Policy Transformation of Illegal Use of Information Networks Under the Covid-19 Epidemic

Yixuan Bai(✉)

Qingdao University, Shandong Province, Qingdao 266071, China
byx12375@163.com

Abstract. The outbreak of the novel coronavirus epidemic and the measures of last resort confinement had direct and indirect effects on various areas of society, including opportunities for crime in the field and cybercrime, such as whether crime shifted from the physical to the cyber environment as a result of reduced access to crime. Surveys have shown that 'anti-space' crimes such as internet-dependent and internet-driven crimes have increased dramatically during the epidemic, with people spending an increasing proportion of their day browsing the web and becoming less active in the real world, meaning that there are fewer opportunities for violent crime and theft of property, and more opportunities for cybercrime. By analyzing the changes and characteristics of cybercrime under the new epidemic, this paper examines measures and solutions to transform the response to the illegal use of information networks, in an attempt to address the impact and 'opportunities' presented by the epidemic and change the situation and state of crime.

Keywords: Unlawful use of information networks · the Covid-19 Epidemic

1 Introduction

The spread over two years since the emergence of Covid-19 epidemic in 2020 has not only led to changes in the way the public works, consumes, social mobility, and cohesion, but also in the forms of cybercrime that are changing and transforming around this mainline. The changes regarding this crime are mainly manifested in the increase in the number of crimes committed, the more diverse means of committing crimes, and the shift in the type of crime from offline to online.

Such changes have triggered discussions and concerns among scholars at home and abroad, and the current research on the crime of illegal use of information networks in the academic community is mainly focused on two levels: first, the crime is studied in the sense of a general theory (Zhanghui, 2019 [1]; Pi Yong, 2018 [2]; Chen, 2018 [3]), Second, from the level of specific judicial application to examine the behavior (Dong Pu-yu, 2020 [4]; Zhang Yin, 2019 [5]; Jiang JL, 2019 [6]).

However, few scholars have discussed the impact of the epidemic on the development of this crime and how the crime should be transformed in response. In this paper, the

© The Author(s) 2022
G. Ali et al. (Eds.): ISEMSS 2022, ASSEHR 687, pp. 855–865, 2022.
https://doi.org/10.2991/978-2-494069-31-2_100

author will use comparative analysis, case study analysis, and summary induction methods to first start with the changes in crime and its causes in the context of the epidemic, and then propose specific measures to change the status quo, such as adjusting the criteria for determining aggravating circumstances, clarifying the specific circumstances of "aggravating circumstances", and issuing corresponding judicial interpretations as soon as possible. At the end of the article, the expected effect and outlook will be proposed, aiming to change the dilemma that this crime has been shelved in practice due to the competing forms of related crimes and the overly broad boundaries of the punishment for this crime, to fail to meet the new challenges of crime in the context of the epidemic and to provide a solution to the "fictionalization" and "pocketing" of the crime of illegal use of information networks. This paper will discuss the measures and paths to solve the problem of "pocketing" and "pocketing" of illegal use of information networks.

2 Crime Change and Causes in the Context of the Epidemic

Under the epidemic, preparatory cybercrime behavior has gradually evolved into the main battleground for crime, i.e. offline to online, while the illegal use of information networks has become increasingly diverse in its manifestations. As the deaths caused by the epidemic have created a psychological panic, online rumors have emerged. "Following the outbreak of the Covid-19 epidemic in early 2020, the information asymmetry caused by the huge disaster and the various social isolation measures taken to prevent the spread of the epidemic fueled the growth and spread of online rumors." [7]. For example, false information surrounding real-time information on the epidemic, development trends and efforts to prevent and control the epidemic spread unchecked in cyberspace. To effectively respond to online rumors and strengthen the prevention and control of the epidemic, in February 2020, the "two high authorities and two ministries" issued the "Opinions on Punishing Illegal Crimes that Obstruct the Prevention and Control of the New Coronavirus Infection and Pneumonia Epidemic according to Law", which addresses the issues of "fabricating false information about the epidemic and spreading it on information networks or other media", "disseminating on information networks, or organizing or instructing persons to disseminate on information networks, causing public disorder by stirring up trouble", "creating or spreading rumors, inciting secession and undermining national unity". The law provides for the conviction and sentencing of cybercriminals for the relevant offenses under the Criminal Law. The fact is that cybercriminals are becoming more and more unpredictable, and the organization of cybercrime is decentralized and without any control structure, but I would like to point out that cybercrime is not new, only the use of the Internet is unique, for which I would like to call it "old wine in new bottles". The simplicity of the criminal method, the low cost of the crime, the strength of the criminal intent, and the unique concealment and permeability of the network environment have led to the following changes in the criminal behavior regarding the illegal use of information networks.

The global instability of the New Crown outbreak is both a challenge and an opportunity for cybercriminals. Home-based policies and models in the context of the epidemic have opened up the possibility of cyberattacks, and unemployment has risen as a result of government-imposed operational controls over Newcastle pneumonia and the collapse

of small and medium-sized businesses that have hit the economy hard. The epidemic has facilitated and made possible such individual-based cyber attacks, as some foreign scholars have noted that "a wave of cybercrime against unsecured personal networks and uninfected computers could lead to serious data breaches or losses". According to relevant survey data, the number of young people as a criminal group has been gradually rising since the outbreak, and most of them have chosen to take up crime due to the lack of a source of income as a result of unemployment. "In March 2020, demand for the teleconferencing technology used by Zoom increased significantly, but it proved to be vulnerable to video hijacking. Hackers were able to access webcams and microphones on personal computers and interrupt web conferences" [8]. The epidemic led to the peak and culmination of a whole new type of criminal activity, cybercrime, from a long-term risk.

In the wake of the outbreak, there has been a marked increase in the illegal use of information networks for crime. According to a 2020 cybercrime survey report, phishing had a whopping 241,342 victims, data breaches endangered population coverage to 45,330, and blackmail, theft, and spoofing also ranked among the highest numbers of victims. Types of crime such as healthcare-related, harassment or threats of violence, and deception, for example, are significantly higher than they would have been in the absence of the outbreak. The number of social media, technical support, and terrorism cases were also higher than usual. Cyber fraud, phishing, and illegal online sales of counterfeit medical supplies, medicines, and personal protective equipment related to the Newcastle pneumonia outbreak are on the rise, with an increase in unverified information and threats. At the same time, cybercriminals used the anxiety and fear caused by the spread of the epidemic and the country's economic downturn to reinforce their tactics and methods by using the Newcastle pneumonia epidemic as a backdrop. The most popular modus operandi during the epidemic was to mimic the government's efforts to deceive or defraud citizens. Criminals often contact people through social media platforms, emails, or phone calls pretending to be from the government, where they try to collect personal information or illicit income through disguises or threats. Or by attacking remote work platforms and channels to obtain illicit information and secrets, criminals have done well to transform and change during the pandemic, making the illegal use of information networks significantly more dangerous to society.

3 The Main Manifestations of the Crime of Illegal Use of Information Networks

It is believed that the reason why the offense was created by law was to achieve an early start on cybercrime, and at the same time it is a representative offense of "preparatory conduct", so it was created to alleviate the practical need for the prosecution to prove the burden of proof and to better combat cybercrime violations. "The original purpose of the offense was to efficiently prevent the emergence of crime by combating the use of the Internet to enhance the transmission of specific information or to provide a platform for the flow of such special information." [9]. The force cases have revealed the unclear nature of the offense of illegal use of information networks, the lack of standards for prosecution, and the inappropriate treatment of judicial competition. The purpose and

position of the legislation of this crime are reflected in the principle aspect of domestic criminal law legislation to punish intentional criminal preparatory acts, because of the increasing prevalence of cybercrime, coupled with the difficulty of investigating and dealing with such crimes and other reasons, to better prevent and punish cybercrime, the publication of illegal criminal information on the network The crime is not dependent on whether the crime is committed or not, and whether the perpetrator is caught or not, which is conducive to a better fight against crime. The current state of judicial practice for this offense runs counter to the original legislative intent and is not in line with the intended development of the legislation in the long run.

In recent years, through the attack on the website information security system to make the target computer information system network or system resources exhaustion including service temporary interruption, stop or paralysis, etc. caused by the user can not normally use the hacking invasion procedures are increasingly intense. For example, Zhu Moumou's illegal use of information networks in the case, the manufacture of the "DDoS attack" is also known as distributed denial of service attacks, mainly through the control of thousands of computer information systems and target systems to launch network attacks and ultimately gain illegal benefits, Zhu Moumou launched the "DDoS attack". The "DDoS attack" launched by Zhu provided the wrongdoers with a choice of "bronze" and "gold" packages, which were designed to provide the perpetrators with a similar online shopping style The website was used by Zhu Moumou to make a total profit of more than RMB100,000. According to the case information released by the Beijing Haidian District People's Procuratorate, the "DDoS attack" service was auctioned as a commodity on the website, which greatly stimulated the unscrupulous elements to get lucky.

In addition, Article [10] of the judicial interpretation issued by the Supreme Court and the Supreme Prosecutor regarding the handling of cases of illegal use of information networks and helping information network criminal activities stipulates the establishment of websites used to commit crimes, the number of registered accounts, the number of messages and the number of groups. From the analysis of the judicial interpretations issued, the seriousness of the illegal use of information networks is mainly considered in terms of the number of times the perpetrator has practiced, the total amount, the illegal purpose, and the number of people receiving it (social harm), and the final amount of profit. In judicial practice, some perpetrators use the exchange or sale of personal information to obtain illegal profits. The difficulty faced in such practical cases is that the perpetrators often set up illegal websites and communication groups to carry out the flow of personal information of citizens for resale. For example, in the typical case of Zeng Moumou and 14 others who illegally used the information network, also known as the "cat pool" case. The so-called cat pool, "that is, originally in several industries widely used, based on a telephone expansion equipment (such as the common GOIP), can be converted into a telephone signal network signal, to achieve the purpose of using virtual number dialing", [11] in recent years, "cat pool" technology has been used by telecommunication network fraudsters, and the wrongdoers have committed crimes mainly by using the information and card numbers of the assembled victims. The Zeng Moumou case is a typical case with a large scale and long chain, with a complex division of labor and cooperation between criminals, and in the illegal use of information network fraud

activities, after carrying out illegal website development, with the help of "cat pools" and other equipment, sending out mass fraudulent SMS messages to lure victims to fall for the scam.

4 Problems Arising in Judicial Practice and Analysis

The effective cases reflect the current lack of accurate grasp of the qualitative characteristics of the crime of illegal use of information networks by judicial staff, and there is an over-expansion of the types of criminal acts to the point of proliferation, while the specific criteria for aggravating circumstances are ambiguous, mostly based on the specific amount of profit made by the offender to provide, over-reliance on the amount can not qualitatively measure the degree of specific social harm. The difficulty of controlling the diversity and concealment of cybercriminals' methods of behavior makes it difficult for practice staff to conduct in-depth investigations and focus on evidence collection. Furthermore, the excessive expansion of the scope of the subject of the act makes the specific object of regulation of this crime blurred and alienated; the excessive generalization of the actor's behavior makes this crime gradually reduced to a "pocket crime" and a "pocket crime" in the legal world. At present, the indicators of aggravating circumstances are mainly the number of illegal information published, the number of illegal profits, the social harm, the number and density of acts, etc. However, when a case has all the above-mentioned reference indicators, judicial practice does not have a unified comprehensive application of standards, so this crime has encountered a bottleneck and stagnant dilemma. And for the new quantitative factors of cybercrime brought by the epidemic, the existing legislative norms do not make clear provisions for them, nor do they provide for other quantitative factors that may emerge from the behavior of the perpetrator of this crime in the subsequent network era. "Due to the queering of relevant prosecution standards, judicial practice lacks clear guidelines on operational norms, leading to a trend of blurring the determination of aggravating circumstances", [12] the author believes that the standards established by the current regulations make it difficult to conduct a comprehensive and comprehensive evaluation of all cases.

Judicial practice can enhance the operability of criminal law convictions and sentences, the use of websites to publish information and the use of information networks are equivalent, currently, judicial practice is specifically characterized. For example, the perpetrator's pursuit of posts made by others, or messages and private messages on social networking platforms also qualify as the indirect publication of information. Therefore, whether the number of illegal information released and the number of people involved in the release of illegal information should be specifically examined belongs to the current should be dealt with, Germany and Japan's criminal legislation three levels of criminal theory system inside, the crime constitutes the appropriate, illegal and culpable belong to the actual examination of the corresponding class. Then from the three-level theory, the objective and subjective level of the actor subject to consideration, from the identity of the actor subject, can be the website set up person, operator, and maintenance personnel as the main punishment object, from the actor's behavior environment, the WeChat circle of friends information release function and the establishment of the communication group function has great similarity, through which the release of illegal criminal information belongs to the scope of this crime regulation.

Secondly, to make up for the loopholes and deficiencies of criminal regulations, criminal law theory, in general, punishing preparatory acts without realistic, specific, direct legal benefit infringement is the exception, and as "preparatory acts to implement the act of" the crime of illegal use of information networks, its application naturally becomes an exception, [13] because this crime is a misdemeanor, set only three years The loopholes and shortcomings of this crime have become apparent by the provisions of our criminal law in the corresponding article of this crime: conviction and punishment by the provisions of the heavier penalty. For example, the lack of a qualitative model for the commission of the act, the lack of obvious infringement of legal interests and criminal intent, the generalization of criminal legislation, the expansion of the scope of punishment, etc. The gap and disorder in the construction of the act have also become a problem in judicial practice. The author believes that it is necessary to change the abstract and broad theory of legal interests of this crime, to create a healthy and safe virtual network space in the tide of "virtual reality", and to avoid the unified standard of network order and safety after the destruction of "accumulation into a crime" without regulation.

Once again, it is ideal to pursue the co-existence of a restricted and expanded interpretation. "The legislative basis for the formalization of preparatory acts lies in the "amended criminal composition, abstracting or materializing the harmful results or social harm in the conformity of the constituent elements, in order to seek the formal mechanism of doctrinal evaluation and the substantive basis of legal benefit infringement" [3]. In order to prevent criminals from In order to prevent criminals from "spreading the net" to commit crimes, the statute of this crime should be interpreted in an expanded manner. In order to prevent criminals from "casting a net" to commit crimes, the statute should be interpreted in an expanded manner. The three types of doctrines are "expansion", "restriction" and "compromise". The "expansion theory" is from the perspective of textual interpretation, which regulates all forms of conduct related to this crime; the "restriction theory" chooses to focus on restricting the interpretation perspective, and believes that some of the illegal use of information networks should be regulated, such as the conduct of serious circumstances. The "restriction theory" chooses to focus on the restriction of the interpretation to regulate some of the unlawful use of information networks, such as the aggravating circumstances. The "compromise theory" considers that the meaning of "crime" includes not only the situations explicitly listed in the legislation but also common illegal and criminal acts such as infringement of citizens' personal information and organizing illegal activities such as pyramid selling".

Ultimately, the boundaries between this crime and the traditional crime competition are not clear in the judicial application, and the corresponding evaluation difficulties arise when competing, such as whether the so-called simultaneous constitution of other crimes and competing laws, competing crimes can be equated, as well as the distinction between several acts forming an implicated offense, absorption offense, etc., to be clarified [14]. "The illegal use of information networks has dual attributes, both as an independent mode of conduct for this crime and as a means of committing other related crimes, so the formal aspect of the crime and the crime of fraud and the crime of disseminating obscene materials for profit, etc. has the potential for judicial competition." [12]. From the traditional criminal law system to the new network. In the transition and transition

from the traditional criminal law system to the new network criminal law, avoid the state of this crime being set aside and abandoned in its application. The statutory penalty for this crime, which is set at a maximum of three years' imprisonment, is prone to become a "substitute" or "alternative" for regulating criminal acts when other crimes are in a gap. In addition, the legal provisions of this offense are very general and vague, and because of the tendency of judges to make conservative decisions when applying this offense, the expansion, restriction, or textual interpretation of judges in individual cases has caused great disagreement in the jurisprudence on the definition of this offense and the analysis of legal benefits, which has led to the so-called overlap and alternative state. To solve this situation, the statutory penalty for this crime can be increased by adding "particularly aggravated circumstances" and "very aggravated circumstances" on top of "aggravated circumstances", to regulate different socially harmful acts respectively. The aim is to increase the statutory penalty for this offense. For example, "particularly aggravated circumstances" could be set at a statutory penalty range of three to seven years. And expand the crime form evaluation mechanism, [13] the actor before and after the stage of behavior into two independent behavior, the first stage belongs to the fraud preparation link, mainly the use of network resources; the second stage is the website or platform supervisor. That is, the two major strata of cybercriminal law for the regulation of this crime are set up, but they do not differ from the three strata of German and Japanese criminal law. The specific examination of whether the perpetrator has violated the normal cyber order of cyberspace, or whether it is a step up from this, violating the legitimate property interests of others or other objects of legal interest protection.

5 Transformative Regulation of the Offense of Illegal Use of Information Networks

There are no physical barriers or boundaries on the Internet. It allows cybercriminals to target victims from anywhere in the world, without geographical barriers. When the new crown epidemic occurred, a large number of criminals on the internet used the epidemic as a banner to trick people into buying medical supplies such as masks and disinfectants or to make all kinds of so-called charity donations. The order of the epidemic prevention and control is national public security, and the purification of information on the internet is a matter of urgency. The illegal use of information networks is an important form of behavior that complements traditional crime, and in many cases cybercrime often involves offline crime, so the knowledge or expertise of technical crime is not applied.

5.1 Regulation of Network Intrusion

The emergence of the epidemic has made the multifaceted and decentralized crime patterns created by cybercriminals even more difficult to predict and control, making the fight against black and grey industry chain crime a central point. According to the act of harm, the object of the act, and the act itself. China provides cybercrime incrimination conditions for intentional and resultant offenders, with a high threshold for incrimination. For the time being, China's crime legislation should lift the light to clarify the heavy and absorb the highlights of legislation from countries such as the UK and the US.

To effectively combat the increasing number of cybercrimes, the UK has been investigating computer-related crimes since 1981, and the relevant UK cyber criminal law was born. In the UK, we can learn from the relevant legislation the strength of the UK network intrusion punishment and the way, the overall British aim to take pre-crime control and preventive measures to nip the crime state in the bud. The United States belongs to the case-law system, so case law has become its most important source of law, so the current precious cybercrime-related legislative norms are relatively scattered, and the United States federal government has not formulated a comprehensive and unified criminal legislation on cybercrime, and also did not carry out detailed provisions on the corresponding cybercrime activities, only through the specific legal practice of judges in case law for reference. However, it is worth learning that cybercriminals in the US are generally convicted of felonies, unlike the high threshold of criminalization for cybercrime in China, which is worth learning from China's criminal law legislation.

5.2 Adjustments to the Determination of Aggravating Circumstances

The adjustment of the severity of the situation is a transformative response that can be taken by the judicial staff. "Whether it is a fraud based on phishing software or fraud in the network economy, criminals take advantage of the uncertainty and fear of the public brought about by the epidemic to carry out the corresponding fraud, which greatly enhances the probability of success of the fraud. What is the response to the legal regulation of the illegal use of information networks in the context of the epidemic? The criminalization of preparatory acts on the Internet covers both "qualitative" and "quantitative" aspects, the so-called qualitative aspect requires that the preparatory acts are extremely harmful before they are considered crimes and require criminal liability; the so-called quantitative aspect requires that the act should be assessed for criminal liability in line with its the quantitative aspect requires that the act should be judged in a manner consistent with its harmfulness. Therefore, the specific definition of the criteria for determining aggravation can also be analyzed from two perspectives: "qualitative" and "quantitative".

Firstly, to avoid expanding the scope of punishment and excessively increasing it to the point of violating the principle of proportionality and the principle of modesty in criminal law, this type of information dissemination cannot be equated with a generalized information network, but should be precisely positioned. A reasonable distinction should be made between everyday acts, the business acts, and criminal acts, to avoid the normal work of network services or technicians being affected. For example, if the criteria for determining the seriousness of a communication group are established, i.e. for numerous similar domain names pointing to a unified website, then they should be accounted for cumulatively. At the same time, the number of hits and registrations on a website can reflect the extent of its dissemination, and the number of groups and members can also be considered as a criterion for determining the seriousness of the offense. Indirect information and dissemination channels should not be included in the determination of aggravation. The act of releasing indirect information independently does not bring actual concrete harm to the legal interests, so I believe that adjustments need to be made here to effectively prevent judicial arbitrariness.

Secondly, the data should be materialized and a corresponding judicial interpretation should be issued. The data I refer to here specifically refers to the number of illegal websites set up, the number of illegal accounts registered, the number of illegal communication groups set up, as well as the specific amount of illegal profits made from participation in illegal activities, the number of participants collected and so on. For example, the threshold and criteria for aggravating circumstances are that the number of illegal websites set up exceeds 100 or the number of illegal profits exceeds 25,000 yuan. Article 37 of the Criminal Code: "For crimes with minor circumstances, criminal penalties may be waived", and thus for illegal criminal acts, judges have a corresponding discretion according to the degree of the illegality of the act, so it is all the more important to speed up the implementation of data concretization. A large number of illegal use of the information network is often accompanied by offline illegal activities, so illegal use of the information network crime will be better than "Internet" behavior of a separate crime, the determination of the seriousness of the circumstances can also be offline crime related to the accompanying activities as a breakthrough in the investigation. As we all know, the abstract dangerous crime only needs to achieve the possibility of damage to the legal interests, rather than the specific content of the composition elements. Therefore, to better regulate the perpetrators of violations of this offense, the data of individual cases should not be used as a breakthrough, but rather the target should be considered whether the target is unspecific and whether the risk of harm caused is uncontrollable, that is, the abstract dangerousness should be considered [11]. "To adjust the conflict between the theory and practice of formal preparatory offense, the criminal law sub-rule can be through the appropriate legal mimetic method with the principle of abstract dangerous offense, in the actual legal benefit infringement inside the existence of abstract dangerous substantial preparatory behavior, rising regulation into the implementation of the act, creating a new crime." [15].

6 Conclusion

This article focuses on the changing characteristics of illegal use of information network crimes in the context of the epidemic and its causes and proposes measures to adjust the criteria for determining aggravating circumstances and to enhance the practicality of the relevant laws. At a time when the development of illegal use of information network crimes is in a stagnant dilemma, coupled with the epidemic as a catalyst, network-dependent and network-driven crimes have proliferated during the epidemic. In this regard, we need to take advantage of the trend of constantly adapting the interpretation of legal norms to the development of new phenomena, so that the two are constantly compatible and fully linked, and seek to use the interpretation of criminal law doctrinal principles to guide the work of judicial practice. On this basis, we should streamline the public communication procedures of governmental institutions, release timely information related to the prevention, control, and safety of the epidemic, and enhance the cyber security of the public health care system, so that the corresponding laws and regulations can also transform and respond to the special times brought about by the catalytic effect of the epidemic context.

The author expects the topic of this paper to become a focus of attention in the field of cybercrime prevention in the future, and hopes that scholars in the industry will pay

attention to the impact of the epidemic as an unexpected factor in the illegal use of information network crime, and gradually reduce the growth trend of this undesirable phenomenon, and contribute to the maintenance of cyberspace security.

References

1. Zhang Hui. Research on the legal application of cybercrime-related crimes [J]. Modern jurisprudence, 2019, 41(04):156-167.
2. Pi Yong. On new cybercrime legislation and its application [J]. Chinese social science, 2018(10):126-150+207.
3. Chen W, Xiong B. The doctrinal interpretation of the binary form of criminal behavior using information networks [J]. Journal of Shanghai University of Finance and Economics, 2018, 20(02):125-138+152. DOI: https://doi.org/10.16538/j.cnki.safe.2018.02.009.
4. Dong Pu-yu. Exploration of the boundary of application of the crime of illegal use of information network [J]. Journal of Dalian University of Technology (Social Science Edition), 2020, 41(06):84-90. doi: https://doi.org/10.19525/j.issn1008-407x.2020.06.010.
5. Zhang Yin. Judicial application of the crime of illegal use of information network [J]. Legal Application, 2019(15):13-22.
6. Jiang JL. Judicial Application of the Crime of Illegal Use of Information Network under the Theory of Explanation of Legal Interests-An Analysis Based on a Sample of Judicial Documents Since the Amendment to the Criminal Law (IX) [J]. Legal Application, 2019(15):33-42.
7. Lu Jianping, Jiang Ying. Criminal law governance of online rumors under epidemic prevention and control [J]. Journal of Social Sciences of Jilin University, 2020, 60(05):40-51+235-236. DOI: https://doi.org/10.15939/j.jujsse.2020.05.fx1.
8. Kari Paul, 'Zoom is malware': why experts worry about the video conferencing platform, The Guardian, 2 April 2020, http://www.theguardian.com/technology/2020/apr/02/zoom-technology-security-coronavirus-video-conferencing.
9. Chen Hongbing. The interpretation of the crime of illegal use of information network as "live" but not "general" [J]. DOI: https://doi.org/10.14154/j.cnki.QSS.2021.01.022.
10. Sun Daocui. Doubts and doctrinal formulations of the application of the crime of illegal use of information network [J]. Journal of Zhejiang University of Commerce and Industry, 2018(01):42-57. DOI: https://doi.org/10.14134/j.cnki.cn33-1337/c.2018.01.006.
11. Beijing Haidian District People's Procuratorate. Haidian District People's Procuratorate releases twelve typical cases of cyber technology crimes [EB/OL]. http://www.pkulaw.cn/fulltext_form.aspx?Gid=21558937. Accessed April 15, 2022.
12. Zhou M. Research on the criteria for conviction of illegal use of information network crimes: a perspective on the construction of the criteria of "manner of conduct" and "seriousness of circumstances" [J]. Journal of Shandong Judges Training College, 2019, 35(04):22-34. DOI: https://doi.org/10.14020/j.cnki.cn37-1430/d.2019.04.003.
13. Hu Sha. Research on the application of illegal use of information network crime - "being deflated" and "pocketing" [J]. Law Society, 2019(03):11-22. DOI: https://doi.org/10.19350/j.cnki.fish.2019.03.002.
14. Guo Xinzheng. Research on the problem of illegal use of information network crime [D]. Guizhou University for Nationalities, 2017.
15. Liang Gendlin. The dilemma and breakthrough of the principle of universal punishment for preparatory offenders: interpretation and reconstruction of Article 22 of the Criminal Law [J]. DOI: https://doi.org/10.14111/j.cnki.gfx.2011.02.008.

Open Access This chapter is licensed under the terms of the Creative Commons Attribution-NonCommercial 4.0 International License (http://creativecommons.org/licenses/by-nc/4.0/), which permits any noncommercial use, sharing, adaptation, distribution and reproduction in any medium or format, as long as you give appropriate credit to the original author(s) and the source, provide a link to the Creative Commons license and indicate if changes were made.

The images or other third party material in this chapter are included in the chapter's Creative Commons license, unless indicated otherwise in a credit line to the material. If material is not included in the chapter's Creative Commons license and your intended use is not permitted by statutory regulation or exceeds the permitted use, you will need to obtain permission directly from the copyright holder.