of time. Therefore, the two types of service providers do not need to bear the duty of care for the situation. Meanwhile, content service provider is the subject which provides subjective information, so it should bear the highest degree of regulatory obligation. Storage service provider and cache service provider is a long time to store a large amount of information, so it has enough time and technology to realize the supervision of illegal information and has a high regulatory obligation to illegal information. In this case, the content service provider has the obligation to actively review. Meanwhile, the storage service provider and the cache service provider need to cooperate with the supervision of relevant departments. If they should not actively review or cooperate with relevant departments, resulting in a large dissemination of illegal information, they shall bear criminal responsibility.

In view of the "leakage of user information caused serious consequences" and "loss of criminal evidence" two cases, because protecting user information from disclosure is one of the basic obligations of network service providers, all types of network service providers should assume the obligation of care for these two situations. Among them, because the information provided by the information content provider is subjective and has the highest regulatory obligation for the content published, it shall bear the obligation of active review, and the above two circumstances shall bear criminal responsibility due to no active review. However, Internet access service providers, storage service providers and cache service providers have high obligations of attention for these two types of situations, so they shall bear the responsibility of cooperating with the supervision of relevant organs. Those two circumstances shall bear the corresponding criminal responsibilities due to the lack of cooperation with the supervision.

5.1.3 The hierarchy of criminal responsibility based on network service providers

The punishment that should be borne for the crime of helping information network crime is set hierarchical. Different types of network service providers bear different levels of punishment for the crime based on different obligations of care.

For the application of the Criminal Law Amendment (ix), article 29, clause 5, Internet service providers can be divided into natural persons and legal persons. According to the different duty of care they bear, the criminal responsibility they should bear is determined. In the cases where the natural person shall bear criminal responsibility, the network service provider with the highest obligation of care, the storage service provider and the cache service provider may be sentenced to fixed-term imprisonment of not more than 3 years. The internet access service provider has a general duty of care and may be sentenced to criminal detention, public surveillance or a fine. Where the legal entity shall bear the criminal responsibility, the content service provider, the storage service provider and the cache service provider shall bear a higher fine, and the Internet access service provider shall bear the general fine. [11]

5.2 Limit at the judicial level

5.2.1 Clarify the identification standard of "knowing" in judicial practice

First of all, whether there is a clear contact between the network service provider and the perpetrator of the criminal act, "knowing" is divided into both knowing and no knowing. [12] Among them, because the network service provider has a clear subjective intention to help to carry out the crime, it should not be punished as the crime of "helping the network information crime", but it should determine the criminal responsibility with the help of the relevant crime according to the theory of common crime.

In the absence of conspiracy knowledge, it should be further divided into knowledge and prior knowledge, and they will determine different responsibilities according to different types of network service providers. [13] As for the knowledge, since the network service has been provided when the criminal act was known, it is difficult for the Internet access service provider to effectively control the information at the technical level. Therefore, these two types of subjects should not take responsibility for the knowledge. Storage service providers and cache service providers are

technically easier to control criminal acts, so they should be knowingly responsible for the incident. For prior knowledge, Internet service providers are aware of the occurrence of criminal acts before they provide network services. Although they do not have a clear connection with the perpetrator of the crime, they have a laissez-faire attitude towards the occurrence of the crime. Due to higher subjective malignancy, in this case all types of network service providers should bear the corresponding responsibility.

5.2.2 Adhere to the same kind of interpretation in the process of applying the extended interpretation

In the process of applying the "expansion interpretation", "other serious circumstances" should be interpreted as "the circumstances in line with the specific nature of the enumerated acts". By limiting the scope of the interpretation of the bottom-line clause to the same nature as the specific circumstances, arbitrarily incorporating different nature and different types of behaviors into the same criminal law provisions will be avoided. Besides, it can prevent the improper expansion of the semantics of the clause and guarantee the unity of its legislative purpose.

Taking the crime of refusing to perform network security obligations as an example, the scope of "other serious circumstances" shall be limited within the same nature as the following acts. The first one is the mass dissemination of illegal information. The second one is the disclosure of user information and serious consequences. The third one is the loss of evidence in criminal cases and the circumstances are serious. The nature, mode and harm degree of the behavior derived from the expanded interpretation of "other serious circumstances" should be similar or similar to the above three behaviors, so as to realize the similar interpretation. In this way, the average person can rationally judge whether their behavior is a crime, and avoid improper expansion of the semantics of criminal law provisions in the process of expansion interpretation, so as to prevent the judicial organs from alienated it into similar interpretation when applying the expansion interpretation, then finally achieve the restriction of the new pocket crime.

5.2.3 In judicial practice to promote the organic combination of Internet development and crime fighting

The benefits and harms brought by the rapid development of the Internet exist in the meantime, and the problem of cybercrime is becoming more prominent with the expansion of the scale of the Internet. In this context, China has cracked down on cybercrimes from various aspects such as legislation and justice. From the introduction of the Criminal Law Amendment (IX) to the rapid growth of the number of "helping letter crimes" in judicial practice, they all highlight China's strict criminal policy for cybercrimes. However, under such high-pressure situation, the scope of the criminal responsibility of network service providers will become wider and wider, which will undoubtedly have a negative impact on the development of the Internet and ultimately damage the development interests of China.[14] Therefore, in the process of cracking down on cybercrimes, the judicial organs should organically combine the crackdown on crime with the development of the Internet, and make appropriate restrictions on the expansion of the criminal responsibility identification of network service providers. In the process of the network service provider criminal responsibility, according to its role and function and technical level, combined with the possibility, difficult possibility and theory, the organic combination of the Internet development and crime for the purpose can be realized through the crime of criminal responsibility for the network service provider scope of limitation.

When punishing Internet enterprises, the subjective aspects and regulatory ability should be fully considered of such enterprises. [15] When they subjectively fail to help criminal acts or intentionally commit criminal acts, it should be carefully considered whether criminal punishment should be applied. If there is no subjective intention and the duty of care has been objectively fulfilled, they should not bear criminal responsibility even if the criminal punishment stipulated by the result of the crime. Even under criminal responsibility for no duty of care, a lower punishment should be imposed

for lack of subjective intent. In this way, the organic combination of crime fighting and the development of the Internet is achieved.

6. Conclusion

Pocket crime is a long-standing problem in China. From the traditional pocket crime to the newly developed pocket crime such as the crime of refusing to fulfill the obligation of network security management, they all reflect the characteristics of a low entry threshold and a high entry crime tendency. In judicial practice, the judicial organs' abuse of expanded interpretation and knowing of confusion further strengthen their tendency of pocket crime, which leads to many disadvantages affecting the construction of the rule of law such as violating the public interests and destroying the law of crimes. Based on this situation, it is particularly important to limit the new pocket crime in the context of the Internet. This paper puts forward the restrictive path from the legislative and judicial levels. Combined with the current legislative situation of the United States and Germany and China's legal tradition, this paper proposes the restriction strategies. At the legislative level, special administrative regulations should be established and relevant criminal regulations should be systematically adjusted based on the hierarchy of network service providers. At the judicial level, this paper suggests the ways of standardizing the recognition standard of knowledge, expanding the interpretation as well as the application and adjusting of criminal policies. Based on this way, the research improves the restriction of pocket crime and contributes to the construction of the rule of law in China.

References

[1] Zhang Mingkai, Understanding and Application of Several Articles in The Criminal Law Amendment (9) -- On the Crime of helping information Network crime [J]. Politics and Law, 2016(2):15.

[2] Yu Zhigang, The Change of The Times, current disorder and elimination of oral crime [J]., 2013, 1(003):63-78.

[3] Qiu Zhiyong, On the Phenomenon of "pocket" in Chinese Legislation and its Influence on the Rule of law [J]. Journal of Beijing People's Police College, 2003(2):4.

[4] Sun Daocui, A restatement of criminal Law Orientation of "Oral Crime" [J]. Journal of National Procuratorial College,202,30(01):105-122.

[5] Xiang Yan, Wu Yuting. Analysis on the Pocketing phenomenon of network crime and thoughts on its reduction path [J]. Journal of Sichuan Police College.2021(01):27-34.

[6] Zhao Liang, On the development trend of information network crime and the improvement of criminal policy [J] Chinese applied law. 2022 (01): 122-134.

[7] Huang Zhongjun, Zhang Zhanying. Analysis and judicial application of the crime of helping information network crime [J]. People's Procuratorate, 2021(23):49-53.

[8] Bu Peipei, Identification of Criminal Liability of Internet Service Providers and Legislative Improvement [D]. Shandong University.2020(02).

[9] Wang Mingfu, Research on the criminal responsibility of network service providers [D] People's Public Security University of China. 2019 (09).

[10] Wang Huawei, Comparative study on criminal liability of network service providers [J] Global legal review. 2016 (04): 41-56.

[11] Yang Xinlu, On the criminal responsibility of network service providers [D] Central South University of economics and law. 2018 (08).

[12] Wang Li, Research on criminal regulation of network service providers [D] China Youth Political College. 2016 (06).

[13] Tu Longke, Analysis on the criminal responsibility model of network service providers and its relationship [J] Politics and law. 2016 (04): 108-115.

[14] Dong Puyu, Reflection on the expansion of criminal legislation of cybercrime in China Treatise on criminal law. 2019 (02): 297-323.

[15] Qi Wenyuan, Application and Reflection on the criminal policy of fighting early and petty crimes under the background of "less arrest, careful prosecution and careful custody" -- from the perspective of cybercrime Governance [J] Political and legal forum. 2022 (02): 62-73.