Research on Legal Issues of Network Information Security

Yang Hui
Teacher of School of Political Science and Law, Zhoukou Normal University, Zhoukou, China

Abstract: The development of network technology goes rapidly, but network information security is a complex comprehensive problem. Law is one of the important means to ensure network information security. Therefore, how to establish the perfect information security related laws and regulations system in the network environment has the very important strategic significance.

Keywords: National Information; Security Information Technology; Network Information Elements

1. Overview of Basic Theories of Network Information Security

1.1 Definition of Network Information Security Concept

Information is a common word in life. The so-called information is defined in the dictionary as "the object transmitted and processed by a communication system, generally referring to events or data." Information security refers to the security of information resources in the process of information transmission and use from generation, production, dissemination, collection, processing to selection, etc. At present, the main concerns of information security are focused on the security of information transmission, the security of information storage and the security of information content in network transmission. information security is a comprehensive concept, and with the development of The Times, its connotation and extension will be more abundant. At present, information security mainly refers to the security of all information system software and hardware including computer system, network and data transmitted, stored and processed on it, that is, the above three aspects.

1.2 The Practical Necessity of Network Information Security Legislation

It emphasizes the urgency of legislation on network information security, not only because information network security plays an important role in realizing information resource sharing, but also because it is a strategic issue to safeguard national network information security, economic security and political security, which is closely connected with national sovereignty. Secondly, network information security legislation is also one of the requirements of security prevention. Internet data security, security, virus transmission and other problems are the common problems in the development of information network. We must resolutely fight against behaviors harmful to the use of information networks. Thirdly, the widespread existence of weak security awareness proves the urgency of legal responsibility for information security.[1] Safety consciousness is not strong, safety technology is backward, is the main problem that causes the safety hazard. The number of unsolicited leaks online is on the rise. Network information security law is one of the protection of the immune system, more important role, its urgency is self-evident.

2. Analysis of Existing Problems in National Information Security

2.1 Legal Punishment Is Low

In cyber crimes, whether it is damaging computer information system or making and spreading virus, the consequences of the crime are often very serious, but the cost of the crime mainly depends on its own network technology, and from the perspective of our legislation and judicial practice, the sentencing of this kind of crime is low, which indirectly leads to the low cost of cyber crime. But on the other hand, in the process of judicial investigation, Law enforcement costs are high, and the incompatibility of these two aspects also allows the prevalence of cybercrime. Taking the crime of making and spreading computer viruses as an example, the "Panda burning incense" virus, listed as the top 10 computer viruses in 2006,

has been widely concerned by the whole society. Virus maker Li Jun and others used the virus to steal user accounts and passwords, destroy user computer systems and hard disk data files, illegal profits of more than 200,000 yuan, but caused hundreds of billions of social losses, Guangdong, Beijing, Shanghai, Tianjin, Shenzhen and other dozens of provinces and cities hundreds of forces. Taiwan Electric.

The brain is attacked. After the case was solved, the four criminals were punished by law for the crime of breaking the computer information system. The main culprit, Li Jun, was sentenced to 4 years in prison, but compared with the serious consequences and bad influence caused by the virus, the sentence was significantly lighter. The current law is unable to determine a specific measure of the value of data files destroyed by viruses, which is also an objective factor contributing to the weak penalties for computer virus creators.[2]

2.2 Restrictions on the Application of Criminal Law

Criminal law, as one of our important basic laws, has many limitations in punishing cyber crime, such as criminal problems of foreigners. At present, foreigners occupy a large proportion of the criminal activities carried out against the network. However, according to Article 8 of the Chinese Criminal Law, if a foreigner commits a crime against our country or our citizens outside the country, the minimum punishment provided by the Chinese Criminal Law is less than 3 years, the Chinese Criminal Law shall not apply; For more than 3 years, the criminal law of our country may apply, but in accordance with the law of the place of criminal punishment is not punished. However, the legal punishment of network information security crimes carried out by most foreigners is less than 3 years. As a result, the criminal law of our country cannot be applied to them. Even if it is the criminal behavior of more than 3 years which causes great harm, we should consider whether the behavior is a crime in the law provisions of their country. This means that the criminal law will appear unadjusted blank field to the greater part of the network criminal behavior. For example, computer hacking is not considered a crime in the Croatian national criminal Code, so if a Croat intrudes into an important area of our national affairs or national defence, even if the consequences are very serious, it cannot be extradited and we have no jurisdiction.[3]

2.3 Cyber Crimes Show A Younger Age

According to the provisions of the Criminal Law, a person who has reached the age of 16 and commits a crime shall bear criminal responsibility; Any person aged 14 or above but 16 who commits the crime of intentional homicide, intentional injury causing serious injury or death to another person, rape, robbery, drug trafficking, fire prevention, explosion or poisoning shall bear criminal responsibility. Any person who has reached the age of 12 but not 14 who commits the crime of intentional homicide or intentional injury, thereby causing death to another person or causing serious injury to another person by special cruel means resulting in serious disability, if the circumstances are egregous and the case is prosecuted with the approval of the Supreme People's Procuratorate shall bear criminal responsibility. The penalty for computer crimes in Chinese criminal law is generally less than five years. In view of the current situation of network information security crimes in China, criminals are obviously showing a trend of younger people, and there is a blank field in the current legal norms, and effective punishment is often unable to be given to those criminals at a lower age.[4]

2.4 The Constitutive Requirements of A Crime Are Too Strict

The laws and regulations concerning information security are limited to the constitutive elements of cyber crime, which is especially evident in the Criminal Law. First of all, the accomplished crime has a strictly limited object of crime. The crime of illegally intruding into computer information systems stipulated in Article 285 of the Criminal Law specifically targets the computer information systems in the fields of state affairs, national defense construction and advanced science and technology. If the perpetrator illegally intrudes into other systems, it does not constitute the crime. However, in real life, a large number of criminals make use of their skilled computer technology. Intrusion into the computer systems of banks, securities, enterprises and other important fields. Even if the data and application programs stored, processed or transmitted in the computer information systems of these important non-state affairs, national defense construction, cutting-edge science and

technology are not modified or deleted, the illegal intrusion itself has damaged or lost the value of these information. And the current legislative system is not enough to effectively and comprehensively protect the security of network information. Secondly, the specific harm result provisions are also relatively narrow, for example, Article 286 breaking the computer information system function crime, must be the computer information system function to delete, modify, increase, interference caused by the computer information system can not run often serious consequences, to constitute a crime, especially serious consequences to constitute a felony, that is to say, Even if the function of the computer system is broken, but does not cause serious consequences, does not constitute a crime. However, there is no specific quantitative standard for the statement of "serious consequences" and "especially serious", and no corresponding judicial interpretation gives clear provisions. For example, in the case of "Panda burning incense", the court ruled that the offender violated Article 286 of the criminal Law and had "serious consequences", but the basis is not clear. In practice, it is generally based on the importance of data or application procedures, large economic loss or bad social impact, but in specific judicial practice, there are still some problems.[5]

3. Put Forward Suggestions on Problems Existing in National Information Security

3.1 Expand the Scope of Protection For Crimes Endangering Information Security

The most typical example of this aspect is the lack of strong criminal protection measures against the infringement of computer communication networks. The Criminal law limits illegal access to computer information and intrusion into computer systems only to the protection of computer systems in the fields of "state affairs, national defense construction, and advanced science and technology," while the criminal law will punish computer systems in other fields only if they "cause serious consequences such as the normal operation of computer information systems." When the computer communication network has become an important way of public communication and information transmission, such a regulation can hardly bear the legal responsibility of protecting the public interest. Increase the intensity of the crackdown. Among all the criminal acts stipulated in the criminal law, all the behaviors related to the manufacture (such as rumour-mongering), publication, dissemination, transmission and application of information, and even illegal acquisition, may directly increase their original social harm because of the use of the Internet. Objectively, the harm of computer crime has been involved in national security and national defense interests. Therefore, it is necessary to adjust the relevant provisions of the Criminal Law according to the new serious crime situation. Corresponding provisions can be added to the crime of endangering national security in Chapter 1 and the crime of endangering national defense interests in Chapter 7 of the sub-provisions, or a separate chapter of the crime of endangering computer and network security can be included to strengthen the fight against computer crimes.

3.2 Legal Liabilities of Network Providers

Internet providers have evaded the law because they simply act as carriers of data and do not participate in editing the information and data they transmit. There are already various corresponding provisions in national laws. If the information possessed is illegal, the law has the power to determine the source of the information. Now, the goal of network security legislation is improving, but on the issue of network service provider responsibility, our law has not clearly stepped forward. Most of our legislation focuses on the "access" stage of network service, but ignores the "management" stage. In particular, the key issue of whether the network provider should bear fault liability or strict liability in the operation is not clearly stipulated. Network facility owners and operators, information controllers and operators, etc., are directly responsible for network information security. Whether it is the security of facilities, the security of information itself, or the security of society and economy, it is directly related to the operation of network and the dissemination of information. Network providers, especially online banking, securities and other departments must have the ability to guarantee security technology, which is also an important part of our current laws and regulations. To require network providers to have the ability of security technology guarantee is to require network providers to undertake the obligation of security guarantee and assume supplementary

responsibility for victims when the injurer cannot confirm.

3.3 Provisions of the Criminal Law on Computer Crimes

Additional property penalty. Because the harm of computer crime is particularly serious, and the perpetrator of computer crime may seek illegal benefits from the crime, the application of property punishment to it can effectively fight crime, so that it can not take advantage of the economy. Therefore, it is suggested that the criminal law should increase the provisions of fine or confiscation of property for computer crimes. Raise the legal penalty range of the crime of trespassing computer information system. The original legal maximum sentence of 3 years was revised to 5 years, in order to achieve the crime punishment, and coordinate with other computer crimes. Additional provisions on unit crime. The unstipulated units in Chinese criminal law can constitute the main body of computer crime. But in practice, it is not uncommon for units to commit computer crimes. Such as a unit in the development of business activities deliberately placed the so-called "Trojan horse" program, in order to achieve the purpose of illegally obtaining business secrets; A company that developed a virus prevention program intentionally created and distributed computer virus programs to gain more business. Therefore, in this case, criminal law should be added to the computer crime unit crime provisions, unit to implement double punishment system.

3.4 Subjective Fault of the Crime of Destroying Computer Information System

It is generally believed that the crime can only be constituted intentionally. And from the provisions of "Criminal Law" Article 286, in addition to the third paragraph expressly stipulates "intentional production, dissemination", paragraph 1 and paragraph 2 are not restrictive provisions on the crime, only the implementation of paragraph 2 behavior caused serious consequences, established the crime, belongs to the result of the crime. Accordingly, the author holds that the crimes in paragraphs 1 and 2 of this article may be constituted by negligence. However, the requirement of harmful consequences and the severity of legal punishment should be distinguished from that of intentionally constituting the crime. Legislation may consider creating another paragraph, "Whoever negligently carries out the acts in paragraphs 1 and 2 of this article, if the consequences are especially serious, shall be sentenced to fixed-term imprisonment of not more than five years or criminal detention." The intention of the legislation is to curb the overconfidence or carelessness of the psychological to the social security of the particularly serious harm, so that everyone using, operating computer should have a high sense of social responsibility, more cautious. As the place of action, result and damage of computer crime are often transnational, so without international cooperation, it is very difficult for one country to punish computer crime completely. As a result, international attention has been paid to the issue. In addition to the eight industrialized countries, 12 countries, including Sweden, Finland, Denmark and Brazil, have signed agreements agreeing to cooperate, allowing law enforcement agencies of participating countries to request immediate legal and technical assistance from participating countries at any time. Therefore, in order to strengthen our efforts against computer crimes, we should join the international cooperation treaty for punishing computer crimes as soon as possible.

References

[1] Zhang Chu. Network Law [M]. Beijing: Higher Education Press, 2003.

[2] Ma Minhu. Research on Information Security Law [M]. Xi 'an: Shaanxi People's Publishing House, 2004.

[3] Ma Minhu. Internet Security [M]. Xi 'an: Xi 'an Jiaotong University Press, 2003.

[4] JIANG Po. Comparison of International Information Policies and Laws [M]. Beijing: Law Press, 2001.

[5] Ning Wei, Yang Hanping et al. Legal Protection of High-tech Industry [M]. Beijing: Xiyuan Publishing House, 2001.

