Research on the Current Situation of Cybercrime and Criminal Law Regulation Issues

Zhitong Wang*
Dalian Ocean University, Dalian, Liaoning 116000, China
*1154044218@qq.com

ABSTRACT

With the continuous development of network technology makes the Internet gradually into thousands of households, the network has increasingly become an indispensable part of people's work and life. In recent years, in the judicial practice of our country, there are a lot of cases about network crime, which makes people have to pay attention to the potential Internet security problems while enjoying the convenience and speed brought by the Internet. Followed by Internet crime cases to get people to re-examine network problems, now the network crime of technology advancement, the degree of complexity and concealment and difficult to obtain evidence is completely different to traditional crime, it also shows our country at present in the network crime in the criminal law on the regulation of some deficiencies, it is necessary to strengthen the regulation of network crime of criminal law, combining with the concrete problems in judicial practice make effective regulation measures, such as constructing cyber crime legislation system, perfecting the relevant charges system, improve the network technology and strengthen to the improvement of the network security system, improve the content of the social public network moral quality, So that citizens can actively participate in crime prevention and control, so that the criminal law regulation measures to play a real and effective role in curbing cybercrime.

KEYWORDS

Network Crime; Criminal Law; Regulation Measures.

1. INTRODUCTION

Nowadays, the rapid development of the social Internet has affected the way of social interaction, social structure and all aspects of people's life. At the same time, the crime mode has also appeared the characteristics of "networking". Cybercrime has increasingly become one of the main focuses of attention in today's society. However, how to regulate cybercrime in China's criminal law is still in the exploratory stage. However, research on the legal norms and institutional construction for punishing cybercrime is still not very complete, and there is still a certain lack of relevant legal systems. Currently, there is a lack of specific institutional planning and measures in criminal legislation. It is necessary to build a relevant legal system, improve relevant charges, clarify the punishment results of cybercrime, and play the regulatory function that criminal law should have, So as to effectively curb cybercrime fundamentally.
2. OVERVIEW OF CYBERCRIME

2.1. The Concept of Cybercrime

Cybercrime has evolved from computer system crimes. Firstly, cybercrime reflects the irreplaceable and indispensable role of computer networks in such crimes. As the main criminal object of cybercrime, network information systems are also an indispensable element in cybercrime. In addition, network information systems also play the role of criminal tools in related cybercrimes. From the perspective of criminal objects and tools alone, there is a significant difference between cybercrime and traditional crime. Although there is currently no clear definition of the concept of cybercrime in China, it is essentially a summary and general term for a certain type of criminal behavior, just like "property crimes" and "crimes against the person." The author believes that cybercrime is a violation of the legitimate rights and interests of citizens committed by natural persons or units using the network system in a virtual network environment, which has social harm. Criminal acts that disrupt the order and environment of network security and should be punished by criminal law.

2.2. The Causes of Cybercrime

With the rapid development of science and technology and the popularity of the Internet, the network plays an increasingly important role in people's life and work, and the network society has gradually emerged. The current use of the internet has penetrated every corner of social life. When people are accustomed to living in the online environment, cybercrime also quietly occurs around us. This has great social harm for both individual citizens and the interests of society and the country. At present, in China's judicial practice, cybercrime cases have become a focus of people's attention. New types of cases such as using the internet to commit virtual property fraud, leaking personal privacy of citizens, and publishing false statements online to infringe on the reputation rights of others are emerging one after another. Cybercrime has gradually become one of the main types of crimes in today's society. The reason for the current situation in our country is that the resolution mechanism for handling criminal offenses has not changed according to the characteristics of cybercrime itself, and traditional criminal crime resolution mechanisms are still used to deal with it, resulting in not achieving significant results.

On the one hand, objectively speaking, China is still exploring ways to deal with cybercrime, and effective solutions for regulating cybercrime have not yet been introduced. This has led to criminals being free to do whatever they want in the virtual online environment, which is the main reason for the frequent occurrence of cybercrime. On the other hand, the network has a significant impact on people's lives, which makes the way of crime also reflect its own distinctive feature, that is, "crime networking". Although there are many similarities between cybercrime and traditional crime, at present, in the social context of the Internet, the groups that use the network are very wide, which also means that the groups that will be hurt by the virtual network have become wide. Criminals may take advantage of information networks to commit property fraud, insult others, or engage in defamation and other criminal activities, which can bring serious social harm. Its criminal methods and targets also rely on network and computer technology, which is another important reason why cybercrime is not uncommon. Cybercrime is a new type of crime, It has certain unique characteristics that distinguish it from traditional crimes, so we need to deeply analyze the problem and start from the root to avoid it more efficiently.

2.3. The Main Characteristics of Cybercrime

There are both similarities and differences between cybercrime and traditional crime. In addition to sharing the same characteristics as other traditional crimes, cybercrime has gradually revealed some unique characteristics. Specifically, cybercrime has the following basic characteristics:
2.3.1. The Complexity of the Means of Cybercrime

The highly complex reason lies in the virtual identity of the perpetrators of related criminal acts in the online environment. Related cybercriminals often appear as character accounts or a certain IP address on the network, which provides a good way for criminals to conceal themselves. Even though these accounts and addresses can be queried through the public security system, in most cases, the results queried do not correspond one-to-one with the perpetrators of related criminal acts. This has increased the difficulty of handling cases. The high complexity of the means reflected in cybercrime stems from the virtual identity of the perpetrator. In order to prevent their identity and criminal address from being exposed, the perpetrator will try various network technology methods to better conceal their identity. For example, they will register multiple accounts for themselves, use virtual IP addresses, or constantly change IP addresses during the crime process. They may even use their own network technology to steal other people's accounts and commit cybercrime. In the process of cybercrime, it constantly exhibits the concealment, virtuality, and complexity brought about by the use of high-tech means. These characteristics, combined together, pose great difficulties to the investigation of cybercrime and also pose great challenges to the traditional criminal law regulation methods in China. This will greatly weaken the effective restraining effect of the traditional criminal law regulation methods.

2.3.2. Technological Progressiveness of Cyber Crime

The arrival of the network information age has changed people's lifestyle. The Internet has entered thousands of households. With the popularity of computers and people's smartphones in every household and people's increasing dependence on the network, people have become extremely convenient to access and use the network. This convenience also directly affects another feature of network crime, that is, the progressiveness technical means of network crime. The most prominent feature of cybercrime related cases is the high level of technical means and high concealment. Compared with traditional crimes, criminals do not need to prepare crime tools in advance, choose crime locations, or seek help from accomplices to complete them together. Nowadays, the continuous improvement of network technology and people's proficiency in operating network technology are the main reasons for the high frequency of cybercrime. It is very easy for criminals to commit crimes through the Internet. It can be easily done either by using network devices at home or by using the public network in Internet cafes or public places. Moreover, the public network areas that can be seen everywhere now also provide good hiding places for criminals, which makes it difficult for public security organs to find the specific personal information of the perpetrators of cyber crimes. This also invisibly increases the difficulty of handling cases for public security organs. For example, for crimes related to information dissemination, such as insults and defamation, if the perpetrator wants to commit such crimes, it becomes extremely simple. The perpetrator only needs to copy and paste the comments and opinions that appear on the internet, and then send them to major websites or various large WeChat and QQ group chats, which can attract public attention and cause large-scale agitation, thus achieving the perpetrator's goal, Constitute acts of insult and defamation. Advanced and convenient network devices, simple keyboard and mouse tapping behaviors, may bring unimaginable consequences and harm to individual citizens, and even have a negative impact on social order. From this perspective, the speed of dissemination, wide harm, and ease of operation of new types of cybercrime are unmatched by traditional crimes, and the difficulty of control can be imagined.

2.3.3. The Virtuality of Cybercrime

The place where cybercrime is committed is the virtual cyberspace, and its most prominent feature is the virtuality of the network environment and system. Criminal behavior in the network environment occurs in an invisible and intangible virtual world. In the current era of global economic integration and close relationships among countries around the world, cybercrime is easily evolving into a cross regional or even cross-border cooperation. Cybercrime is not limited by time, location, or character requirements. No matter where you are, you only need a computer, phone, or internet cable to connect
people from all over the world, and the number of participants in the crime is also significant. The crime location and criminal behavior can be unrestricted by traditional geographical restrictions, and can even be infinitely expanded.

2.3.4. Difficulty in Obtaining Evidence for Cybercrime

The characteristic of difficulty in obtaining evidence is mainly manifested in the individuals who commit cybercrime. Most of them are professionals with advanced skills in computer networks. They are not only very proficient in computer systems and network technology, but also have a good understanding of the shortcomings and loopholes in network systems. At the same time, they utilize their own advantages, Compared to ordinary people, more advanced network technology and electronic devices are used to commit cybercrime. By invading network systems and launching attacks, various electronic data, materials, and other information are destroyed, causing huge social harm and corresponding economic losses. The implementation of cyber crime is supported by high technology, which shortens the crime time on the basis of the criminal elements that constitute traditional crimes. Although the criminal means are complex, they are highly hidden. Using the Internet, criminal acts can be completed instantly and often leave no criminal traces, leaving investigators nowhere to find. As is well known, computers and criminals nowadays not only effectively conceal themselves, but also bring great difficulties and challenges to the investigation and trial of cybercrime cases. The network system itself does indeed have some large or small loopholes, and the legal lag in regulating cybercrime in reality makes the risk of such crimes being discovered lower. However, the harm caused by cybercrime is incomparable to traditional crimes.

2.4. Types of Cybercrime

With the advent of the information age, behaviors suspected of cybercrime have emerged one after another, such as "human flesh search" and "online water army" behavior, which are not uncommon in people's daily lives. Among the behaviors related to cybercrime, "human flesh search" and "online water army" behavior are representative of harmfulness and typicality. Not only does the behavior cause enormous social harm, but it also causes dual physical and mental harm to the victim. Such behavior violates the victim's personal rights, insults their dignity, and has a very negative impact on their reputation. In addition to bringing negative effects to the victim themselves, it also infringes on the social order of the virtual network society. It may even cause harm to the real social order, and so on.

On the one hand, in recent years, the main content of the frequent occurrence of "human flesh search" behavior on the Internet is to collect personal information and even personal privacy of the target object, and after collecting a certain amount of information, publish it on the Internet. Among the personal information that is searched, there will inevitably be a portion of personal privacy. In this society with developed networks, these personal information should not be exposed to the public. This will make it easier for criminals to engage in criminal activities, and the harm caused to the searched person is incalculable. Apart from the searched person themselves, "human flesh search" will not spare his family and friends. It will also expose the work or life of the searchee's family and even friends to the online and public view. "The essence of 'human flesh search' is a way of information search, which includes the conflict and balance between citizens' freedom of speech, right to know, and right to public opinion supervision, as well as privacy and reputation rights. For behaviors that violate citizens' basic rights and infringe on their privacy and reputation rights, they should be severely punished by China's criminal law." On the other hand, the phenomenon of "online water army" has also become one of the common behaviors on the internet. Some of the actions of the online water army have clearly violated the laws and regulations of our country. While using false accusations, defamation, malicious smearing and other means to attack others, they not only infringe on their reputation, privacy, and various legitimate rights and interests, but also disrupt the normal social and economic order of citizens on the internet.
3. ANALYSIS OF THE CURRENT SITUATION OF CYBERCRIME

3.1. Underage Cybercrime

With the growth of teenagers and minors in the online environment and the flexible use of network technology, they have increasingly evolved into the main perpetrators of cybercrime. Whether driven by their young and ignorant curiosity or intentional behavior, related cybercrime incidents occur frequently among them. However, China has not yet launched relevant education to address this issue. Teenagers are not even aware that their behavior has violated the law, which is one of the important reasons for the current phenomenon of younger age groups in cybercrime. According to the relevant provisions of China's Criminal Law, only natural persons who have reached the age of sixteen and have full criminal responsibility will be recognized as such criminal subjects for computer network crimes. However, the criminal subjects of computer network crimes are only units and natural persons. It is not difficult to draw a conclusion that China's criminal law only punishes natural persons over the age of 16 for committing computer network crimes. Such criminal law provisions undoubtedly indicate that even if minors under the age of 16 commit network crimes, they will not be punished by the relevant criminal law.

However, with the gradual networking of society and judicial practice in recent years, it has been proven that a considerable number of minors under the age of sixteen are committing cybercrime. The motivations for committing cybercrime among them may not be the same. Some minors may be curious about the virtual environment of the internet or to highlight their online talents among peers in pursuit of spiritual stimulation and satisfaction, Or it could be pranks between three or five playmates, regardless of the reason that led them to think about cybercrime. In short, minors under the age of sixteen are an indispensable part of the team of computer cybercrime. With the increasing development of network technology and the proficient use of mobile phones, computers and other network devices by minors, minors under the age of sixteen have shown special talents in this regard. In fact, the social harm caused by their computer network crimes is not less than the social harm caused by committing other traditional types of crimes. However, due to the current lack of punishment methods for juvenile cybercrime in China's criminal law, it also means that it is not possible to punish minors under the age of sixteen for committing cybercrime, and it does not have the effect of deterring their criminal psychology and preventing their criminal behavior. Minors are still in a stage where their understanding of society is not comprehensive and their minds are not yet mature. The author believes that both from a legal perspective and from the perspective of school and family education, they should be guided in the correct direction during their growth stage. If the double-edged sword of the internet is neglected during this period, it may affect a child's life.

3.2. Backward Network Tracking Technology Means

One of the most prominent characteristics of the criminal acts related to network crime is the progressiveness of network technology means. However, one of the major deficiencies in China's handling of cases related to network crime is the backwardness of network tracking technology means, which makes the regulatory measures in the criminal law insufficient to deal with the current situation of network crime, seriously restricting the criminal law regulatory capacity of network crime. With the continuous development of network science and technology, criminals have to improve their mastery and application of network technology in order to carry out online criminal activities more proficiently and conveniently, making their criminal methods appear more advanced and sophisticated. In order to cope with the constantly improving information network crime technology of criminals, The most effective solution is for the personnel of the public security network supervision department to continuously learn and improve their network technology in order to quickly formulate preventive and regulatory measures. Advanced cybercrime technology also reflects the complexity and concealment of cybercrime. For example, in some cybercrime cases, criminals
hope to use high-tech means to evade legal supervision, and the corresponding network supervision department staff should conduct in-depth research on network technology and combine the existing technological strength of the public security department to arrest criminals. However, in terms of the current tracking technology for cybercrime in China, there is still a lot of room for improvement, and there are more advanced technological means waiting for relevant personnel to learn. In order to more effectively solve this dilemma, a team of network technicians with high technical content and fast computer technology response speed can be formed for handling some special cases, to deal with sudden network crime events with high technical expertise and difficulty. They can be used as the backing and technical support for public security organs to specifically respond to high-tech issues.

3.3. The Regulatory Scope is Too Narrow

One of the problems that the current criminal law needs to address in regulating cybercrime is that its regulatory scope is too narrow. In fact, the harm caused by cybercrime is much more serious than we imagine, and the simplicity of implementation is also the root cause of this problem. By large-scale destruction of network information systems or multiple attempts to destroy network information systems and then taking advantage of the situation to engage in cybercrime, such incidents are not only easy to occur, but the harm they cause is also quite serious. If these two characteristics are ignored and only serious criminal consequences are used as a condition for conviction and sentencing, it means that the regulatory scope is too narrow. This problem is clearly present in the relevant legal provisions in China at present. The consequence of facing this problem is that it will inevitably lead to the proliferation of a large number of illegal online behaviors that cause serious harm to society but are not sufficient to convict, thus making the criminal law unable to play its due regulatory role. With the rapid development of the current economy and society, and the continuous popularization of computer network information system applications, various fields of social life, as well as various departments of major units, have established their own applicable computer network technology systems. If a criminal in a certain aspect uses convenience and proficiency in the network technology system to invade the computer network systems of these important fields or departments, it will cause irreparable losses, and its social harm and influence are unimaginable. In the judicial practice of our country, many real cases have occurred, such as bank staff using the identity of their internal employees to illegally invade the bank's fund settlement system, causing huge financial losses to the bank after committing a series of criminal acts. At the same time, the losses caused to market order and public and private property security are also incalculable. It may even affect the financial order of the entire industry and endanger the property safety of the people. In the current criminal legislation of our country, the act of damaging computer network information systems has not yet included network crimes similar to those in virtual environments in the scope of criminal law protection, which may lead to criminals taking the opportunity to commit crimes, greatly weakening the role of criminal law in punishing crimes and protecting the people.

4. CURRENT LEGISLATIVE DEFICIENCIES IN CHINA REGARDING CYBERCRIME

4.1. The Age of Criminal Responsibility is Relatively High

In the rapidly developing social context of the internet age, the subject of cybercrime is showing a trend towards younger age groups, and among the perpetrators of related cybercrimes, juvenile delinquency accounts for a large proportion. However, the legislation of our country's criminal law is not perfect in this regard. According to the relevant provisions of our country's criminal law, the criminal subject must bear criminal responsibility when they reach the age of 16; Individuals who have reached the age of fourteen but not the age of sixteen and commit crimes such as intentional homicide, intentional injury resulting in serious injury or death, rape, robbery, drug trafficking, arson,
explosion, or the release of hazardous substances shall bear criminal responsibility; Under the age of 14, there is no criminal responsibility. From the perspective of prevention and control of juvenile cybercrime, such regulations undoubtedly indulge juvenile criminal behavior and will not have any educational effect on teenagers. Therefore, the author believes that China's criminal law should appropriately lower the age of criminal responsibility in identifying the subject of cybercrime. After investigation and research, soliciting broad opinions from all sectors of society, and discussions among experts and scholars, the age of criminal responsibility can be appropriately lowered to twelve or even ten years old. However, based on the overall principle of national and social protection for minors, The law can still make provisions for lenient or mitigated punishment for minors aged 12 or 10 to 18 who commit criminal acts. This approach of appropriately reducing the age of criminal responsibility not only effectively controls the behavior of minors in cybercrime, but also strictly regulates the online behavior of all minors, allowing minors to safely and properly access the internet in a virtual online environment. I believe that this approach will have a huge positive impact on the use of criminal law to regulate minors from committing cybercrime.

4.2. The Legislative System for Cybercrime is Incomplete

Due to its unique and complex means, advanced technology, wide range of criminal targets, and virtual nature of the internet, cybercrime results in a higher degree of harm and a wider scope compared to other traditional types of crime. The current criminal law's regulatory system for cybercrime is not yet perfect, which cannot effectively curb cybercrime. At present, the regulations on cybercrime in China's legislative system are still only at the level of criminal law and judicial interpretation, and there are no other relevant provisions to control cybercrime. A significant problem in the current legislative system is that in terms of cybercrime, the classification of criminal penalties that criminals should receive is not clear, and the levels and methods of punishment are also not perfect. The degree of punishment that some criminals deserve does not match the actual punishment results. For example, the crime of illegal intrusion into computer information systems, which emerged with the widespread use of network computers, refers to the act of violating national regulations, invading computer information systems in national affairs, national defense construction, and cutting-edge scientific and technological fields. National affairs and defense construction play the most important role in various countries. Once a country's defense construction, national affairs, and cutting-edge science and technology are stolen by criminals, it will suffer huge losses for a country, and even lead to the inability to stand in front of other countries. However, those who commit such crimes through computer networks have advanced means and the harm is evident. Such criminals should be punished severely in comparison to those who destroy other computer systems. However, throughout the legal provisions, the statutory penalty for this criminal act is only imprisonment or detention of up to three years. The lenient criminal punishment is not compatible with the criminal consequences it brings.

4.3. Incomplete Types of Criminal Penalties

"Among the specific charges stipulated in China's Criminal Law, Article 285 states that the maximum sentence for the crime of illegal intrusion into computer information systems is 3 years; Article 286 states that the sentence for the crime of damaging computer information systems is imprisonment for less than 5 years or detention, and imprisonment for more than 5 years, depending on the severity of the consequences. The punishment results and sentence duration for these two criminal acts are determined." , ④ The author believes that China's criminal law has not yet made clear provisions on the punishment of cybercrime, which cannot fully reflect the importance of protecting the legal interests of computer networks. Although there are already individual charges applicable to cybercrime, the forms and methods of cybercrime are diverse, and its social harm is deeper and wider than traditional crimes. Therefore, China should currently introduce more detailed and specific
punishment methods for cybercrime in order to better apply the principle of criminal responsibility and punishment to judicial practice, and effectively curb the occurrence of cybercrime.

5. SOLUTIONS TO THE PROBLEM OF CYBERCRIME

5.1. Expand the Scope of Legislative Protection for Cybercrime

Due to the serious social harm and concealment of cybercrime, it is necessary to appropriately expand the legislative protection scope of cybercrime. The author believes that on the one hand, it is necessary to modify the relevant provisions of Article 286 of the current Criminal Law, which stipulates that the criminal act of damaging computer information systems can only be criminalized if the consequences are serious, and to modify it to be criminalized if the circumstances are serious, thereby expanding the effective scope of criminal law regulation for this criminal act. This measure can greatly improve the starting point for criminalizing illegal acts, effectively respond to criminal acts of large-scale destruction of network information systems, and also serve as a deterrent and preventive measure for some cybercriminals.

On the other hand, the author believes that for the relevant charges of transferring traditional criminal acts to the online environment, the reasonable part of judicial interpretation should also be included in the formal provisions of the criminal law to appropriately expand the scope of criminal law regulation. Specifically, it includes amending the provision in Article 364 of the current Criminal Law that only "disseminating obscene materials" can be criminalized to "disseminating obscene or materials with adverse effects". By appropriately expanding the scope of criminal law regulation on cybercrime, we can strengthen the crackdown on cybercrime and maintain a good order in both online and social life.

5.2. Building a Legislative System for Cybercrime

In order to effectively and comprehensively curb cybercrime, China should now further improve and supplement the problems in the legal system. After more and more Internet penetration into people's lives, it has also quietly changed people's work, learning, payment and other aspects of society. In practice, cyber negligent crime due to negligence or unintentional loss has gradually emerged. This means that China's criminal law needs further improvement in the area of network negligence crimes. Some important negligent behaviors of subjects in virtual cyberspace should be included in the regulation of criminal law. Clear provisions should be made in the regulation of criminal law for the disposal of negligent offenders. In cases where negligent crimes cause serious harm, they can be criminalized. This enables China's criminal law to regulate negligent offenders under the premise of causing serious harm, and the true purpose of using criminal law to regulate is to prevent and warn criminals, so that network entities can always be vigilant, rational, and pay attention to safeguarding their own and others' legitimate rights and interests in the virtual cyberspace.

5.3. Improve the Moral Quality of the Public on the Internet

The most common way to fundamentally and effectively curb the occurrence of cybercrime is to improve the moral quality of the public on the internet, carry out nationwide education activities, fundamentally transform the thinking of citizens to attach importance to cybercrime, learn to protect their legitimate rights in the virtual online world, and encourage every citizen to actively participate in crime prevention and control. Criminal law is the last line of defense for social order, and its punishment method is the strictest and most deterrent to a law. Relying solely on the regulation of criminal law is not enough to create a secure and good network environment. There is still much we need to do. For social prevention and control, the significance of prevention far outweighs punishment. On the one hand, through propaganda and education, it can serve as a deterrent and warning to
criminals who attempt to commit cybercrime, enhance their awareness of crime deterrence, and timely pull them back onto the correct path of life, stopping the pace of crime. On the other hand, through publicity and education, it is also possible to enhance the awareness of online security among netizens, strengthen their own security prevention, identify the criminal means of criminals, and protect their legitimate rights and interests to the greatest extent possible. Netizens actively prevent and avoid losses through education, and perpetrators understand the serious consequences behind criminal behavior through education. Only in this way can the combination of the two be the best solution to maintain the order and security of the virtual society on the internet.

6. EPILOGUE

The rapid development of the internet has brought great impact to people's lives. The internet is a double-edged sword, which not only brings convenience to people but also invisibly brings many dangers. We can only effectively improve the current social situation by improving our own legal system and establishing a complete legal system. At present, China's criminal law is still actively exploring the issue of cybercrime. However, we believe that with the continuous improvement of network regulatory technology, the continuous enhancement of citizens' network literacy, and the improvement of the criminal law regulatory system, China's future virtual network environment will definitely have significant changes.

REFERENCES