Vol.5 Iss.2 2024
https://doi.org/10.37420/j.mlr.2024.013
Modern Law Research

Research on the Application of the Criminal Policy of "Early Crackdown on Petty Crimes" in the Governance of Cybercrime

Suwan Yu[1*]
[1] College For Law, Beijing Normal University, Beijing, China
[*] Corresponding author,E-mail: yusuwan2000@163.com

Abstract
Based on the "chain" of cybercrime and the correlation between upstream and downstream crimes, when legislation has not yet responded to the governance and regulatory measures related to cybercrime in a timely and definite manner, applying appropriate criminal policies, such as the "early crackdown on petty crimes" criminal policy, is a good strategy for addressing the source of cybercrime and providing some experience for legislation. The application of the criminal policy of "early crackdown on petty crimes" in the governance of cybercrime is in line with the basic core of "source governance", conforms to the spirit of the criminal judicial policy of "less arrest, more cautious prosecution, and more cautious detention", and follows the petty crime criminal legislation model of China. However, we should follow the "Nulla poena sine lege" in the criminal law when it is applicable, and build a diversified governance system for cybercrimes to achieve the coordinated development of crime governance, human rights protection, and technological progress.

Keywords
Criminal policy of "early crackdown on petty crimes"; Source governance; Cybercrime; "Nulla poena sine lege"

1 Introduction

The Fourth Plenary Session of the 19th Central Committee of the CPC put forward specific requirements and methods for national and social governance, namely, "strengthening systematic governance, governance by law, comprehensive governance, and source governance". Among them, systematic governance emphasizes the need to strengthen the systematicity and integrity of the governance system, avoid using localized and fragmented governance methods, and cause governance chaos; Rule of law proposes that the basis for governance has a legal nature, which means that national and social governance needs to be carried out within the legal scope and the law is the criterion; Comprehensive governance highlights the diversity of governance methods and requires the comprehensive utilization of multiple feasible means of governance based on actual situations; Source governance points out the need to focus on the root causes of problem, emphasizing the need to address both symptoms and root causes. The "four governances" form an organic system of national and social governance, and the "source governance" also provides clear direction for the governance of cybercrime.

© 2024 by the author(s); licensee Mason Publish Group, this work for open access publication is under the Creative Commons Attribution International License (CC BY 4.0). (http://creativecommons.org/licenses/by/4.0/)

Based on the "chain" of cybercrime and the correlation between upstream and downstream crimes, if the upstream crimes of cybercrime are not punished in a timely manner, the source of cybercrime will not managed, and the criminal chain will not be cut off. So that it will continuously expand the cybercrime's scale and extend the criminal chain, ultimately resulting in huge impact and irreparable consequences. Therefore, when legislation has not yet timely and clearly responded to the governance and regulatory measures related to cybercrime, it is a good and important strategy to apply appropriate criminal policies to address the source of cybercrime and provide some experience for legislation. The criminal policy of "early crackdown on petty crimes" in our country has played an important guiding role in the early governance of the source of combating gang crimes, and there is a certain degree of similarity between gang crimes and cybercrime. For example, both are developing from the primary stage to the mature stage, and then expanding and extending to downstream crimes. Once a criminal group or chain with huge influence is formed, it will cause serious harm to national security and social order, and require significant costs for regulation. Therefore, the most direct and effective way to deal with such crimes and save regulation costs is to start from the source, and take appropriate measures to regulate them at the initial stage of crime formation and when the harm is low, to avoid further aggravation of related crimes.

Based on this, we attempt to integrate the "early crackdown on petty crimes" criminal policy into the governance of cybercrime. We are going to explore the application path of the "early crackdown on petty crimes" criminal policy in the governance of cybercrime, in order to more effectively govern cybercrime.

2 The Formation and Development of the Criminal Policy of "Early Crackdown on Petty Crimes"

In terms of the essence of criminal policy, Feuerbach believes that criminal policy exists alone, and it is a legislative policy that guides criminal legislation. The intrinsic values of the criminal policy and the legislative policy are consistent; Liszt extends criminal policy to social groups or national levels beyond the scope of legislation. Criminal policy is positioned as crime prevention and perpetrator correction. It is independent of criminal law and is unable to break through the law's limitations; Klaus Roksin advocates integrating the value of criminal policy into the criminal law system, exploring the necessary and purposeful responses that criminal policy needs to adopt for crime prevention and control.

As one of the criminal policies, the "early crackdown on petty crimes" criminal policy was originally and innovatively proposed to better prevent and control crimes, based on the premise of following criminal legislation and combining practical experience. The criminal policy of "early crackdown on petty crimes" in our country can be traced back to the police policy of the public security organs, stemming from the comprehensive social security governance guidelines of "combining prevention and control, focusing on prevention", as well as the crime prevention and control strategies of "striking when exposed" and "concentrating on the serious crimes while not neglecting the petty offenses" proposed by the public security organs based on the experience which is accumulated from "strict crackdown", then mainly and systematically applied in the fight against gang crimes. Specifically, in 2006, the Central Political and Legal Affairs Commission deployed a national special crackdown on gang crimes, pointing out the need to adhere to the

© 2024 by the author(s); licensee Mason Publish Group, this work for open access publication is under the Creative Commons Attribution International License (CC BY 4.0). (http://creativecommons.org/licenses/by/4.0/)

working principles of "early crackdown on petty crimes" and "striking when exposed". In July 2009, the Central Political and Legal Affairs Commission issued the "Work Opinions on Deepening the Special Struggle against Gang Crimes", emphasizing once again the need to adhere to and apply the criminal policy of "early crackdown on petty crimes" in the struggle. In January 2018, the Central Committee of the Communist Party of China and the State Council issued a notice on the special struggle against gang crime, which clearly pointed out that in response to gang crimes, we should "adhere to strict punishment in accordance with the law, crack down on petty crimes early, address both the manifestation and root cause, and persist in source governance." From this perspective, the criminal policy of "early crackdown on petty crimes" has been a basic strategy for combating gang crime since its inception and the criminal policy has also played an important role in it.

Specifically, the important role of the criminal policy of "early crackdown on petty crimes" in its practical application mainly includes three points. Firstly, the essential purpose of criminal policy is to maintain social order. Implementing the criminal policy of "early crackdown on petty crimes" is conducive to achieving the criminal policy goal of benign control over social order; Its primary and long-term mission is to protect the personal and property safety of citizens and ensure the continuation of social harmony. The criminal policy of "early crackdown on petty crimes" advocates punishment and regulation of low-level forms of crimes, effectively reducing the social harm of gang crimes and maximizing the maintenance of social harmony and stability, as well as national security and legal protection. Secondly, implementing the criminal policy of "early crackdown on petty crimes" is conducive to the normative purpose of protecting social fairness and legal interests. The criminal policy of "early crackdown on petty crimes" takes it as its responsibility to eliminate related crimes in the primary stage and avoid their further expansion. It is a reasonable and effective response of the country and society to such crimes, curb the encroachment of criminal forces on social justice and civil rights, and promote the construction of a just social order. Thirdly, implementing the criminal policy of "early crackdown on petty crimes" is conducive to achieving the goal of crime prevention and punishment. In the case of criminal organization crimes, this policy scientifically grasps the development law of organizations from "petty" to "serious" and from "scattered" to "gang-style". In combination with the actual situation in China, according to the unique stage characteristics of the development of criminal organization, it needs to be prevented and controlled in advance to effectively suppress its growth.

3 The Application Basis of the Criminal Policy of “Early Crackdown on Petty Crimes” in the Governance of Cybercrime

With the advent of the artificial intelligence era, new types of crimes based on online platforms are becoming more frequent. On January 22, 2021, the Supreme People's Procuratorate issued the "Regulations on Handling Cybercrime Cases by People's Procuratorates" (hereinafter referred to as the "Regulations"), which pointed out that cybercrime referred to crimes committed against information networks, crimes committed using information networks, and other upstream and downstream related crimes. Cybercrime can mainly be divided into: (1) Crimes committed against information networks (using the network as the criminal object), such as the crime of damaging computer information systems; (2) Crimes committed us-

© 2024 by the author(s); licensee Mason Publish Group, this work for open access publication is under the Creative Commons Attribution International License (CC BY 4.0). (http://creativecommons.org/licenses/by/4.0/)

ing information networks (using the internet as a criminal tool), such as fraud and gambling crimes through the internet; (3) Other upstream and downstream related crimes. This regulation clearly defines cybercrime as including its own and upstream/downstream related crimes. Its upstream/downstream related crimes are comprised of new types of crimes derived from information networks, new forms that traditional crimes rely on information networks to present, and upstream/downstream crimes that are related the above two types of crimes. This regulation also points out that cybercrime has the characteristics of chain and industrialization, and there is a process of gradual development from the primary stage to the mature stage, and once it develops to the mature stage, it is difficult to govern, which has a certain degree of similarity with the characteristics of gang crimes.

Based on the important role and significant achievements of the "early crackdown on petty crimes" criminal policy in cracking down on gang crimes, it can be considered to gradually expand the "early crackdown on petty crimes" criminal policy from cracking down on gang crimes to the field of network crimes governance. In addition to the good results achieved by the "early crackdown on petty crimes" criminal policy in similar types of gang crimes, the application of the "early crackdown on petty crimes" criminal policy in the governance of cybercrime also has the following three policy bases.

3.1 Complies with the Basic Core of "Source Governance"

Firstly, the criminal policy of "early crackdown on petty crimes" is consistent with the basic core of the "source governance" policy proposed in the Fourth Plenary Session of the 19th Central Committee of the Communist Party of China. The criminal policy of "early crackdown on petty crimes" emphasizes the implementation of crackdowns on criminal organizations in the initial and primary stages of crime occurrence and the formation of criminal organizations, in order to achieve effective governance of crime when the scale of criminal organizations is relatively small. "Source governance" emphasizes that crime governance should be carried out fundamentally from the source that triggers the emergence, formation, and development of crime, in order to avoid the continued development of crime and the derivative of other crimes. Therefore, the criminal policy of "early crackdown on petty crimes" is a concrete manifestation of the "source governance" policy. One of the effective ways to achieve "source governance" by tracing the origin and upstream situation of crime, is to adhere to the policy of "early crackdown on petty crimes" and crack down on crimes in the primitive and embryonic stages, in order to achieve effective and comprehensive governance of crimes.

From the perspective of criminal characteristics, the official points out that "the current trend of network crime chain and industrialization is obvious, and a complete network black market chain has been built." From this perspective, the new era of network crime shows characteristics of "chain" and "industrialization". With the help of the black market chain on the internet, online crimes related to upstream and downstream have been strengthened and extended, and the trend of frequent and high incidence of online crimes and related crimes is obvious. Article 3 of the Regulations states that "the People's Procuratorate should strengthen the punishment of the entire chain when handling cases of cybercrime, pay attention to reviewing and discovering clues of upstream and downstream related crimes." The criminal policy governance path of "early crackdown on petty crimes" is in line with the basic core of "source governance" of cyber-

© 2024 by the author(s); licensee Mason Publish Group, this work for open access publication is under the Creative Commons Attribution International License (CC BY 4.0). (http://creativecommons.org/licenses/by/4.0/)

crime. When upstream crimes in the online black market chain are prepared as tools or means for subsequent crimes, timely and effective governance measures should be taken against upstream cybercrime to cut off the chain of cybercrime and avoid the formation of a complete and mature cybercrime chain.

From a technical perspective, cybercrime has the characteristics of widespread impacts and uncontrollable consequences. Besides, its criminal targets have expanded from acquaintances to strangers. With the stimulation of modern network technology, criminal behavior will experience a qualitative leap in its harmfulness and uncontrollability. In the era of Web 2.0, people can share information and remotely communicate with others through the internet, and achieve multi-type interaction between people based on online platforms. The manifestation of cybercrime during this period is the use of the internet as a tool and means of crime, using the internet to commit traditional or new crimes. The criminal object gradually expands from traditional acquaintances to strangers, and cybercrime such as cyberbullying and defamation also shows a characteristic of aggregation, which is reflected in the crowding effect, spillover effect, and cyberbullying effect. In the era of Web 3.0, the functions of online platforms will be weakened, and there will be direct two-way information interaction between people and the network. The connection between individual and network will become closer. At the same time, artificial intelligence's unique algorithm and deep learning ability make human-computer interaction a reality. However, the harm of cybercrime will be further enhanced. Scholars have pointed out that the danger of using artificial intelligence to commit cybercrimes is worth attention since the harm and uncontrollability of cybercrime derived from constantly developing technology will be greatly enhanced. Only by "early crackdown on petty crimes" on the growing number of cybercrimes, prioritizing prevention measures and governance stages, reasonably and early intervening in risk control, and preventing further expansion of risks, can we realize the minimization of criminal damage and the maximization of social interests.

3.2 Correspond to the Spirit of Criminal Justice Policy of "Less Arrest, Cautious Prosecution, and Cautious Detention"

The criminal policy of "early crackdown on petty crimes" is also highly consistent with the spirit of the criminal justice policy of "less arrest, cautious prosecution, and cautious detention", both of which focus on cases of petty offenses. The criminal justice policy of "less arrest, cautious prosecution, and cautious detention" mainly refers to that "the majority of petty crime cases should be treated with more leniency, and more attention should be paid to custody and prosecution. The review of social risks of arrest should be strengthened, and those who can not be arrested according to law should not be arrested. Non-detainment compulsory measures should be applied as far as possible, so as to reduce the number of suspect in custody pending trial". According to the work report of the Supreme People's Procuratorate in 2020, the proportion of felonies decreased from 19.6% in 1999 to 2.7% in 2019, and the proportion of people sentenced to fixed-term imprisonment of less than three years increased from 54.6% in 1999 to 78.7% in 2019. The official data currently released shows that in terms of quantity, petty crime cases have become the main component of criminal justice cases, and the "petty crime handling model" has gradually been recognized and improved in judicial practice.

The focus of the criminal policy of "early crackdown on petty crimes" is on "petty" and "early", which

© 2024 by the author(s); licensee Mason Publish Group, this work for open access publication is under the Creative Commons Attribution International License (CC BY 4.0). (http://creativecommons.org/licenses/by/4.0/)

means cracking down on them in the early stages of crime development. At this time, the governance of cybercrime mainly faces petty criminal cases with little social harm, and focuses on long-term and stable governance effects, rather than short-term and urgent changes. The similar criminal justice policy of "less arrest, cautious prosecution, and cautious detention" mainly targets at petty crimes. The criminal justice policy of "less arrest, cautious prosecution, and cautious detention" advocates for a specific case analysis. Based on the different situations of different cases, the social harm of relevant crimes is fully measured, and the social danger of not arresting or detaining them is comprehensively considered. Finally, the decision is made to approve arrest, detention, and prosecution or not arresting, detaining, or prosecuting. When applying the criminal policy of "early crackdown on petty crimes" in cybercrime, it is necessary to conform to the spirit of the criminal justice policy of "less arrest, cautious prosecution, and cautious detention". Specific considerations should be given to the situation exhibited by cybercrime in the primary stage, including the reasons for the crime, whether a settlement has been reached, and whether it has caused adverse effects, in order to avoid a broad scope of attack. A cautious attitude should be taken towards whether the primary stage of cybercrime constitutes a crime.

3.3 Following the Legislative Model for Criminalizing Petty Crimes in China

Adhering to the criminal policy of "early crackdown on petty crimes" is also a manifestation of following China's model of legislation for petty crimes. Throughout the eleven amendments to China's Criminal Law, the amendments have distinct features of adding new crimes and expanding the crime circle. The criminal legislation with petty crimes and the criminal justice with petty crimes as the main body have become important trends in the current criminal rule of law in China. The criminal policy of "early crackdown on petty crimes" emphasizes regulation in the early stages of crime formation. At this time, the harm of criminal behavior is relatively petty, and the criminal responsibility that the perpetrator should bear is relatively light. Sorting out the legislative trend of the Criminal Law Amendment on cybercrime, the legislation on petty crimes is currently the main mode of adding cybercrime. For example, the additional statutory penalties of such as "aiding in information network activities" and "illegal use of information networks", all of which are "less than three years". By regulating the upstream behaviors of cybercrime, such as providing Internet access, server hosting, network storage, communication transmission, and other technical assistance behaviors in cybercrime activities, based on the risk society theory, we can prevent cybercrime from further developing through these upstream preparations and assistance behaviors. We can also minimize the adverse impact and risks on society contained in the behaviors, which is in line with the connotation of the criminal policy of "early crackdown on petty crimes". This also means that the application of the criminal policy of "early crackdown on petty crimes" in cybercrime follows the petty petty criminal legislation model of China.

Of course, the expansion of legislation on petty crimes has moved the criminal law's defense against illegal acts forward, and has brought crime closer to people's lives. In order to avoid excessive interference of criminal law on people's normal life and technological development, we should approach the trend of expanding the crime circle and the legislation model of petty crimes in China with a cautious attitude, and uphold the criminal law principle of cautious and passive intervention in social governance. Similarly, in

© 2024 by the author(s); licensee Mason Publish Group, this work for open access publication is under the Creative Commons Attribution International License (CC BY 4.0). (http://creativecommons.org/licenses/by/4.0/)

the governance of cybercrime, it is not necessary to emphasize the active involvement of criminal law in cybercrime. Instead, intervention should be carried out when other departments or regulations are unable to regulate the cybercrimes. We should balancing crime governance with the protection of civil rights. We should not attend to one aspect and neglect the other and we should avoid resulting in bias.

4 The Application of the Criminal Policy of "Early Crackdown on Petty Crimes" in the Governance of Cybercrime

The application of the "early crackdown on petty crimes" criminal policy in the governance of cybercrime is in line with the basic core of "source governance" and the spirit of the criminal justice policy of "less arrests, cautious prosecution, and cautious detention". It also follows the criminal legislation model of petty crimes in China. However, criminal policy is not the legislative and judicial system itself, nor can it directly serve as a procedural or substantive law basis for conviction and sentencing. The current application of the criminal policy of "early crackdown on petty crimes" in the governance of cybercrime faces challenges in violating the principle of legality as well as neglecting the important role of other relevant systems. They need to be properly addressed, otherwise the application direction of the criminal policy of "early crackdown on petty crimes" in cybercrime governance will be deviated.

4.1 Violated the Principle of Legality

The value of criminal policies' guiding function for cybercrime relies on the legislative provisions of cybercrime. In cases where relevant legislative provisions are not clear, criminal policies play a reasonable role in guiding relevant cases. However, the guiding role of criminal policies in cases must not exceed the scope of legislation, and policies cannot replace laws. At present, there is a practice of neglecting specific legal provisions and directly targeting cybercrime with "early crackdown on petty crimes". It is over-anxious for quick results, which goes against the original intention of the criminal policy of "early crackdown on petty crimes" for guiding the governance of cybercrime. It also violates the principle of legality in criminal law. Currently, China's criminal law does not provide comprehensive provisions for all aspects of cybercrime. Therefore, caution should be taken when applying criminal policies to guide the governance of cybercrime and using criminal law to regulate cybercrime.

Specifically, taking the first maliciously faking orders case in China, "The Crime of Disrupting Production and Operation by Dong and Xie" as an example, this crime presumes that the defendants have "malice" based on the platform rules formulated by Taobao Company. The subjective existence of "malice" by the defendants are used to determine that the behavior of "faking orders" constitutes a crime, and then it is inferred that the defendants have "intention" of disrupting production and operation. This logic of sentencing the defendants to the crime of disrupting production and operation violates the principle of legality. The basis for conviction in the sense of criminal law is not a document rule formulated by private entities, unofficial entities, etc., but should be a clear provision of legislation. It is not possible to infer objectively whether an act is illegal and whether it constitutes a crime based solely on whether it belongs to "malice" subjectively. Instead, it should infer subjectively whether there is "intention" in the sense of criminal law

© 2024 by the author(s); licensee Mason Publish Group, this work for open access publication is under the Creative Commons Attribution International License (CC BY 4.0). (http://creativecommons.org/licenses/by/4.0/)

based on whether the act itself meets the objective elements of a crime, and whether it constitutes a crime. Otherwise, there is a suspicion of breaking the principle of legality.

4.2 Neglecting the Important Role of Other Relevant Systems

The "source governance" policy focuses more on exploring the causes of crime, emphasizing the identification of the "root cause" of the problem for "radical treatment". Due to the diverse causes of crimes, the unclear nature of the causes, and human cognition limitation, the process of "eradicating" crime is a long process, and it should not be over-anxious for quick results. Criminal law has a humble nature and is not a "universal" means of governance, nor should it overly intervene in all aspects of human society. Criminal law is only one of the means to comprehensively and fundamentally govern cybercrime, rather than the only "weapon". The criminal policy of "early crackdown on petty crimes" is an effective means to cooperate with "source governance". Under the guidance of the criminal policy of "early crackdown on petty crimes", the governance of cybercrime should comprehensively consider the application of relevant systems.

Compared to real activities, online activities have special characteristics. The interactivity of online behavior, the wide range of behavioral influences, the diversity of interactive subjects, and the fast transmission efficiency make the process of online behavior from beginning to end take less time. It is not feasible to use the strictest criminal law to strictly regulate it, or the criminal law may lose its deterrent power and humility. Citizens do not learn professional codes seriously before engaging in related online activities in their daily online lives. More citizens rely on simple moral values to act in online life. Therefore, some scholars suggest that a "normative group" should be formed by platform rules and legal norms such as civil law, commercial law, economic law, and administrative management law to provide specific behavioral guidance for online activities. Multiple arbitrary or mandatory solutions such as comprehensive technical governance, industry ethics, administrative management, and legal rules should all be taken into account. This will provide citizens norms in engaging in online activities, so that they will not feel "trembling" or "walking on thin ice" when they are using online platforms.

5 The Application Path of the Criminal Policy of “Early Crackdown on Petty Crimes” in the Governance of Cybercrime

The criminalization of criminal policy should always adhere to the principle of legality. The criminalization of criminal policy at the judicial level should also follow the criminalization at the legislative level. Therefore, the application of the criminal policy of "early crackdown on petty crimes" in the governance of cybercrime should be within the framework of criminal law legislation, to avoid including numerous illegal but non-criminal online behaviors in the scope of criminal law regulation, thereby undermining the humility of criminal law and affecting the normal participation of the public in online activities, as well as the development of information technology. Therefore, the application path of the "early crackdown on petty crimes" criminal policy in the governance of cybercrime should follow the principle of legality in criminal law, and build a diversified governance system for cybercrime, in order to achieve the reasonable effect that is initially envisioned by the "early crackdown on petty crimes" criminal policy in the governance of cybercrime.

© 2024 by the author(s); licensee Mason Publish Group, this work for open access publication is under the Creative Commons Attribution International License (CC BY 4.0). (http://creativecommons.org/licenses/by/4.0/)

5.1 Adhere to the Principle of Legality in Criminal Law

To avoid "deviating from the legal track", the application of the criminal policy of "early crackdown on petty crimes" in the governance of cybercrime should be fully based on the law. The criminal policy of "early crackdown on petty crimes" can only confirm the basic principle of strict punishment, and specific punishment still needs to be achieved through criminal law. Additionally, it is necessary to avoid the alienation of the criminal policy of "early crackdown on petty crimes" in the governance of cybercrime due to the pressure of rigid target, so as to mistakenly treat illegal acts that do not constitute crimes as criminal acts. Otherwise, it will finally result in an unreasonable and too broad scope of punishment. When implementing criminal policies, one should not artificially elevate or rush for success. We should follow the relevant development laws of cybercrime, combine the characteristics of cybercrime, avoid using policies as a direct substitute for laws as the basis for cracking down cybercrime, adhere to the principle of "cracking down according to law", and finally promote the application of "early crackdown on petty crimes" criminal policy orderly and steadily on the track of the rule of law in the governance of cybercrime.

At the same time, following the principle of legality means that criminalization of one illegal behavior needs to be objectively and subjectively unified, and the behavior must meet both formal and substantive standards to be recognized as a crime. In the case where the behavior meets the formal criminalization criteria in the sense of criminal law, it is still necessary to make substantive judgments on whether there is legal interest infringement and the magnitude of legal interest infringement. When substantively identifying an online behavior, it should be fully recognized that the existence of legal interest damage does not definitely constitute a crime. The infringed legal interest must be protected by criminal law and the infringement needs to reach the level of punishment, in order to constitute a cybercrime. For example, in the guiding case of "Illegally Controlling Computer Information Systems by Zhang Junjie and Others" issued by the Supreme People's Court, it points out that modifying or adding computer information system data and implementing illegal control behavior on the computer information system should only be recognized as the crime of damaging the computer information system if it causes substantial damage to the system function or make the system cannot operate normally. Cybercrime can only be established when the unity of formal illegality and substantive illegality is met.

5.2 Structure a Diversified Governance System for Cybercrime

Giving full play to the post governance role of judicial authorities in cybercrime, clarifying the standards for conviction and punishment of cybercrime, strictly regulating the legal framework for upstream and downstream behaviors of cybercrime, and implementing legal conviction and punishment for cybercrime offenders are beneficial to regulating cybercrime to a certain extent. However, their governance effectiveness is extremely limited and requires significant judicial costs. Therefore, exploring the diversification of governance mechanisms for cybercrime, actively building a diversified governance system for cybercrime, paying more attention to the social supervision, platform supervision and other means in the primary stage of preventing and controlling cybercrime, and playing the role of prior supervision and in-process supervision are very important.

© 2024 by the author(s); licensee Mason Publish Group, this work for open access publication is under the Creative Commons Attribution International License (CC BY 4.0). (http://creativecommons.org/licenses/by/4.0/)

From the perspective of network governance entities, administrative regulatory agencies, private network platform regulators including e-commerce platforms, operators, and so on, and netizens can all become participants in network governance. For example, in response to malicious false orders and transactions, the Taobao platform will take measures such as manual and system troubleshooting to monitor abnormal transaction data. The system will analyze the predetermined program logic to determine whether it belongs to malicious false orders and transactions. Afterwards, temporary or permanent penalties will be imposed on sellers or participating buyers, such as delisting products, searching for lottery tickets, not accumulating sales, restricting the use of Alibaba Wangwang, resetting credit points, and restricting member login, in accordance with the "Taobao Market Management and Violation Regulations" and "Taobao Implementation Rules for False Transactions". Netizen supervision is also an important part of building a diversified governance system for cybercrime. Netizens are direct participants and viewers in online life. Improving the supervision system for netizens, as well as improving feedback and reporting channels for netizens, are also effective means of cracking down on cybercrime. Additionally, some scholars believe that losses can be borne by the one with the lowest cost of loss prevention. Undoubtedly, in the implementation of cybercrime based on online platforms, it is a relatively direct means for the platform to implement preventive measures. However, due to the rapid development of information technology, the complex and diverse network environment, the large number of network participants, and the anonymity inherent in the network, the governance responsibility of the platform should not be overly demanding. It is possible to establish a reasonable responsibility system for minimizing network platform control damage. The system should consider about the existing funds and technological level of the platform party that can support it without affecting the platform's normal operation and development. Specific policies should be used to encourage platform operators and regulators to improve relevant regulatory technologies, timely detect illegal behaviors based on the network, and regulate them. By integrating various reasonable means, fully mobilizing the enthusiasm of all sectors of society to participate in governance, calling for multi-party supervision to achieve early detection and governance of cybercrime. At the same time, we should also adhere to the dominant position of national governance. With the state holding the correct direction of governance development, the main role of organizations and institutions at all levels of society in implementing the criminal policy of "early crackdown on petty crimes" in the governance of cybercrime can fully leverage, and a dual standard of criminal policy model for both the state and society can be constructed.

From the perspective of network governance norms, in addition to criminal regulations, consideration should also be given to comprehensive governance in conjunction with other non-criminal, non-punitive, preventive, and restorative measures. It is important to utilize diverse measures and avoid fully incorporating the governance of illegal online behavior into the scope of criminal law norms, in order to maintain the modesty of criminal law and protect the stable development of the network. At the same time, based on the causes and sources of cybercrime, a comprehensive governance system can be formed around the black market chain related to cybercrime, consisting of prevention and control measures of different levels and effectiveness. Reasonable application and in-depth implementation of relevant criminal policies will be carried out, and criminal law with humility, compelling force, and deterrence will be used as supplementary measures. Normative adjustment measures, as well as education, correction, compensation, mediation, and

© 2024 by the author(s); licensee Mason Publish Group, this work for open access publication is under the Creative Commons Attribution International License (CC BY 4.0). (http://creativecommons.org/licenses/by/4.0/)

other flexible adjustment measures can be comprehensively applied for cybercrime governance, in order to promote the construction of a diversified governance system for cybercrime.

References

[1]Qi Wenyuan. (2022). Application and Reflection on the Policy of Early Cracking down on Petty Crimes under the Background of "Less Arrest, Caution in Prosecution, and Caution in Detention"- From the Perspective of Cybercrime Governance. Political and Legal Forum, 2022(2), 62-69.
[2]Otani Shih. (2009). Criminal Policy (New Edition), Beijing: Renmin University of China Press.
[3]Yoichi Morita. (2004). Criminal Policy, Beijing: People's Public Security University of China Press.
[4]Klaus Roksin. (2011). Criminal Policy and Criminal Law System (Second Edition), Beijing: Renmin University of China Press.
[5]Luan Li. (2020). Research on the Legalization of Criminal Policy of "Early Crackdown on Petty Crimes" in the Fight against Black and Evil. Public Security Research, 2020(5), 42-53.
[6]Luo Duo. (2014). Reflection on the Application of the "Early Crackdown on Petty Crimes" Policy in Crime Involving Black and Crime. Journal of Jiangxi Police College, 2014(4), 39.
[7]Mikhail Delmas Mati. (2000). The Main System of Criminal Policy, Beijing: Law Press.
[8]Liu Xianquan. (2021). Criminal Law Regulations on Upstream Crimes of Cyber Black Market. Journal of the National Institute of Prosecutors, 2021(1), 5.
[9]Yu Chong. (2023). Criminal Law Evaluation of Internet Aggregated Insult and Defamation Behavior. China Legal Review, 2023(3), 88.
[10]Chu Chencheng. (2018). The Position and Function of Criminal Law in the Era of Artificial Intelligence. Chinese Journal of Criminal Law, 2018(6), 80.
[11]Zhuang Yonglian, Sun Changyong, Miao Shengming, Peng Shengkun, and Chang Feng. (2021). The Connotation, Function, and Implementation of the Criminal Justice Policy of Less Arrest, More Prosecution, and More Detention. People's Procuratorate, 2021(15), 40.
[12]Yuhuatai District People's Court of Nanjing City (2015) No. 29 Criminal Judgment of Yuxing Erchu Zi.
[13]Ji Yang. (2020). Judicial Misunderstandings of the "Source Governance" Policy of Cybercrime. Political and Legal Forum, 2020(6), 70.
[14]On December 31, 2020, the Supreme People's Court issued a notice on the release of the 26th batch of guiding cases (Guiding Case No. 145 • Zhang Junjie et al. Illegal Control of Computer Information Systems Case).
[15]Qi Wenyuan, Yang Liu. (2017). Criminal Law Regulations on Network Platform Providers. Legal Science (Journal of Northwest University of Political Science and Law), 2017(3), 114.

© 2024 by the author(s); licensee Mason Publish Group, this work for open access publication is under the Creative Commons Attribution International License (CC BY 4.0). (http://creativecommons.org/licenses/by/4.0/)