ISSN 2616-5783 Vol.5, Issue 6: 61-66, DOI: 10.25236/AJHSS.2022.050612

On the Charges of Destruction and Illegal Control of Computer Network Crime —— Taking the Ninth Batch of Guidance Cases of the Supreme People's Procuratorate as an Example

Yuanyuan Sun

Law School of Northwest Normal University, Lanzhou, Gansu, China
1067814908@qq.com

Abstract: *In Chinese Criminal Law, there are great qualitative disputes about the crime of destroying computer information system and the crime of illegally controlling computer information system. There are some phenomenons such as different evaluations of the same behavior, improper expansion of the semantics of the keyword "destruction", improper limitation of the scope of "illegal control" and so on. Taking the ninth batch of guidance cases of the Supreme People's Procuratorate as the starting point, the author analyzes the deficiencies in the identification of the two crimes in theory and practice, and provides a five-step idea to distinguish the difference between this and that crime, and weaken the emergence of this pocket crime and empty crime.*

Keywords: *Crime of destroying computer information system; Crime of illegally controlling computer information system; Qualitative analysis of computer crime*

1. Introduction

The crime of illegally controlling computer information system and the crime of destroying computer information system are two charges which are easily confused and controversial.

<Criminal Law of the People's Republic of China >Article 285 states : Whoever, in violation of the state provisions, intrudes into a computer information system other than that prescribed in the preceding paragraph or uses other technical means to obtain the data stored, processed or transmitted in the said computer information system or exercise illegal control over the said computer information system shall, if the circumstances are serious, be sentenced to fixed-term imprisonment not more than three years or limited incarceration, and/or be fined; or if the circumstances are extremely serious, shall be sentenced to fixed-term imprisonment not less than three years but not more than seven years, and be fined.

<Criminal Law of the People's Republic of China >Article 286 states: Whoever violates states regulations and deletes, alters, adds, and interferes in computer information systems, causing abnormal operations of the systems and grave consequences, is to be sentenced to not more than five years of fixed-term imprisonment or limited incarceration; when the consequences are particularly serious, the sentence is to be not less than five years of fixed-term imprisonment.

Whoever violates state regulations and deletes, alters, or adds the data or application programs installed in or processed and transmitted by the computer systems, and causes grave consequences, is to be punished according to the preceding paragraph.

Whoever deliberately creates and propagates computer virus and other programs which sabotage the normal operation of the computer system and cause grave consequences is to be punished according to the first paragraph.

Where an entity commits any crime as provided for in the preceding three paragraphs, the entity shall be sentenced to a fine, and its directly responsible person in charge and other directly liable persons shall be punished according to the provisions of paragraph 1.

In practice, many similar acts are evaluated as two different charges. In recent years, some scholars state that the crime of destroying computer information system tends to become a *pocket crime*, while the crime of illegally controlling computer information system has become an *empty crime*.

ISSN 2616-5783 Vol.5, Issue 6: 61-66, DOI: 10.25236/AJHSS.2022.050612

Fundamentally speaking, this is due to the careless definition of the two crimes in the criminal law, no particularly clear difference, and no further elaboration of the judicial interpretation. At present, only the Supreme People's Procuratorate has issued some guiding cases to guide practice. Through the further analysis of Supreme Procuratorate guiding cases No. 34 and No. 35, it is found that the prosecution cases do not fundamentally point out the difference between the two crimes, but only one thing and one explanation. At the same time, the qualitative nature of the case is still worth discussing. Therefore, this paper makes reflection and dialectical analysis on the supreme prosecution cases from the following aspects, and puts forward new practical discrimination methods.

From the intention of legislation, the crime of illegally controlling of computer system is a new crime in the criminal law amendment (VII). In order to solve the problem of use theft of computer information system, that is, for some people who do not carry out relevant destructive acts after invading the computer information system, they are the acts of making profits by controlling the computer to carry out specific operations. At the beginning of its establishment, it has its necessary significance, which should be different from the crime of destroying computer information system. The confusion in practice is mainly due to the improper expansion of the semantics of "destruction", the improper restriction of the scope of "illegal control" and the concurrence of legal provisions in the constituent elements of the two crimes.

2. The boundary between illegal control, destruction and serious consequences

Although there is no interpretation in the judicial interpretation, there are three usual situations of *illegal control*: the victim is completely unable to log in to the computer information system (completely exclusive); Can log in to the system, but cannot make corresponding operation according to will (partial exclusivity); You can log in to the system, and the use is not limited, only the system is remotely controlled (non exclusive). In practice, it is easy to appear restrictive interpretation, that is, only when the defendant's behavior completely excludes the victim's use of the computer information system can it be regarded as *illegal control,* and those partial exclusive and non exclusive illegal control behaviors are classified as the crime of destroying the computer information system due to the necessity of imputation, resulting in the abuse of *destruction* and the overhead of *illegal control*.

To what extent does *damage* in the first paragraph of Article 286 of the criminal law mean? Further, are there any restrictions on the object of destruction? The author thinks that three points need to be met at the same time: the object of destruction is the key data, the key function of the computer information network is infringed, and the result reaches the degree of unable to operate normally.

For example, for Taobao's evaluation website, buyer evaluation is the key data (Supreme Procuratorate guiding case No. 34 :The defendant Zeng Xingliang teamed up with Wang Yusheng or used chat social software alone, pretended to be a young woman and chatted with the victim, lied that his apple phone could not log in to icloud (cloud storage) due to failure, asked the victim to log in on his behalf, and tricked the victim to log out of the original ID on his apple phone first, and then log in with the ID and password provided by the defendant. Subsequently, Zeng and Wang immediately logged in to Apple's official website with the new ID and password on the computer, modified the victim's mobile phone settings by using the relevant functions of Apple mobile phone, and modified the password of the ID by using the "password protection problem", so as to remotely lock the victim's apple mobile phone. Zeng and Wang then contacted the victim with online chat software on their personal computers and asked for money on the condition of unlocking. In this way, Zeng Xingliang committed 21 crimes alone or in partnership, involving 22 Apple phones, locked 21 Apple phones and claimed a total of 7290 yuan; Wang Yusheng participated in 12 crimes, involving 12 Apple phones and 11 Apple phones. He claimed a total of 4750 yuan), and evaluation is the most important function of the website, However, deleting comments does not make the website be unable to operate normally (the website can still be accessed without exception). Therefore, the problem of the highest inspection example No. 34 is that the third point does not meet the concept of destruction, but it is characterized as the crime of destroying computer information network. For mobile phones, passwords are the key data (Supreme Procuratorate guiding case No. 35), the correct password can be turned on, and turning on and unlocking is a necessary condition for a mobile phone to realize its functions, so the password can also reflect the important functions of the mobile phone. Changing the password can indeed cause the phone to not work properly (unable to unlock). Therefore, it meets the composition of destruction.

On the contrary, for Taobao's evaluation website, the password may not be the key data, because only the password can not reflect the function of the computer information system and evaluate the function of the website; For mobile phones, photo albums are not the key data in this computer information system.

ISSN 2616-5783 Vol.5, Issue 6: 61-66, DOI: 10.25236/AJHSS.2022.050612

Whether it is the key data should be judged in combination with the nature and function of the specific computer information system. Whether it can not operate normally is also based on the purpose and value of the computer information network, which can not be generalized. In practice, these three aspects are prone to expanded interpretation.

How to understand the *serious consequences* of Article 286 of the criminal law? In terms of the object of crime, the three modes of behavior are respectively aimed at the functions of computer information system, the data and applications stored, processed or transmitted in computer information system and computer system. *Serious consequences* is a necessary condition for the criminalization of the three ways of behavior. The author believes that, as different clauses in the same law, the extension of the word *damage* is small and the extension of the word *serious consequences* is large. The consequences are not limited to economic loss and personal injury. All acts with objective infringement in the legal sense will produce consequences, and the meaning of *serious* is flexible. There are two main bases for a certain behavior to be included in the interpretation path of the crime of destroying computer information system: one is to reduce the standard of *serious consequences*, and define the situation of no obvious consequences, only potential consequences, incalculable consequences or low correlation between consequences and computer information system security as *serious consequences* in the crime of destroying computer information system. See Luo Lu's case of destroying computer information system for details. In this case, the defendant deleted the scores of 9991 candidates by illegally logging in to the information technology grade examination website of primary and secondary schools in Jiangsu Province, which is in line with the deletion of data in the computer storage system in paragraph 2 of Article 286 of the criminal law. The focus of the court trial dispute is whether it constitutes *serious consequences*. The defender believes that it does not constitute damage to the information network, and the website can still operate normally, so it does not belong to *serious consequences*. It can be inferred from common sense that in the official examination, the destruction of the normal examination order and process will have a significant impact on the society. Moreover, the examination results are the key data for the examination website, which of course belongs to the category of *serious.*

3. The relationship between the two crimes and the concurrence of legal provisions

The clear concept only delimits their respective scope, but does the comparison of the two phases produce intersection or no overlap? Is it necessary to destroy the functions or data of the computer information system in order to control the computer information system? Or as long as the functions or data of the computer information system are destroyed, it is impossible to establish the crime of illegally controlling the computer information system? In other words, are they exclusive, mutually exclusive and independent behaviors, or are they inclusive or cross competitive?

Some scholars believe that there may be the possibility of nesting among diversified computer crimes, and the illegal control behavior may show the behavior of deleting, modifying and adding data in practice.

The criminal law stipulates that destruction is caused by deletion, modification, addition and interference, and there is no other revealing behavior. In order to achieve the result of control, these four behaviors are inevitable in the process. Whether it is aimed at the functions of the computer information system, the deletion, modification, addition and interference of the data and application programs of the new computer information system, or the dissemination of computer viruses and other destructive programs, it is an unauthorized operation behavior beyond the authority, and these behaviors themselves will affect the use of the computer information system by the relevant obligees, It is difficult to say that these behaviors are not a control of computer information systems. Therefore, from the objective elements, there are competing parts between them. In terms of results, the degree of control should be less than that of destruction, and control may not produce destruction, but the premise of destruction is control (refer to the analysis of three possibilities of control: complete exclusivity, partial exclusivity and non exclusivity). This view can also be proved by comparing the range of punishment: destruction corresponds to fixed-term imprisonment of less than five years or criminal detention; If the consequences are especially serious, he shall be sentenced to fixed-term imprisonment of not less than five years. Illegal control corresponds to fixed-term imprisonment of less than three years or criminal detention, and shall also or only be fined; If the circumstances are especially serious, he shall be sentenced to fixed-term imprisonment of not less than three years but not more than seven years and shall also be fined. Therefore, the two crimes also overlap to some extent, which is related to the seriousness.

Based on this, there is a concurrence of legal provisions in the constituent elements of the two crimes. Furthermore, it belongs to the absorption relationship, that is, when the connotation of one criminal fact

ISSN 2616-5783 Vol.5, Issue 6: 61-66, DOI: 10.25236/AJHSS.2022.050612

includes the connotation of another criminal fact, the latter has been included in the former, so the former is absorbed. Taking Supreme Procuratorate guiding case No. 35 as an example, when modifying or deleting the data in the computer information system leads to the behavior that the oblige cannot use normally, whether it is defined as the crime of destroying the computer information system or the crime of illegally controlling the computer information system is controversial in practice. Locking other people's mobile phones by modifying account and password, thus depriving others of the right to use, is an illegal control behavior, which is in line with the crime of illegal control of computer information system. However, at the same time, the ID account and password of Apple mobile phone are part of the functions of the computer information system in the form of data. The locking behavior of modifying the ID account and password directly leads to the failure of the operating system of the whole mobile phone, which is also in line with the criminal composition of the crime of destroying the computer information system. The principle of treatment is that emphasizing the law is better than neglecting the law. When there is a destructive behavior, it is recognized as the crime of destroying the computer information system. On the contrary, it belongs to the crime of illegally controlling the computer information system, which can better reflect the characteristics of the adaptation of crime and punishment.

The necessity of establishing a crime cannot be evaluated by the number of facts involved in the case. The reason why illegal control is established (combined with the legislative background) must have its considerable necessity. In practice, the difference between the two crimes is unclear and controversial. In essence, it is not because the two crimes cannot be distinguished, but the complexity of the facts of the case. When the defendant acted, he considered whether he could achieve the "ultimate goal" (money, reputation, etc.), but did not act in strict accordance with the difference between the constituent elements of the two crimes. Based on this, the concurrence relationship between the two crimes is completely normal.

4. Practical ideas

For the identification of such computer information system crimes, we can follow this five parts: whether the object of the crime is the computer information system - what is the specific object of infringement - what is the data - whether the data is key data - whether it has caused damage / failure to operate normally / serious consequences.

First of all, the fundamental difference between computer information system crime and other types of crime lies in the object of crime. This step is to determine the large type of crime. Secondly, the computer information system is a large scope, and its functions include computer storage, transmission, processing, etc. the general crime is aimed at a part of it, which requires a specific analysis of the object of infringement. Furthermore, analyze what the data is and whether the data belongs to the key data for the computer information system. If there is key data, there must be non key data. The judgment standard is whether the deletion or modification has an essential impact on the system. Finally, whether the system can not operate normally or not, this step is to distinguish the confusing crime of destroying computer information system and crime of illegally controlling computer information system. The fourth and fifth steps are easy to be expanded and abused in practice.

In case No. 33, the Internet belongs to the computer information system, the specific infringement object is the router DNS setting, the data is the Internet user traffic, and the traffic is the key data for the profit-making website, resulting in the destruction of making the website unable to operate normally, so it belongs to the crime of destroying the computer information network.

In case No. 34: In order to seek illegal interests, the defendant lipinglong premeditated to modify the domain name resolution direction of large Internet websites, hijack Internet traffic to visit relevant gambling websites, and obtain a commission on advertising and promotion traffic of overseas gambling websites. On October 20, 2014, Li Binglong pretended to be a staff member of a well-known website and cheated the registered service provider of the website to obtain the management authority of the website domain name resolution service by forging the business license of the website company. On October 21, through his account registered on the domain name resolution service website platform, Li Binglong automatically generated the DNS (domain name system) resolution list of the secondary subdomain of the well-known website by using the relevant functions of the platform, modified the IP direction of the subdomain of the website, and connected it to the advertising page of the gambling website established by renting an overseas virtual server. At about 19:00 on the same day, Li Binglong's modification to the domain name resolution server of the website took effect, resulting in the normal operation of the website. At about 23:00, the well-known website resumed its normal operation after

ISSN 2616-5783 Vol.5, Issue 6: 61-66, DOI: 10.25236/AJHSS.2022.050612

technical investigation. On November 25, Li Binglong was arrested by the public security organ. At the time of the crime, Li Binglong failed to make a profit. the Internet belongs to the computer information system, the specific object of infringement is the internal evaluation system of the shopping website, the data is the buyer's comments, and the buyer's comments are the key data of the evaluation system, which has not caused the damage of *abnormal operation* (there is no problem with the use of the evaluation system). Therefore, the author's view is different from that of the Supreme People's Procuratorate, and believes that the case does not meet one of the five elements, Therefore, it does not belong to the crime of destroying the computer information system, and because the two crimes have the concurrence of absorbing laws, it belongs to the crime of illegally controlling the computer information system.

In case No. 35, the mobile phone belongs to the computer information system (refer to Article 11 of the interpretation of the Supreme People's court and the Supreme People's Procuratorate on Several Issues concerning the application of criminal cases endangering the security of the computer information system). The specific object of infringement is the apple mobile phone ID, the data is the mobile phone password, and the mobile phone password is the key data for the unlocking and use of the mobile phone. Although the mobile phone is controlled, However, it also causes the damage of unable to start up and normal operation, so it belongs to the crime of destroying computer information system.

Some scholars pointed out that the model of shortened two act crime is used to distinguish the two crimes, that is, to recognize the influence of the actor's subjective purpose on the objective result. It requires the perpetrator to have a specific purpose subjectively, but does not require the realization of the specific purpose. It is a form of crime in which the subjective elements are more than the objective elements and include the subjective elements of overflow objective elements. Its basic feature is that the complete criminal act originally consists of two acts, but the criminal law stipulates that as long as the perpetrator implements the first act for the purpose of implementing the second act, he will be punished as a crime (accomplished); If the perpetrator does not take the implementation of the second act as the purpose, even if he objectively implements the first act, he will not establish a crime (or only establish other crimes). The author holds a negative view on this. Whether there is the purpose of destruction or control is not only difficult to verify afterwards, but also violates the legal theory, especially in criminal cases, we should follow the basic principle of consistency between subjectivity and objectivity. Take a malicious mining case as an example: on June 4, 2018, the security management department of a company found that the server used by the company for daily business was running abnormally. It is suspected that the mining program was maliciously deployed by others and occupied the computing resources of the company's server. After internal investigation, it was found that the perpetrator used the company's intranet computer information system to compile the mining program, and took advantage of his work to log in for many times from January 26 to May 30, 2018, and deployed the mining program on the internal server in batches to obtain virtual currency. After investigation by the public security organ, it was found that during the period from January to July 2018, the perpetrator an took advantage of the convenience of operating and maintaining the internal server in the company, deployed the application through technical means, and exceeded the authorization to use the internal server of the enterprise to obtain virtual currencies such as bitcoin and Monroe currency, with an illegal income of RMB 100000. The subjective purpose of the perpetrator must not be to hope that the computer information system will be damaged. Once so, bitcoin cannot be obtained. However, from the objective result, if the function of the computer system is not damaged, it is impossible to illegally enter the system. Then subjective pushing objective falls into the paradox of purposeful behavior and process behavior. Moreover, the defendant often defends with a lighter subjective purpose in order to avoid responsibility.

5. Theoretical supplement

At the normative level at this stage, justice is ahead of legislation. Due to the careless legislative provisions, typical cases and guidance suggestions have to be issued in the administration of justice, but the forms of cybercrime emerge one after another, which always lags behind the actual situation. Fundamentally speaking, the legislation lacks the definition and difference between computer professional interpretation and legal interpretation. Many terms are completely different in the field of computer, in the field of law and in the general interpretation of ordinary people. Taking the concept of computer information system as an example, we all think that computer is computer, and Article 11 of the interpretation of the Supreme People's court and the Supreme People's Procuratorate on Several Issues concerning the application of law in handling criminal cases endangering the security of computer information system: the *computer information system* and *computer system* mentioned in this interpretation refer to systems with automatic data processing functions, including computers, network equipment, communication equipment Automatic control equipment, etc. In the field of computer

ISSN 2616-5783 Vol.5, Issue 6: 61-66, DOI: 10.25236/AJHSS.2022.050612

specialty, the scope of computer is wider than this. What is the storage system, operating system, deletion and destruction? These specific behaviors and terms need to be further explained. The more detailed the explanation, the smaller the deviation in practice.

6. Conclusions

There are five steps to distinguish the crime of destroying computer information system from the crime of illegally controlling computer information system: Computer Information System - specific object of infringement - Data - whether the data is key data - whether it has caused damage / abnormal operation / serious consequences. It is urgent to improve the legislation and judicial interpretation. In practice, it is also necessary to distinguish the fundamental differences between the two crimes and analyze them in combination with the specific circumstances of the case.

References

[1] Hu Yunteng. Opinions on criminal procedure of cybercrime and understanding and application of relevant judicial interpretations [M]. Beijing: People's court press, 2014:109, 94-9.
[2] Yu Xiaohai. Judicial practice analysis and normative meaning reconstruction of the crime of destroying computer information system [J]. Law of Jiaotong University, 2015 (03): 140-154 DOI: 10.19375/j.cnki. 31-2075/d.2015.03.013.
[3] Li Gang, Li Tao. Discrimination between the crime of illegally controlling computer information system and the crime of destroying computer information system -- from the perspective of short two act crime [J]. Chinese prosecutor, 2021 (14): 38-41.
[4] Wang Yu. A behavioral perspective of computer information system crime -- from the perspective of the boundary and concurrence of "destruction" and "illegal control" [J]. Journal of Jiangxi Police College, 2019 (02): 108-113.
[5] Liu Hongyan. A study on the elements of the purpose of shortening the second act crime [J]. Politics and law, 2014 (07): 138-146 DOI: 10.15984/j.cnki. 1005-9512.2014.07.001.
[6] Zhang Mingkai. On the Shortened Crime of Two Acts [J]. China law, 2004, issue 3.