DOI: 10.54254/2753-7048/41/20240738

A Study on Criminal Law's Safeguarding of Cybersecurity in the Context of Artificial Intelligence

Chang Yu[1,a,*], **Junrui Hu**[2,b]

[1]Jiangsu Coal Geological Exploration Team 2, No. 13 Coal Construction West Road, Quanshan District, Xuzhou City, Jiangsu Province, China

[2]China Geological Mining General Bureau, No. 20 Jia, Thirteen District, Heping Street, Chaoyang District, Beijing, China

a. 530375818@qq.com, b. 615801524@qq.com

**corresponding author*

Abstract: With the rapid development of information technology in China's Internet, the associated cybersecurity issues have gradually gained social attention. Incidents involving the infringement of citizens' legitimate rights by unlawful individuals using information technology vulnerabilities occur frequently. These incidents pose serious threats to the safety of citizens' lives and property, as well as the stability of social order in our country. In recent years, the rapid development of artificial intelligence has further brought this issue to the forefront of public opinion. Therefore, it is necessary to strengthen the legal foundation and improve criminal legislation to ensure the information security of Chinese citizens.

Keywords: Artificial Intelligence, Cybersecurity, Information Security, Legitimate Rights

1. Introduction

In daily life, education, and work, computer networks have demonstrated their high convenience and openness. With the gradual improvement of information transmission efficiency and quality requirements in the context of the new era in China, our country's information technology has rapidly developed. In the current stage in China, the integration of various advanced scientific and technological fields, such as Internet technology, automation technology, big data, and artificial intelligence, is deepening. This integration has had a significant impact on people's lives and has deepened the dependence on artificial intelligence technology. However, various security concerns have quietly grown. At present, numerous malicious actors in our country are utilizing artificial intelligence for cybercrime, causing significant harm to society. Simultaneously, it has created significant challenges for our public security departments. Due to certain shortcomings in our country's criminal law, the inability to timely investigate and apprehend criminals involved in cybercrime is evident. Therefore, to address this issue, it is necessary to strengthen and improve legislation and law enforcement related to the personal information security of citizens. Additionally, practically utilizing criminal law to protect the cybersecurity of Chinese citizens is imperative. Furthermore, from a practical perspective, conducting comprehensive research on the legal protection of cybersecurity in the era of artificial intelligence in China can provide a theoretical basis and reference for enhancing the management of our country's cybersecurity.

2. Concept of Criminal Law Regulation on Information Network Security Management Obligations

2.1. Necessity for Establishing Sound Criminal Law Relevant to Information Network Security

Novel technological methods cannot thrive without the protective framework of the law. Therefore, on the one hand, the rapid development of informatization in China currently requires adherence to effective laws and regulations. Due to the uncertainty and virtual nature inherent in the development of the internet industry in our country, organizers and providers of various network service platforms often do not directly engage in criminal activities. Instead, they primarily offer network platform services. However, there is a phenomenon of these platforms tolerating the dissemination of related illegal information and being somewhat lax in effectively managing the platform's legality and compliance. On the other hand, existing criminal law provisions in our country are inadequate to effectively regulate such behaviors. Hence, to curb the expansion of our country's cybercrime sphere, it is necessary to reevaluate and improve the criminal law regulation concerning network service providers.

2.1.1. Escalating Proliferation of Cyber Criminals

While network information technology brings convenience to people, it also provides opportunities for many malicious actors. They exploit network technology to carry out various criminal activities. Even certain terrorists may use the online environment for disseminating information, planning terrorist attacks, and engaging in illegal fundraising, causing significant harm and insecurity to society [1]. In recent years, there has been a surge in criminal activities, such as fraud, conducted by numerous wrongdoers using various online platforms in our country. This has had severe adverse effects on the personal and property security of our citizens. From the perspective of perpetrators of cybercrime, their activities are characterized by broad dissemination, severe consequences, and difficulty in control. This makes many opportunistic wrongdoers eager to use network technology to carry out criminal activities. Particularly in recent years, the frequency of cybercrime in our country has been increasing annually, and various traditional forms of crime are gradually shifting to the internet [2].

2.1.2. Uniqueness of Criminal Law Regulation on Network Platform Services

It is often said that the internet is not beyond the reach of the law. Therefore, to punish and prevent the occurrence of cybercrime, it is imperative to subject various network service platforms to reasonable criminal law regulation, making every effort to eliminate the occurrence of cybercrime. Typically, individuals committing crimes through network service platforms are merely utilizing the platform's resources and do not represent the platform as a participant in the crime. Therefore, in the criminal governance of various network service platforms, it is essential to avoid adopting a blanket prohibition approach. Legislators should implement punitive measures in advance and appropriately allocate the responsibility for monitoring harm to each network service provider platform. This ensures that, while providing network services, they also bear the criminal obligation of preventing harm from occurring.

2.2. Governance Concept of Criminal Legislation on Acts of Omission

Due to the uniqueness mentioned earlier of network service platforms, the decision to employ criminal governance requires adopting innovative forms. In the current legislation of our country, the general approach to criminal management mentioned above is through the establishment of the crime of failing to fulfill information network security management obligations. The introduction of this charge signifies a significant enhancement and improvement in the responsibility of network service platforms for the criminal obligation of information network security. It is a necessary expansion of our country's legislative content. Furthermore, the phenomenon of an expanding criminal sphere resulting from criminal legislation should ultimately reach a balanced state. Meanwhile, from the perspective of the criminal obligations of the mentioned network service platforms, they need to maintain a dynamic balance between citizens' freedom of speech, protection of citizens' legitimate rights, and the development of network information technology [3]. In summary, while legislative expansion increases the criminal responsibility of network service platforms, there should also be reasonable regulation of such expansion. The dynamic balance between expansion and restriction reflects the tension between citizen rights and security and freedom of speech that has persistently existed on the Internet in our country [4].

3. Forms of Cybersecurity Crimes

According to the "National Information Security Report," computer network crimes in our country are currently categorized into the following concentrated types: unlawful individuals stealing enterprise or government confidential information, fraudsters utilizing new network technologies for extortion, and malicious hackers conducting cyber attacks on targeted entities by creating and utilizing new network viruses or malicious programs.

3.1. Information Theft and Misuse

Among all prevalent types of cybercrimes in our country, information theft and misuse are the most common, particularly in the extensive business sector involving economic issues. Many wrongdoers employ this type of criminal method to illicitly gain benefits, causing significant direct economic losses to individuals or corporate entities [5]. With the increasing level of information technology development in our country, the widespread occurrence of this type of crime has become a major concern in the field of Internet security in our country.

3.2. Online Fraud and Extortion

In recent years, cases of unlawful individuals counterfeiting residents' credit cards or other payment instruments resulting in economic losses have been frequently reported in our country. Moreover, some hackers, through illicit means, infiltrate a company's network systems, causing operational paralysis and subsequently extorting substantial compensation from the affected company.

3.3. Cyber Virus Attacks

In addition to the aforementioned forms of cybersecurity crimes, there is another type wherein wrongdoers habitually use the internet as a channel for committing crimes by launching information attacks and destruction against others. This form of crime primarily manifests when unlawful individuals target specific computer programs and network data, design corresponding computer viruses, and package them as normal programs to invade others' computer programs and networks. According to statistics, there are currently over 4000 known computer network viruses, including common ones such as the Panda Burning Incense virus and the Shockwave virus. Unlawful individuals have exploited these viruses, causing significant economic losses.

4. Analysis of Causes for the Existence of Various Cybercrimes

Considering the current stage of internet development in our country, the emergence of cybercrime is deeply associated with social factors to a certain extent. An analysis and organization of the main reasons for the prevalent cybercrime phenomena in our country at this stage include the following points:

4.1. Lack of Adequate Cybersecurity Awareness Among Netizens

The Internet has brought convenience to the lives and work of Chinese residents; however, it has also introduced certain usage risks. Due to the inherently virtual nature of the Internet, it implies the existence of numerous instabilities and insecurities, making it a crucial factor that attracts many criminals to engage in cybercrimes. Therefore, to curb cybercrimes effectively, users of the Internet are required to possess a high level of awareness of network security, thus reducing the frequency of cybercrimes. However, considering the current user base of the Internet in China, as the Internet has been popularized for a relatively short period, a significant portion of netizens is still in the early stages of exposure to the Internet. This implies that due to a lack of a certain level of awareness regarding the virtual nature of the Internet, they are unable to form a robust sense of network security, making them prime targets for cybercriminals. Particularly in recent years, with the widespread use of smartphones, an increasing number of middle-aged and elderly individuals have started to engage with and use the Internet. This demographic is also susceptible to becoming “primary targets” for cybercriminals.

4.2. Lack of Targeted Relevant Laws and Regulations

In fact, since humans began using the internet, seeds of various cybercrimes have been sown. As people’s utilization of the internet deepens, the governance of cybersecurity becomes a challenging issue. The fundamental reason lies in the imperfect legal framework regarding internet security. Generally, the authoritative nature of law dictates that the legislative process must undergo thorough argumentation and practical implementation to be truly effective. However, the internet industry’s exceptionally rapid development creates an evident disconnection between the construction of internet security laws and the reality of cybercrimes. Consequently, some wrongdoers exploit the lack of relevant legal basis, engaging in various activities that skirt the edges of the law, significantly jeopardizing the cybersecurity environment.

4.3. Lack of a Reasonable and Systematic Network Security Management Platform

Combating cybercrime often requires a combination of technical means and management methods. This implies that relying solely on technology or management is insufficient for effective governance. Due to the wealth of international experience in internet governance, China has conducted extensive research and drawn inspiration from global experiences in combating cybercrime. Many countries and regions have constructed comprehensive network security management platforms to prevent and combat cybercrimes. This seems to have become a consensus in international internet security governance, as systematic platforms can organically integrate technical means and management methods to prevent and combat cybercrimes. However, China lags behind in this regard compared to the international community. Our country’s research on network security management is still in the exploratory stage, resulting in the lack of a reasonable and systematic network security management platform. This, in turn, hinders the ability to unite various forces in addressing internet security issues, making it difficult to curb the frequent occurrences of cybercrimes.

4.4. Lagging Development in Network Security Technology

Due to the greater instability inherent in cybercrime compared to traditional crime, it is imperative for network security technology to keep pace with advancements. Only by increasing investment in research and development in network security technology can its decisive role in the governance of cybercrime be highlighted, thus achieving effective prevention and combating of cybercrimes. However, considering the current trend of internet technology development in China, there is insufficient attention and investment in the research and development of network security technology. Most enterprises or units in China, driven primarily by profit motives, channel the majority of their research and development efforts into consumer-oriented businesses, seeking greater economic returns. In recent years, due to the increasing emphasis on cybersecurity in China, many internet enterprises have heightened their focus on network security. Against this backdrop, numerous companies have begun redirecting a portion of their research and development resources towards network security technologies. However, assessing the overall state of technology research and development in the current Chinese internet market reveals that the majority of enterprises face challenges. This is primarily because they are unable to obtain timely profit returns from investments in network security technology. Consequently, these enterprises still struggle to maintain a robust enthusiasm for the development of security technologies. As a result, the cybersecurity governance of various enterprises in China currently lacks effective technical support.

4.5. Lack of a Comprehensive Mechanism for Preventing and Governing Cybercrimes

While it is true that the internet possesses a certain virtual nature, from another perspective, the online society is not entirely virtual. At times, it serves as a true reflection of the real-world society, implying that the contradictions in the online society align closely with those in the real world. Therefore, to achieve genuinely effective prevention of cybercrimes, it is necessary to draw on various related issues present in the real-world society. Additionally, just like the real-world society, the online society harbors various types of crimes. These different types of crimes also pose varying degrees of harm to both the online and real-world societies. This necessitates having a specific focus when preventing and governing cybercrimes. However, due to a lack of relevant governance experience in the prolonged process of managing internet security, China lacks a rational and scientific governance mechanism for combating cybercrimes. Consequently, the current cybercrime issues in China cannot be systematically addressed.

5. Key Points for Improving Criminal Protection in Network Security

From the current perspective in China, it is imperative to emphasize the criminal protection of network security in the era of artificial intelligence. This work is crucial for ensuring the legitimate interests of every individual in China. Moreover, with the rapid development and progress of the era of artificial intelligence in China, various cybercrime methods employed by criminals continue to emerge. Incidents of theft of citizens' user data are challenging to prevent, and the amounts involved in malicious online fraud and extortion crimes are increasing. The depth and breadth of criminal activities conducted by malicious actors through cybercrime are also continuously expanding. In this urgent situation, relevant departments responsible for network security must be fully prepared to respond effectively. They should explore and establish new paths to strengthen and improve China's criminal protection system for network security.

5.1. Optimization of Criminal Law Principles

To comprehensively improve criminal protection for network security in the era of artificial intelligence in China, it is necessary to address the ideological aspects. Adjustments and improvements must be made to the existing criminal law principles in China to make legislation and judicial guidance more effectively implemented. As the dependence of Chinese residents on the internet continues to increase, the boundaries between the online and real-world societies have become blurred. Various security incidents related to the online society have a significant impact and cause considerable distress to Chinese citizens. Therefore, to effectively prevent and avoid such adverse situations that may interfere with the development of Chinese society, it is necessary to strengthen the existing criminal protection for network security. This process requires the exploration and practical utilization of more practical criminal law systems. Additionally, during the phase of criminal law protection, distinctions between the online society and the real-world society must be identified. This ensures avoiding excessive interference in the online society, hindering the development of the internet. Simultaneously, considerations should be given to whether the management is too lax, leading to unfavorable supervision of network security and providing opportunities for malicious actors. Therefore, in the optimization of criminal laws related to network security, it is crucial to ensure a balance between combating cybercrime and preserving online freedom. This involves implementing criminal protection for network security while maintaining a balance between the two, allowing them to interact and influence each other. Furthermore, in the optimization of China's criminal laws related to network security, various collaborative protection measures should be fully utilized. This helps avoid limitations in the governance methods for cybercrime, requiring substantial attention and research on multiple governance methods.

5.2. Improvement of Legislative Norms

To adapt to the changing demands for criminal protection in network security in the era of artificial intelligence, relevant departments need to appropriately enhance and amend the norms of criminal legislation. This aims to achieve effective protection of network security and comprehensive regulation. In practical implementation, the above methods can effectively address the emergence of new legal interests and order management in the online environment. This is also a necessary step in the comprehensive improvement of criminal legislation related to network security in China. During the specific implementation of this phase, relevant departments should pay attention to effectively setting up criminal charges related to cybercrime. It is recommended to include charges related to the endangerment of critical information infrastructure in this work. Legislators should further enrich and clarify charges related to network security to accurately define the facts of cybercrime and more precisely assess the impact of cybercriminal activities on society or individuals. For example, terms such as "destruction" or "negligent destruction" can be adopted as defining conditions to measure the types of offenses and the severity of crimes related to critical information infrastructure. Additionally, legislative bodies can regulate types of cybercrimes related to network products and network services by adding relevant charges.

5.3. Optimization of China's Criminal Law Explanatory Function

The primary content of the implementation process of China's criminal law is criminal law interpretation, which serves as a crucial basis for implementing criminal law during the enforcement process. Criminal law interpretation plays a significant role in the work of judicial personnel, facilitating a deeper understanding of criminal law for relevant professionals. It also inspires judicial personnel to identify legislative deficiencies in the current stage, thereby contributing to the improvement and enhancement of legislation in China. Therefore, it is essential for China to organically combine criminal law interpretation with legal practice to ensure the normativity of criminal protection for network security in the current era of artificial intelligence. Additionally, considering the current realistic background in China, various criminal law regulations are noticeably lagging due to multiple objective reasons. This implies a discontinuity in the legislative and judicial processes, making it easy for existing laws in China to lack comprehensive coverage of the content in the online environment. Ultimately, the inherent lag in criminal law regulations determines its inability to provide clear guidance and assurance to law enforcement personnel during the legislative and enforcement processes. Therefore, to seek solutions to the above issues, it is necessary to effectively utilize the adjusting advantages existing in China's criminal law interpretation. This approach is expected to leverage the expansiveness of criminal law interpretation to address deficiencies such as lag and one-sidedness in the legislative process. Furthermore, during the process of utilizing relevant criminal law to protect China's network security, attention must be paid to controlling the degree of expanding the interpretation limits. For instance, using the protection scope of legal interests as the basic criterion for strengthening macro guidance, employing criminal law interpretation as a general standard for reinforcing micro judgments in the enforcement process, and using criminal law technical reasons as a theoretical basis to comprehensively consider and summarize optimal conclusions. In addition, this phase also requires judicial interpretation as the basis for action, embodying the principles of rationality and specificity to achieve re-interpretation.

5.4. Innovation of Regulatory Systems

As cybercriminals increasingly employ the internet as a new means of committing crimes, their methods are continually evolving. This means that traditional legislative charge systems are struggling to apply to new types of crimes in the current information era. Therefore, a genuine improvement in criminal protection for network security is urgently needed. To achieve this goal, relevant departments should actively adjust their legislative approaches, making efforts to avoid controversial issues. Looking at the current state of network security in China, there are two main legislative models for legislation on cybercrimes: independent legislation and integrated legislation. Among these, independent legislation can be further divided into single criminal laws and independent chapter criminal laws. Both of these legislative models have been widely used worldwide, providing numerous case experiences for China to draw upon. Considering the current development in China, it is essential to choose a legislative model that aligns with the national situation to regulate existing crimes that harm network security. It is crucial to continuously evaluate its compatibility with the national situation as the primary criterion [6]. Therefore, considering the factors mentioned above, China currently adopts the integrated legislative model. However, to avoid the shortcomings of a single model, it is advisable to gradually transition towards the independent legislative model. From the perspective of the legislative stage of China's criminal law, relevant departments must improve the relevant sections of criminal charges based on the various crime realities present in the current network environment. In this process, special attention should be given to independently setting up sections for criminal charges and categorizing and classifying criminal charges, which are the two most important tasks. Additionally, in the practical operation of criminal law, legislative bodies should emphasize the normativity and standardization of legislation. This ensures the precision and logical correctness of language expressions when describing criminal charges, preventing criminals from exploiting tactics like confusion or muddying the waters to evade charges. It also ensures the clear denotation of charges and judicial fairness.

5.5. Adjustment of Sentencing Standards

Due to the inherent virtual nature of cyberspace, traditional conviction and sentencing standards in China are challenging to apply to emerging forms of cybercrimes. Examining various cybercrime cases in China's previous experiences, it is evident that the existing conviction and sentencing standards in reality do not match or adapt well to the online environment. This mismatch poses a significant challenge in effectively regulating and sentencing unlawful online activities. To address these issues, a detailed analysis of the current state of the artificial intelligence era in China is required.

Based on this analysis, a comprehensive reform and adjustment of China's criminal law conviction and sentencing standards are necessary. The ultimate goal is to perfect the conviction and sentencing standards in China's cyberspace, exploring guidelines for criminal law that genuinely fit the current online environment in the country. Furthermore, in the operational phase of criminal law, core conviction and sentencing standards should be set based on the severity of harm caused to society by cybercriminals. This involves adapting sentencing standards to different cybercrime methods, the extent of harm to legal interests, specific circumstances of criminal actors, and the concrete impact of criminal activities. For instance, there should be an expansion of quantitative evaluation elements for cyber crimes, promotion of quantitative evaluation standards related to cybersecurity, and an expansion of the monetary standards associated with cybersecurity. On the other hand, efforts should be made to systemize the quantitative standards for criminal charges, ensuring a precise basis for conviction in the sentencing process.

5.6. Establishment of Network Security Management Obligations for Online Service Platforms

The evolution of the types of cybercrimes often synchronizes with the advancements and developments in information technology. Therefore, targeted legislation against cybercrimes should have the ability to promptly eliminate threats arising from these crimes. Cybercrime is often considered a "technology-sensitive" crime. In China, as society rapidly digitizes, networks expand, and intelligence technology progresses, various new crime methods and technologies emerge, reducing the cost of crime and increasing the success rate year after year. This ultimately leads to a sustained increase in the harm caused by cybercrimes to Chinese society. Hence, it is crucial to consider service providers of various online platforms as key entities for the prevention and control of cybercrimes. Only in this way can effective control and investigation of criminal activities related to the platform be carried out promptly upon the occurrence of cybercrime. Additionally, when controlling unlawful activities in cyberspace, emphasis should be placed on the obligation of network platform providers to assume necessary responsibilities for the security management of cyberspace. Currently, many developed countries with advanced information systems have established specific obligations for their domestic network service platforms, such as assisting law enforcement, supervising content information, and protecting user data. Such measures play a critical role in the prevention and control of domestic cybercrime activities.

6. Conclusion

In summary, with the rapid development of the Internet and information technology industry in China, artificial intelligence (AI) is playing an increasingly crucial role in the daily work and lives of Chinese residents. Ensuring the secure use of AI technology, curbing the continuous emergence of new forms of cybercrime, and preventing malicious actors from exploiting network technology for novel criminal activities have become important issues that cannot be ignored in contemporary society. In the current social context of China, the high-speed development of the AI era demands an improvement in the quality of network security. Therefore, there is an imminent need to further deepen reforms and enhancements to China's criminal laws related to network security. Safeguarding network security in accordance with the law is a long-term and complex task. It necessitates the full utilization of the legal system, particularly by enhancing innovation and foresight in the ongoing legislative process of China's criminal laws. This calls for relevant departments to address the root causes of cybercrime, improving China's criminal laws regarding network protection. Ensuring the effective implementation of the law and further refining China's proactive legal framework are essential to better confront the challenges of network security. This, in turn, guarantees the sustainable development of network security in the backdrop of the artificial intelligence era.

References

[1] Wang, S. A., & Zhao, Z. B. (2021). Realistic Manifestations and Sanction Strategies of Cyberterrorism Crimes. Journal of Jiangxi Normal University (Philosophy and Social Sciences Edition), 2021(5).

[2] Zhou, J. H., & Yu, H. S. (2019). Understanding and Application of the "Interpretation on Several Issues Concerning the Application of Law in Handling Criminal Cases of Illegal Use of Information Networks and Assisting in Information Network Crime Activities." People's Judicature, 2019(31).

[3] Tu, L. K. (2016). Obligations of Network Content Management and Criminal Liability of Network Service Providers. Law Review, 2016(3).

[4] Gan, S. P. (2020). Ethical Dilemmas of Freedom and Security. Journal of Hubei University (Philosophy and Social Sciences Edition), 2020(2).

[5] Wang, C. C., Xu, Y. B., Fan, Y. G., et al. (2021). Implementation and Key Technologies Analysis of Computer Network Security Defense System. Network Security Technology and Application, 2021(5), 20-22.

[6] An, K. Y., & Lu, H. (2019). Criminal Protection of Network Security in the Era of Artificial Intelligence: A Perspective on the AI Transformation of Cybercrime. Journal of Yunnan Minzu University (Philosophy and Social Sciences Edition), 2019, 35(6), 145-156.