Proceedings of the 4th International Conference on Educational Innovation and Philosophical Inquiries
DOI: 10.54254/2753-7048/17/20231220

Research on Recognition Standards of Destructive Programs in Digital Crime

Jinglan Ding[1,a,*]

[1]*Faculty of Law, Chengdu College of Arts and Sciences, Chengdu, 610066, China*
a. dingjinglan@cdcas.edu.cn
**corresponding author*

Abstract: Destructive programs in computer network systems have become the leaders in digital crime in contemporary society. However, the current laws for judicial recognition of destructive programs are not yet clear enough, and judicial personnel still need to combine their own experience to efficiently judge whether criminals use destructive programs to conduct internet Crime. This article will use the case study method, based on the case of Zhang Chaojie's destruction of a computer information system, combined with document collection and empirical analysis, and analyzing the recognition dilemma, reasons and improvement measures of destructive programs with specific reference to 100 typical cases of destructive program crime in conjunction with legal interpretation, and the empirical results show that there are many types of destructive programs, so their concepts and identification procedures should be clearly defined.

Keywords: digital crime, destructive programs, recognition dilemma

1. Introduction

The rapid development of computer technology has left a heavy mark on human civilization. It not only drives the economic, market, and technological development of the entire era but also leads to the fourth industrial revolution—the information technology industry revolution. With the rapid development of computers, some traditional crime patterns are gradually being phased out. Due to the drawbacks of the current legal recognition standards for destructive programs in terms of concept confusion and non-rigorous judicial procedures, illegal elements have also raised their "value" and switched to committing crimes on the Internet, causing damage to prevent computers from operating normally [1-3]. Consequently, the damage becomes the key punishment object of digital crime. The definition of destructive programs has not yet been clearly defined in the Criminal Law of the People's Republic of China, causing many criminals to turn to create operations that embed legal programs in computers to prevent them from operating normally or directly or indirectly cause damage to computer network systems through destructive programs. In this passage, cybercrime does not suitable for using to describe the process that is brought by criminals as the conception is a criminal activity that either targets or uses a computer, a computer network, or a networked device. Most cybercrime is committed by cybercriminals or hackers who want to make money [4, 5]. This means that this form of crime cannot find a specific culprit, while digital crime can do so. The article is based on traditional crimes, so it applies to digital crime or internet crime.

DOI: 10.54254/2753-7048/17/20231220

In Zhang Chaojie's case, the Bull Helper software developed by the defendant Zhang Chaojie during his previous employment could interfere with the unauthorized processing and transmission of geographic location data of the victim's unit's DingTalk system to obstruct its function of acquiring a user's real geographic location. When judicial practice handles the case, different recognition models appear in the recognition of destructive programs, which seriously reduces the trial efficiency of the case [6]. Therefore, to improve the judgment efficiency of judicial practice for future cases of destructive programs, this article will provide some modest contributions around the recognition model of destructive programs.

2. Analysis of Identification Dilemma of Destructive Programs

2.1. Ambiguity in the Concept of Destructive Programs

In the academic and theoretical community, there are many definitions for destructive programs. Firstly, according to Article 273 of the Russian Federation Criminal Code, which is implemented in Russia, the standard for identifying destructive programs is a program that can destroy, modify, or prevent the normal operation of a computer program, or a program that can occupy computer resources, destroy computer systems or networks. According to Articles 168 and 179 of the Japanese Criminal Code, it is known that a destructive program must be a program that is intentionally inputted or changed without authorization, to destroy computer data or interfere with computer functions, causing damage to others [7,8]. According to Section 35 of the United Kingdom Criminal Code, a destructive program refers to a program or code that can destroy, interfere with, or otherwise affect computer systems, data, or programs. In domestic judicial determinations, according to 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 Involving Endangering the Security of Computer Information Systems", the applicable objects of destructive programs are (1) able to replicate, spread, and damage computer system functions, data or application programs through networks, storage media, files, and other media; (2) able to be automatically triggered under pre-established conditions and damage computer system functions, data or application programs; (3) other programs specially designed to destroy computer system functions, data, or application programs. Only destructive programs that meet the above three conditions can be identified as destructive programs.

Secondly, in the "Operational Specifications for Destructive Procedure Inspection" issued by the Judicial Appraisal Management Bureau, the definition of a destructive program refers to an application program that unauthorizedly acquires, deletes, adds, modifies, interferes with, etc. the functions of a computer information system or data stored, processed or transmitted in the computer information system. In other words, the determination criteria for a destructive program require that the user has not authorized it. There are similarities and differences between the two viewpoints to some extent. The similarity lies in that the attack targets the systems and data in the computer network system, making them lose their normal functions. The difference lies in the ambiguous definition of the behavior mode. The former upholds behaviors such as replication and dissemination, while the latter holds behaviors such as acquisition, deletion, addition, modification, and interference, and there are also legal hierarchical issues involved. Therefore, the concept of destructive programs cannot be efficiently applied in specific cases. When defining whether a program belongs to a criminal case on a computer, it is not only necessary to examine whether it has the function of acquiring, controlling, or interfering with computer information system data, but also to focus on the subjective motives of the creators and users of such programs. Only those programs that have the function of bypassing or breaking through computer information system security measures without obtaining corresponding authorization or exceeding authorization and

DOI: 10.54254/2753-7048/17/20231220

obtaining the function of acquiring computer information system data or implementing system control belong to "destructive programs" as specified in computer crime cases. In conclusion, the dilemma is that in judicial practice, it is difficult to directly convict and sentence criminal behavior based on the provisions of destructive programs specified by laws or judicial interpretations.

2.2. The Identification Process of Destructive Programs Is Questionable

The judicial appraisal opinion on the identification process of destructive programs is one of the types of case evidence, which is an important basis for public security judicial organs to determine crimes and accurately sentence. During the identification process of destructive programs, several issues greatly hinder the accuracy of the trial. Firstly, the identification technology is outdated. With rampant electronic crime, the demand for evidence-collection tools by judicial organs has become stronger, which has also led to the market for foreign evidence-collection product tools. However, due to the lag in the development of computer and judicial appraisal theory, it is impossible to sort out a unified standard for evidence-collection processes. Research and practice related to computer forensics are still in the initial stage. Regardless of the required software or equipment, domestic law enforcement agencies mainly use foreign products and standards for computer forensics and execution of operating procedures have not yet been established. Secondly, the nature of the judicial appraisal opinions issued by professional institutions for technical-level identification of destructive programs varies. In practice, different appraisal institutions often issue different appraisal opinions for the same case and the same appraisal application. Regarding the effectiveness of appraisal opinions, the law has no clear provisions, and the "Decision of the Standing Committee of the National People's Congress on Judicial Appraisal Management Issues" only provides regulations on the management of judicial appraisal personnel, the establishment of appraisal institutions, and the operation management system of judicial appraisal institutions. However, no provisions have been made regarding the relationship between appraisal institutions, the geographic scope of appraisal institution appraisals, and the effectiveness level of monitoring opinions.

2.3. The Analysis of the Reasons for the Identification Dilemma of Destructive Programs

The Extensiveness of the Connotation and Extension of Destructive Programs Firstly, the basic connotation of destructive programs is programs that can cause damage to computer network systems. How damage is inflicted is diverse, resulting in a wide range of extensions for destructive programs. According to one viewpoint proposed in the "Interpretation of Several Issues Concerning the Application of Law in Handling Criminal Cases Involving Endangerment of Computer Information Systems" by the Supreme People's Court and the Supreme People's Procuratorate, not all programs that obtain or control computer information data and systems fall within the scope of criminal law regulation. Some programs are deemed "neutral programs," which means they do not have a certain level of aggression and should therefore be fully recognized in conjunction with judicial practice [9]. Based on the content of the "Interpretation" and 100 cases consulted on the China Judgements Online, the targets of destructive programs include the following seven points: (1) programs that can achieve hacker functions after compilation; (2) programs that illegally control other people's computer information systems by technically making it possible to accept commands issued by them; (3) programs that circumvent legal management mechanisms by connecting to platforms and interfering with the normal operation of the system by communicating with related user information; (4) programs that obtain, add, modify, and interfere with the function and data of the system without authorization; (5) programs that criminals purchase to engage in illegal online sales to the public; (6) programs that damage the normal operation process and running mode of the official program by external attachments; (7) programs that provide functions not offered by the

DOI: 10.54254/2753-7048/17/20231220

official client. From the above seven points, three categories can be finally summarized: (1) illegal control of computer network systems based on technical means; (2) unauthorized acquisition, addition, modification, and interference with computer network systems; (3) providing functions that the public does not have in computer network systems. From the above three points, it can be seen that the extension of destructive programs is quite extensive.

At present, the author can only understand the fundamental nature of destructive programs according to the context, that is, a program that possesses self-replication, unauthorized access, or spontaneity (which can be regarded as an extension of unauthorized access) and is capable of damaging the functionality, data, or application programs of a computer information system is considered a destructive program. Therefore, it is clear that "Big Bull Helper" is a non-destructive program since users need to download and install the software themselves before engaging in destructive behavior, and it does not possess spontaneity. The diversity of connotation leads to the diversity of extension, which also makes it difficult for judicial workers to efficiently solve cases. Therefore, the definition of destructive programs should be specifically defined.

2.4. The Appraisal Process May Have Errors

The general approach taken by the appraisers is to compare intact computer information systems with damaged ones, analyze the differences, and identify the points where destructive programs escape detection by the computer network system. This is crucial in judicial decision-making, as it largely determines the conviction and sentencing of criminals. For example, in determining whether or not cheating software constitutes a destructive program, the first step is to locate the software, followed by installing it for later comparison with the original software, and finally, to analyze the reasons for its ability to evade detection by the computer network system. If an appraisal report fails to reflect this complete and adequate appraisal approach, its validity and truthfulness remain to be verified. Each step of the appraisal process is essential and must be strictly carried out according to the requirements. The adherence of destructive program appraisal to the professional standards set by computing appraisal regulations decides the admissibility and final acceptance of the appraisal report by the court, which may directly determine the conviction or acquittal of computer-related cases. In judicial practice, the emphasis is often placed on checking if the appraisers and the appraising institutions comply with relevant laws and regulations, while the professional standards of the appraisal process and methods are often overlooked. In contrast, the process and methods are important indicators that can measure the truthfulness of the appraisal results. Thus, any deviation in the appraisal process can render the appraisal report inadmissible. If problems exist in the appraisal process and methods but are not discovered, subsequent review work is likely to be flawed, creating a vicious cycle that leads to wrongful convictions and miscarriages of justice. This not only raises suspicion about the professional competence of the handling officers but also erodes public trust in the judiciary, thereby disrupting market order. Therefore, the appraisal process should be strictly regulated.

3. The Improvement Measures for Identifying Destructive Programs

3.1. Defining the Concept of Destructive Programs

Destructive programs can be divided into two categories: computer viruses and non-computer viruses. Therefore, in order to define the concept of destructive programs clearly, it is necessary to understand the concepts of computer viruses and non-computer viruses first. According to the interpretation of Article 28 of the Regulations on the Protection of Computer Information Systems Security, computer viruses can replicate a set of computer instructions or program code, and compile or insert computer programs on their own to damage data or computer functions. It can also

DOI: 10.54254/2753-7048/17/20231220

be considered a type of computer virus that requires a legitimate program to run and actively spreads to other computers through self-replication in order to damage the components, data, or software built into its system [10]. Non-computer viruses, on the other hand, are generated based on malicious intent and hidden within executable programs or data files, running inside the computer. In judicial practice, destructive programs in the category of computer viruses not only damage the software functionality of the computer but also cause damage to the hardware, which can change parameters and cause damage to the hard drive under high-intensity action. Generally speaking, the concept of destructive programs in the category of computer viruses needs to have the following conditions: it must be able to self-replicate and have a legitimate program as a carrier to damage the internal functions, data, or application programs of the computer system. The concept of destructive programs in the non-computer virus category is a program that generates destruction inside the computer, hidden in executable programs or data files based on malicious intent.

From the perspective of criminal prosecution, the concept of destructive procedures is particularly important. Almost all convictions and sentences are based on the norms and articles of the criminal law. Therefore, judicial authorities should summarize the differences and similarities of typical criminal cases, extract the most authoritative legal concepts for identifying destructive procedures, and improve the efficiency of judicial practice and trial while promoting the development of legal practice. From the perspective of judicial practice, a clear definition of the concept of destructive procedures is beneficial to various judicial practitioners in accurately determining the applicable legal provisions for criminal behavior, speeding up the investigation and handling of cases, and saving judicial resources to a great extent.

3.2. The Process for Identifying Destructive Programs Follows Certain Rules and Regulations

Firstly, if unsure whether a program is destructive, an evaluation agency at or above the provincial level can be commissioned for identification. Secondly, it is necessary to ensure that the review and identification process conforms to the requirements of the “Destructive Program Inspection Operation Specification” and the “Software Function Identification Technical Specification”. Thirdly, according to Articles 97 to 101 of the Criminal Procedure Law of the People’s Republic of China, the evaluation opinion should focus on whether the technical methods used in the evaluation opinion, as well as the examination process, and subsequent identification agency authenticity, evaluator avoidance system, and acquisition of inspection materials, comply with legal provisions. Thus, the evaluation opinion plays a crucial role in the case itself, and the judicial authorities should combine judicial interpretations and practice, jointly improve identification technology, and review systems. For example, they should clarify the legal status of identification technology, establish appropriate standards and thresholds for identification technology, and prohibit unqualified personnel from using it. Also, attention should be paid to matters before, during, and after the use of technology. The review mechanism should be further improved based on relevant provisions of the Criminal Procedure Law and must not violate the standards of review. All legal requirements should be strictly reviewed, and the accuracy of the identification technology should be strictly controlled. This will lead to fair conviction and sentencing of criminal behavior. In judicial practice, correct evaluation opinions are important supporting materials, but judges will also make value judgments and, based on the “freedom of belief” system, together judge the case fairly.

3.3. Judicial Determination of “Disruptive” Programs Categorized as “New Technology”

In the rapidly developing 21st century of networks and big data, various industries have normalized the use of network technology. Many criminal activities have also surpassed traditional crime limits

and no longer use physical tools such as knives, hammers, and ropes to commit crimes. Instead, seemingly legal actions such as exposing orders and pushing notifications are used to invade users' mobile phones and computers, impacting the normal operation of user devices, ultimately stealing personal information such as user privacy and achieving fraudulent purposes.

However, this phenomenon lacks a complete response mechanism in the current legal enforcement practice. For example, when discussing an interesting topic with friends, the device may record words and accurately push the information that want to collect or know to the application. During this process, the device decodes customer privacy information, leading to the theft of user privacy information and invisible property losses caused by users being unaware. Due to the inability of existing laws to keep up with technological development, there is a backward trend, and the recognition of this new destructive program and the issue of compensation for the losses suffered by victims have become urgent problems that need to be resolved. So far, there haven't been any cases that need to be judged by a court in current judicial practice because an inherently illegal program has been given a "legal" guise, and the public doesn't care too much about their leaked privacy because they haven't suffered significant losses, so they neglected to pay attention to this phenomenon. These programs can only be effectively reduced through effective regulation by judicial interpretation to control illegal behavior leading to criminal phenomena. However, there are such cases abroad, due to different judicial systems and practices in these two countries.

4. Conclusion

Digital Crime is a hot topic in today's society, and the use of destructive programs for criminal activities is not uncommon. However, existing laws cannot keep up with technological innovation and development, resulting in lagging regulations. From a legal perspective, relevant judicial interpretations should be timely issued to regulate this phenomenon. From the perspective of computer network systems, the public should strengthen their awareness of network security. Technological innovators should innovate within legal boundaries, and relevant departments should increase supervision and management of computer technology to minimize and regulate network crimes that use destructive programs as means.

References

[1] *Zhu, H. (1999) On the Main Characteristics of Production and Spread of Destructive Computer Virus and Other Criminal Computer Programs. Legal Review. 5, 108-112.*

[2] *Zheng, H. Y. (2018) Qualification of Illegal Intrusion into Computer Systems and Demanding Bitcoin [D]. Southwest University of Political Science and Law. 7, 14-21.*

[3] *Che, C. (2020) Research on Computer Crime Series (VII) How to Understand the "Destructive Programs" in Computer Criminal Cases [EB/OL].*

[4] *Sun, Q. (2014) Reflection on the Establishment of the Crime of Producing and Spreading Destructive Computer Virus and Other Programs. Jilin University. 04, 55-59.*

[5] *Chinalabs :Research Report on Rogue Software and Countermeasures in China, (2016) , Retrieved from: http://www.chinalabs.com/.*

[6] *Yu, X. H. (2015) Judicial Practice Analysis and Normative Meaning Reconstruction of the Crime of Destroying Computer Information System, in: SJTU Law Review, 3, 140-154, DOI: 10.19375/j.cnki.31-2075/d.2015.03.013.*

[7] *Feng, J. (2014) The Standpoint and Method of Criminal Law Dogmatics, in: Peking University Law Journal, 1, 172-197, DOI: CNKI:SUN:WFXZ.0.2014-01-010.*

[8] *Wang, X. M. (2019) How to determine the crime behind "crazy traffic", in: Beijing Daily, 6, 014.*

[9] *Zheng, Y. M., Zheng, H. F. (2018) Research on Cross-border Personal Data Protection and Relief Mechanism in the Internet Era——Taking "EU–US Privacy Shield" as an Example, in: Journal of Guangxi University(Philosophy and Social Science), vol.02.2018, pp.42-48, DOI:10.13624/j.cnki.jgupss.2,6.*

[10] *Guo, Q. (2020) A Compilation of Interpretations of Technical and Legal Terms for Cybercrime Cases by the First Office of the Supreme People's Procuratorate, Post & Telecom Press, Beijing.*