DOI: 10.37420/j.mlr.2023.015

The Legal Governance on Cybercrime through the Lens of Positive Criminal Law

Gao Erqi
Law School, Beijing Foreign Studies University, Beijing, China
Corresponding author, e-mail: gaoerqi@bfsu.edu.cn

Abstract

At present, the number of cybercrime is gradually increasing, and the forms of cybercrime are also constantly updated, which accelerates the development of cybercrime. Striving for security and stability in modern social governance continues to evolve and be challenged. In response, the positive view of criminal law is to prevent in advance, criminal legislation has become increasingly active, criminal law has become more proactive and the penalties for crime have become more severe. In the light of this legislative philosophy, in order to obtain the ideal effect of punishing crimes and protecting legal interests, it is necessary to control the boundaries of the application of the positive view of criminal law, and it is also necessary for law enforcement and the judiciary to cooperate in the practical implementation of legislation. This article focuses on the legal governance of cybercrimes in the light of the current concept of positive criminal law from three aspects: crimes involving network infringement of citizens' personal information, crimes that impede the order of information network management, and crimes related to Internet finance.

Keywords

The positive view of criminal law; Cybercrime; Legal governance

Introduction

In today's society, driven by the rapid development of Internet technology and the rapid pace of economic and social progress, risks are gradually increasing. Cases of moral misconduct in social life are on the rise, prompting criminal law to become more proactive in the management of social security and to place more emphasis on forward-looking criminal protection. As a result, the nature of criminal punishment has evolved from being primarily an after-the-fact measure to an effective tool for preventing crime in advance1. Positive prevention has become a clear trend in contemporary criminal legislation. Acts such as the enactment and implementation of the Amendment (XI) to the Criminal Law in China embody the legislative realization of this positive and preventive concept in criminal law. This represents a significant shift in criminal legislation, promoting a proactive and preventive approach to enhance social security.

The positive and preventive view of criminal law is reflected in both the substantive area of criminal law and the area of criminal law and punishment. In the substantive area, it is manifested mainly through conviction and sentencing, while in the area of punishment, it is manifested mainly through the aggravation of penalties. Moreover, the "positive preventive view of criminal law" applies mainly to offences that exceed individual or collective legal interests2, including the following eight types of criminal acts. First, terrorist crimes,

such as the complicity and preparatory acts of terrorism are all criminalized, and preparatory planning acts are criminalized3; second, cybercrime, cyberviolence will be severely punished in accordance with the law, focusing on the malicious initiators, organizers, malicious promoters and persistent offenders4; third, bribery crimes, Thirdly, bribery offences, China's bribery offence punishment strategy has experienced a historical evolution from "active and passive bribery and combined penalties" to "emphasis on passive bribery and light active bribery", and then gradually to "active and passive bribery and heavy penalties"5; Fourthly, food and drug criminal offences, such as Amendment (VIII) to the Criminal Law, have increased the strength of the fight against food and drug crimes, highlighting the determination of the Central Government to highly punish food and drug crimes, but the situation of food and drug crimes in practice is still grim6; Fifthly, environmental crimes, since the 1997 Criminal Law provides for environmental resource crimes, the Criminal Law Amendment (IV) and Criminal Law Amendment (VIII) have expanded the scope of punishment for environmental crimes from the level of criminal legislation, and the crime of polluting the environment has reflected the earlier criminal law punishment7; Sixth, public order criminal offences, such as the addition of the offence of fabricating and intentionally disseminating false information in Amendment (IX) to the Criminal Law8; Seventh, the obvious expansion of unit criminal offences, the significant expansion of the scope of unit subject offences in all criminal law offences, and the organizational supervision and control mechanism for the prevention of internal criminal offences (compliance plan) of enterprises cut into the determination of criminal liability and prosecution of unit subjects9; eighth the marked increase in criminal offences of omission, in the area of cybercrime, Amendment (IX) to the Criminal Law added the offence of assisting criminal activities in the information net, reflecting the transformation of China's criminal legislation from passive general prevention to active general prevention10. This paper focuses on the current situation of several types of cybercrimes and their governance under the positive view of criminal law.

1.Trends in the development of cybercrime and problems under a positive criminal law perspective

The Internet's inception is a mere few decades old, and the market-driven adoption of this technology is even more recent. However, the advancement of emerging technologies such as cloud computing, artificial intelligence, big data analysis, and the Internet of Things, along with the ever-expanding market for smart devices, has led to a gradual increase in cybercrimes. The methods of cybercriminals are continually evolving, propelling cybercrime into a rapidly developing field.

Within the realm of cybercrime, there are three overarching trends. Firstly, the proliferation of malicious ransomware in the online environment has led to more frequent and severe network attacks. The interconnected nature of our digital infrastructure has lowered the barriers to attacking critical information systems, intensifying the associated risks. Secondly, cybersecurity is no longer solely concerned with safeguarding the integrity of network infrastructure. It now encompasses the vast volume of information and data present in cyberspace, leading to significant incidents of data breaches. This has raised the stakes for national security as it faces increasingly severe challenges. Lastly, the integration of new technologies such as artificial intelligence and blockchain in cybercrime has given rise to novel methods and heightened risks in the digital landscape.

Under the positive view of criminal law, as the trend of cybercrime intensifies, criminal law further extends the scope of criminal categories, broadens the range of criminal activities, and exhibits a clear tendency towards proactive measures. Simultaneously, criminal law places greater emphasis on the lawful interests of

the public and society, actively engaging in social management with a focus on pursuing national security and social stability11. Some scholars have argued that caution should be exercised in this transformation of criminal law and have expressed opposition to excessive criminalization12; Some scholars also argue that the criminal policy orientation of criminal law is an important trend in the legislative practice of various countries today13. In fact, while the positive view of criminal law aligns with the spirit of the times, at the same time, criminal law should also maintain a certain level of restraint and modesty. It should deter criminal behavior through proportionate penalties without excessively expanding the scope of its application or the severity of punishments. This article primarily explores the legal governance of cybercriminal behavior under the positive view of criminal law, focusing on three aspects: crimes involving the infringement of citizens' personal information through the internet, crimes disrupting the order of computer information management, and internet-based financial crimes.

2. Legislative Evolution and Judicial Status of Cybercrimes under the Positive View of Criminal Law

2.1Cybercrimes involving the infringement of citizens' personal information under the positive view of criminal law

With the rapid development of information network technology, the internet has gradually become the most common and widespread medium for carrying citizens' personal information. The collection, processing, and exchange of citizens' personal information all rely on the convenience of the internet. At the same time, there is a growing trend in cybercrimes involving the infringement of citizens' personal information. These types of crimes are characterized by the diversity of personal information involved and their wide-ranging impact. Information like identity details, phone numbers, home addresses, as well as privacy-sensitive data such as mobile phone information, online account passwords, shopping records, travel histories, and even lifestyle habits all fall within the category of personal information that can be compromised.

Even worse, the sources of information leakage are diverse, including hacker attacks, phishing websites, free Wi-Fi, counterfeit QR codes, and more. Criminal organizations often have a strong counter-surveillance awareness, significantly increasing the risk of citizens' personal information being compromised14.

In this context, under the positive view of criminal law, China's legislative activities concerning cybercrimes involving the infringement of citizens' personal information have gradually become more detailed and stringent, expanding the scope of protection for citizens' personal information.

The scope of cybercrimes involving the infringement of citizens' personal information is extensive and encompasses more than 40 sectors and industries, including education, healthcare, commerce, finance, telecommunications, real estate, and many others. Under the positive view of criminal law, China's Criminal Law has provided corresponding regulations in this regard. In 2009, the "Amendment to the Criminal Law (VII)" introduced, for the first time, the offenses of "selling or illegally providing citizens' personal information" and "illegally obtaining personal information" into the Criminal Law, thus incorporating the protection of citizens' personal information as a legal safeguard. In 2015, the "Amendment to the Criminal Law (IX)" consolidated these two offenses into a single crime known as "infringement of citizens' personal information"15. Subsequently, the "Provisions on Several Issues Concerning the Application of Law in Handling Criminal Cases of

Infringement of Citizens' Personal Information" were promulgated and implemented. Citizens' personal information was explicitly defined as "any information that can identify a citizen's identity or activities, including information that can be identified individually or in combination." Since then, the protection of citizens' personal information has extended to encompass not only basic identity information such as name and gender but also information related to citizens' daily activities, such as travel records16, which essentially protects citizens' personal privacy even further. With the development of the internet, there has been a continuous increase in the nation's attention to the protection of citizens' personal information. This is evident in criminal legislation, where there is a consistent implementation of the positive view of criminal law.

Furthermore, the "Amendment to the Criminal Law (VII)" stipulated that if the perpetrator violated only local regulations or departmental rules concerning the protection of citizens' personal information, rather than "national regulations," it would not constitute a criminal offense. This provision had a narrow scope and was not conducive to the protection of citizens' information. Subsequently, the "Amendment to the Criminal Law (IX)" extended the term "violating national standards" to "violating relevant national provisions" and made timely supplements to the content related to crimes involving citizens' personal information from the "Amendment to the Criminal Law (VII)." The later "Provisions" stated that violations of national laws, local administrative regulations, and departmental rules regarding the protection of citizens' personal information should be included within the scope of "violating relevant national provisions." Consequently, both national-level regulations regarding citizens' personal information and non-national-level regulations, such as local administrative regulations, are considered as "violating relevant national provisions." From a legislative perspective, starting from the "Amendment to the Criminal Law (VII)" to the "Amendment to the Criminal Law (IX)" and then to the "Provisions on Several Issues Concerning the Application of Law in Handling Criminal Cases of Infringement of Citizens' Personal Information," the legal basis for safeguarding citizens' personal information will be further refined. The scope of "citizens' personal information" will be expanded, leading to more comprehensive protection of citizens' personal information.

Maintaining online order, ensuring cybersecurity, and enforcing the law rely on law enforcement agencies. In 2021, a special operation named "Clean the Internet 2021" was led by China's public security departments. They carried out comprehensive and in-depth investigations and enforcement activities, grouped and classified according to significant issues related to the protection of Chinese citizens' information. They successfully cracked more than 9,800 cases of infringements on people's information and arrested over 17,000 criminal suspects17. Meanwhile, the Chinese Ministry of Public Security recently released ten typical cases of crimes involving the infringement of citizens' information in China in 2021. Among these cases, the Anhui Public Security department successfully cracked down on the "case of Wu and others illegally obtaining information from the elderly and selling counterfeit health products," the Fujian Provincial Public Security department, under the leadership of Xie and others, solved the "case of using Trojan horses to steal online shopping information from netizens," and the Liaoning Provincial Public Security department, led by Shi and others, apprehended those involved in the "case of illegally acquiring citizens' personal information to register online gaming accounts and selling them to minors." These actions represent a stern crackdown on the current prevalent methods of using the internet to disseminate crimes that infringe upon citizens' information.

Under the positive view of criminal law, judicial authorities have shown a proactive shift in their approach to crimes involving the infringement of citizens' personal information through the internet. Judicial authorities now place greater emphasis on personal information protection and impose stricter criminal penalties to safeguard citizens' privacy and data security. This reflects the society's heightened concern for personal infor-

mation protection and is also a necessary response to the new challenges posed by the digital age. However, in recent years, judicial authorities have faced challenges in handling cases involving the infringement of citizens' personal information, including a lack of understanding among investigators about emerging internet technologies and the methods employed by cybercriminals18. Balancing criminal prosecution and prevention is of paramount importance for enhancing public security and instilling a sense of safety in the community. With proactive criminal legislation in place, law enforcement agencies responsible for internet security should collaborate with relevant authorities to diligently implement regulations such as the Personal Information Protection Law and the Data Security Law. The judicial authorities should ensure impartial enforcement of the law to continually establish and improve the legal framework for combating unlawful crimes that threaten citizens' information and personal safety.

2.2 cybercrimes disrupting information network management order under the positive view of criminal law

In this context, crimes disrupting information network management order primarily refer to offenses related to the failure to fulfill information network security management obligations, unlawful exploitation of information networks, and aiding activities related to information network crimes. In recent years, legislators have adopted a "strike early and strike small" approach, focusing on cracking down on aiding behaviors. Aiding behaviors have been criminalized, and they no longer require reliance on principal offenders to be separately convicted19. Additionally, preparatory actions have been formalized, reflecting a form of expansion in criminal law. The "Criminal Law Amendment (IX)" introduced Articles 286-1, 287-1, and 287-2, specifying offenses related to the failure to fulfill information network security management obligations, unlawful exploitation of information networks, and aiding activities related to information network crimes. The legislation for these three offenses is a targeted response to the current state of cybercrimes.

When analyzing the deleterious effects of this category of criminal conduct, it is imperative to recognize that the modus operandi of such crimes yields consequences of exponential significance. We must refrain from evaluating individual criminal acts in isolation from their specific method and instead consider them as integral components of the overall criminality, taking into account the recurrent and extensive utilization of information networks20.

The establishment of the crime of "refusal to fulfill obligations in information network security management" represents an elevation and criminalization of joint civil liability for internet service providers. The establishment of the offense of "refusal to fulfill obligations in information network security management" represents an elevation and criminalization of joint civil liability for internet service providers. The introduction of an "order to rectify" administrative pre-procedure signifies that actions of non-compliance with information network security management obligations beforehand do not constitute a criminal offense. It is only when an individual or entity receives an "order to rectify" notice but refuses to rectify the situation, resulting in the expansion of harm or the occurrence of severe consequences, that a criminal offense is established. This approach aims to strike a balance between safeguarding innovation in internet technology and maintaining network security while limiting the scope of criminal law penalties. It exhibits a certain degree of reasonability21. The establishment of the crime of illegal use of information network, which independently criminalizes the use of information network to set up websites and communication groups for the purpose of committing unlawful criminal activities, publish unlawful criminal information and publish information for the purpose

of committing unlawful criminal activities, is the implementation of preparatory acts and the attempt of attempts, and the crime is also likely to become the "underpinning crime" of information network crimes in the future.

The establishment of the offence of assisting criminal activities in the information network is the criminalization of the act of helping or the criminalization of the act of helping, and the establishment of this offence presupposes that the object of assistance has begun to commit a criminal activity in the information network, but it does not require that the degree of the offence be reached, which is also a manifestation of the positive view of criminal law.

Furthermore, the introduction of the offense of "Aiding Information Network Criminal Activities" involves transforming those aiding or abetting individuals into principal offenders or facilitating the execution of aiding actions. To establish this offense, it is a prerequisite that the aided party has initiated information network criminal activities, but it does not require the realization of a threshold level of criminality. This aligns with the principles of the positive view of criminal law.

In theory, these three offenses structurally differ. The offense of "Failure to Fulfill Information Network Security Management Obligations" constitutes a nonfeasance crime, characterized as a passive form of criminal liability. With regard to the legally defined societal harm outcomes, the offender does not hold a hopeful subjective attitude. The establishment of this offense as a charge is contingent on the violation of relevant national laws and regulations. The accumulation of societal dangers and harmful facts must satisfy higher legal conditions for the offense to be established. Both "Illegal Exploitation of Information Networks" and "Aiding Information Network Criminal Activities" are intentional offenses, possessing an active criminal behavior structure. All three offences are assisting, preparatory offences for upstream and downstream offences.

From the research findings, it is evident that there is a lack of clarity in the conviction and sentencing standards for the offenses of "Refusal to Fulfill Information Network Security Management Obligations," "Illegal Exploitation of Information Networks," and "Aiding Information Network Criminal Activities." Ambiguities persist regarding the scope of internet service providers, the determination of non-compliance when ordered by government authorities to rectify, the interpretation of "unlawful criminal activities" in the context of "Illegal Exploitation of Information Networks," and the distinction between "crime" and "aiding in information network criminal activities" in the offense of "Aiding Information Network Criminal Activities." These legal application issues have sparked significant disputes and require clarification through judicial interpretations22. Such clarity is urgently needed to comprehensively address the challenges faced in practical law enforcement and enhance the effectiveness of combating these offenses.

2.3 Internet financial crimes under the positive view of criminal law.

Leveraging modern digital information technology, internet finance has experienced rapid growth in recent years. From payment and settlement products typified by Alibaba's Alipay, to deposit and asset products represented by Yu'EBao, and ultimately the emergence of financing and lending financial products with P2P lending as a prominent example, internet finance has progressively penetrated the core of traditional financial services and is increasingly challenging the conventional financial sector23. Currently, the development of the internet finance industry can be broadly categorized into several types. Payment and settlement products include offerings such as Alibaba Group's Alipay and Tencent's TenPay. Investment products encompass platforms like PPDAI, and there are virtual currency products like Bitcoin. Additionally, there are wealth man-

agement products such as Yu'EBao.

The most significant difference between internet finance and traditional finance lies in its reliance on network technology-based big data analysis and statistical algorithms. Internet finance combines the advantages of speed, efficiency, and cost reduction while exhibiting characteristics of being off-market, involving multiple parties, and blurring boundaries. It can transcend the limitations of traditional finance and cater to the interests of a broad consumer base. Through this new model of serving the public, it can effectively lower the entry barriers for investors and optimize the allocation of financial market resources to the maximum extent24. This represents a key new area for "financial inclusion" and market-oriented development.

However, while internet finance promotes financial innovation, it can also give rise to a series of internet financial crimes and their dissemination. In the realm of internet financial services, the most likely risks include, firstly, the criminal hazards arising from operating internet financial services themselves. This primarily encompasses crimes explicitly stipulated in Chapter Three of China's Criminal Law, such as fundraising fraud, illegal acceptance of public deposits, and illegal operations. Secondly, risks arise from the use of internet financial services as tools for engaging in illicit criminal activities, including money laundering and embezzlement.

In the current societal context, issues related to internet financial crime, the scale of internet financial risks, and the impact of internet financial crimes have become quite prominent, significantly affecting the stability of our society. It is worthwhile to conduct in-depth research on regulating internet financial crimes through the lens of the positive view of criminal law. Particularly, speculators operating within this decentralized environment, driven by limited knowledge and the allure of high external returns, often tend to overlook investment risks. In the era of widespread participation in the internet financial market, irrational investor behavior can make them more sensitive to fluctuations in the financial market and more vulnerable. Such individual behavior can easily escalate into larger-scale, more influential societal panics25.For instance, crowdfunding models like "Shuidichou" have a broad audience, and any issues that arise can have a substantial negative impact.

Therefore, it is necessary to take proactive measures to prevent and harshly combat internet financial crimes. This includes addressing illegal fundraising cases with a massive number of potential victims, such as P2P lending platform collapses and sudden disappearances of lending platforms. In such cases, active criminal legislative intervention is essential. Without such intervention, both social stability and citizens' sense of security would be significantly compromised.

Some scholars argue that within China's criminal law framework, financial penalties, primarily in the form of fines, play a central role in addressing internet financial crimes. These fines are often based on monetary value, with the crime's magnitude serving as a measure. Internet financial crimes typically involve significant sums, and imposing fines alone does not provide a sufficient deterrent. It becomes challenging to achieve the goal of preventing such crimes26. Therefore, the addition of measures such as criminal occupational prohibitions within the governance of internet financial crimes is necessary to enhance deterrence. This aligns with the principles of the positive view of criminal law.

China is currently in a phase of high-quality economic development, and criminal activities, as well as methods, have become more complex compared to the era of traditional criminal law. Internet crimes have become a common means of illegal activities. The positive view of criminal law is well-suited to address these challenges and reflects the adaptability and flexibility of China's criminal justice system. Whether through legislative or judicial measures, the positive view of criminal law plays a crucial role in the practical fight against

criminal activities within internet financial institutions.

3. Legal governance of cybercrime under a positive criminal law perspective

With the rapid development of internet and digital technologies, the internet has evolved beyond being merely the object and tool of criminal activities; it has gradually transformed into a criminal space. Online criminal activities have gained an increasing share, and due to the large amounts of wealth and economic crimes involving internet properties, as well as the substantial number of individuals involved, criminal justice agencies must invest more effort and attention in the punishment of internet crimes. This also requires investigative departments and personnel to possess advanced skills, rich professional knowledge, and flexible ways of thinking.

Under the positive view of criminal law, legislation related to internet crimes is becoming increasingly comprehensive and systematic. However, the core challenge lies in the synchronization of enforcement and judicial departments with the legislative process, ensuring that they can better combat crime and protect legal interests. The following three aspects explore the legal governance of internet crimes under the positive view of criminal law.

3.1 Regularly Review Cybercrime-Related Laws to Address Emerging Threats

Cyber threats are constantly evolving, and the law should keep pace with these changes. It is essential to ensure that the legal framework remains flexible enough to adapt to the ever-changing forms of cybercrime and technology. Legislative bodies should have a forward-looking perspective, anticipating or identifying potential types of crimes, conducting regular reviews, and updating cybercrime laws to effectively address emerging threats.

Simultaneously, legislative bodies should provide clear definitions of cybercrimes, criminal responsibilities, the limits of penalties, and delineate the powers of various regulatory authorities, including law enforcement agencies, regulatory bodies, and relevant industry associations. Establishing interdepartmental cooperation mechanisms and defining their respective responsibilities is crucial to ensure information sharing and coordinated actions.

Furthermore, legislative bodies should take into account that cybercrimes often involve activities that cross national borders. Therefore, international cooperation is essential. Establishing international cooperation mechanisms and collaborating with other countries and international organizations to combat cross-border cybercrime and share information and intelligence are crucial steps.

3.2 Enhancing the Supervision of the Entire Process of Implementing Technical Investigation Methods

Law enforcement agencies should strengthen technical surveillance methods, particularly throughout the entire process of developing, marketing, and using illegal information technology software. They should crack down severely on aiding activities within various criminal chains. Special emphasis should be placed on intensifying efforts to combat and prevent the use of illegal information technology to lure minors into participating in internet-related criminal activities. This is crucial for effectively controlling the trend of internet

crimes becoming more juvenile. Departments responsible for intellectual property protection, cybersecurity, and data protection should monitor software developers' actions through network surveillance. They should enforce relevant laws and regulations related to cybercrimes, requiring entities that develop and sell software to obtain permits or go through an approval process. This is to ensure that software developers comply with legal requirements, including those related to intellectual property protection and data privacy.

Furthermore, law enforcement agencies can establish reporting mechanisms to encourage the public and insiders to report internet criminal activities, which can help law enforcement agencies gather leads. It's important to note that law enforcement agencies need to possess sufficient technical capabilities to effectively process and analyze large-scale data. This might require investments and training. Additionally, when collecting, storing, and analyzing vast amounts of data, strict adherence to data privacy regulations is essential to prevent the misuse of personal information and privacy infringements.

3.3 Strengthening Comprehensive Determination of Cybercrime Evidence

In cases of cybercrime, the sheer volume and dispersion of evidence mean that it is prohibitively costly, if not practically impossible, for law enforcement agencies to collect comprehensive evidence for proof, particularly the corroboration of case facts. If judicial authorities insist on adhering to high traditional standards for criminal evidence, requiring verification and corroboration of each element of evidence, it will undoubtedly encourage criminals. This is the primary reason for the low conviction rates in the prosecution of such crimes. New forms of cybercrimes, especially those involving multiple individuals, are characterized by the abundance and dispersion of evidence27. This evidence may be scattered across various physical locations within and outside the country and may also be stored on different online platforms. Faced with this practical challenge, relevant judicial interpretations and other normative documents have specifically provided alternative methods known as comprehensive determination. Comprehensive determination refers to the assessment of overall facts in cases where it is challenging to collect all the necessary evidence for corroboration. This involves evaluating evidence that partly corroborates the facts at hand and other evidence that, while verified, has not necessarily resulted in corroboration.

By appropriately reducing the qualitative evidence standards and adopting a comprehensive determination approach for a quantity of criminal cases, it is possible to effectively overcome the challenges of producing vast amounts of evidence, expedite the case handling process, and respond more quickly to cybercrime. This approach enhances the applicability and effectiveness of the law, allowing law enforcement agencies to more effectively track and combat cybercrime, preventing criminal actions. This method can contribute to more effective legal governance, but it should be implemented cautiously to balance legal fairness and individual rights.

However, it's essential to note that due to the current regulations containing extremely concise and abstract provisions regarding comprehensive determination, various issues have arisen in judicial practice, including unclear conditions of use, expanded application, and lowered statutory evidence standards28. The judicial evidence mechanism for cybercrime still requires ongoing optimization.

4. Conclusion

In the rapidly evolving landscape of the internet, new forms of cybercrime are continually emerging, posing an increased threat to society. Cybercriminal methods are versatile, their activities have long chains, and the complexity of charges compounds the challenges. The criminal justice system for cybercrime is still in the

process of development, leading to legal discrepancies in the application of the law. In light of the previous analysis, it is essential for criminal legislation and criminal justice to adopt a proactive view.

In the substantive and punitive domains of criminal law, legislative bodies should regularly review cybercrime-related laws to address emerging threats in the field of cybercrime. Law enforcement agencies must strengthen technical investigative methods and conduct comprehensive supervision of the entire process of cybercriminal activities. Judicial authorities should enhance the comprehensive determination of cybercrime evidence.

However, the proactive view is not universally applicable and should adapt as society evolves. In specific cases or with the progression of a more civilized society where the social harm or crime rate of certain offenses decreases, criminal justice should also be appropriately more lenient. Nonetheless, adopting a proactive view is of paramount significance in addressing and preventing current cybercrime issues, especially in the backdrop of the substantial growth in cybercrime within the digital realm. The research on the legal governance of cybercrime should not be confined solely to theoretical discussions but must also integrate the existing state of judicial practice, responding to real-world challenges. It is only through this approach that we can genuinely provide the necessary support for resolving the novel criminal problems brought about by the evolution of the internet.

References

[1] Zhang, M. (2020). The Concept of Introducing New Crimes - Support for the Positive View of Criminal Law. Modern Law, 5, 150.

[2] Gao, M., & Sun, D. (2018). The Preventive View of Criminal Law and Its Doctrinal Thinking. Chinese Legal Science, 1, 168.

[3] Mei, C. (2016). Review and Improvement of China's Counter-Terrorism Criminal Legislation - An Evaluation of the Relevant Terrorism Clauses in the Ninth Amendment to the Criminal Law. Modern Law, 1.

[4] Xie, J. (2023). Strictly Punishing Cyber Violence and Correcting the Wrong Tendency of "Legal Immunity." People's Public Security Daily.

[5] Chen, J., & Zheng, H. (2023). Model Selection and Legislative Shaping of Bribery Crime Control Strategy. Journal of Politics and Law, 3, 73-83.

[6] Fu, Y. (2023). Prevention and Governance of Crimes in the Field of Food and Drug - Based on the Sample of Judicially Concluded Cases in City F of Province G in the Past Seven Years. Journal of Heilongjiang Provincial Institute of Political Science and Law, 4, 31-37.

[7] Wang, Q. (2023). The Expansion and Limitation of Punishment Range in the Period of Transformation of Environmental Crimes. Law Studies, 8, 59-71.

[8] Yu, B. (2022). Criminal Regulation of Public Order Disturbing Rumors on the Internet. Journal of Taishan University, 2, 70-78.

[9] Zhao, C. (2022). Unit Crime Structure and Path of Corporate Criminal Compliance Perspective. Forum on Politics and Law, 5, 103-115.

[10] Lao, P. (2022). Doctrinal Analysis of Criminal Assistance Behavior in Cybercrimes - Taking Article 287.2 of the Criminal Law as the Object of Analysis. Journal of Hebei Normal University of Science and Technology (Social Science Edition), 2, 80-87.

[11] Lao, D. (2016). Active Judicature and Functionalism in Criminal Law Interpretation. Jurist,6,13-28.
[12] He, R. (2015). Philosophical Critique of "Over-Criminalization" in Social Governance. Chinese and Foreign Legal Studies, 2, 523-547.
[13] Lang, S. (2017). "The New Development of China's Criminal Law." Chinese Legal Science,5.
[14] Ji, F. (2017). Analysis and Countermeasures of Cybercrimes Infringing on Citizens' Personal Information. Network Security Technology and Application, 10, 158-159.
[15] Shi, J., & Li, X. (2023). Dilemmas and Ways out of the Execution of Criminal Offenses Infringing on Citizens' Personal Information. Journal of Jilin University (Social Sciences Edition), 5, 78-90+237.
[16] Miao, C., & Yin, S. (2019). Preliminary Exploration of "Citizen Personal Information" Identification in the Crime of Infringing on Citizens' Personal Information. Journal of Shanghai University of Political Science and Law, 6, 63-69.
[17] Ministry of Public Security of China. (2021) Press Conference of the Ministry of Public Security on Deploying the Work Measures and Achievements of the Nationwide Public Security Organs in Launching the Special Action "Clean Net 2021". https://www.gov.cn/xinwen/2022-01/15/content_5668284.htm.
[18] Wang, W., & Zhu, L. (2019). Dealing with Cybercrimes Infringing on Citizens' Personal Information - Taking New Types of Cases of Illegally Obtaining Citizens' Personal Information as the Starting Point. People's Procuratorate, 10, 59-61.
[19] Gao, Y. (2021). The Criminal Law Should Set a Red Line for "Malicious Technology." Procuratorial Daily, 3. DOI: 10.28407/n.cnki.njcrb.2021.003133.
[20] Chen, X. (2003). Discussion on the Quantity Elements as a Constituent Element of Crime - Based on Chinese Criminal Law. Global Law Review, 3, 278-280.
[21] Chen, H. (2022). Examination of China's New Information Network Crime Legislation and Application. Journal of Guangxi University (Philosophy and Social Science Edition), 44(02), 185-198.
[22] Zhou, J., & Yu, H. (2019). Understanding and Application of "Interpretation on Several Issues Regarding the Application of Laws in Handling Criminal Cases of Illegal Use of Information Networks, Assisting Criminal Activities on Information Networks, etc." People's Justice, 31, 25-29.
[23] Du, J. (2017). From "Big Data" to "Big Data Transformation in Banks. http://bank.hexun.com/2017-02-20/188211596.htm.
[24] Zhou, J., & Yu, H. (2019). Understanding and Application of "Interpretation on Several Issues Regarding the Application of Laws in Handling Criminal Cases of Illegal Use of Information Networks, Assisting Criminal Activities on Information Networks, etc." People's Justice, 3, 25-29. DOI: 10.19684/j.cnki.1002-4603.2019.31.007.
[25] Mao, L. (2014). Legal Regulation of Internet Finance in Developing Countries. Journal of East China University of Political Science and Law, 5, 4-9.
[26] Chen, X., & Li, L. (2021). The Shifting and Restructuring of Penalties in the Governance of Online Financial Crimes. Study and Practice,6,44-51. DOI:10.19624/j.cnki.cn42-1005/c.2021.06.005.
[27] Wang, Z., & Zhang, X. (2021). Dilemmas and Solutions in Cross-Border Electronic Data Collection. Journal of Chongqing University of Posts and Telecommunications (Social Sciences Edition), 5, 45-46.
[28] Tu, S., & Lai, J. (2023). Comprehensive Determination of New Types of Cybercrime Cases. Journal of Chongqing University of Posts and Telecommunications (Social Sciences Edition), 5,47-58.