Legal Risk of Electronic Forensics and Standardization of Forensics

Xiaoyi Yuan

Xi'an Peihua University

yuan150289@163.com

Keywords: Electronic Forensics; Electronic Evidence; Legal Risk; Standardization of Forensics; Process of Forensics

Abstract: With the popularization of electronic information technology represented by the Internet, human society has fully entered the information age. Illegal and criminal activities have also followed the development of information technology in a large number of new situations, and electronic data has widely appeared in various types of crime. Electronic forensics to a certain extent puts forward new requirements and brings new challenges to the technical work of forensic evidence collection. How to regulate electronic evidence collection procedures and achieve effective electronic evidence collection is bound to become an important issue at present. The purpose of this article is to study the legal risks and standardization of electronic forensics. This article introduces the concept of electronic evidence to complete the conceptual understanding and grasp of electronic evidence. Then on this basis, it introduces the process of electronic forensics and points out the legal risks that may exist in the process of electronic forensics. In the experimental part, a questionnaire survey method was used. In this paper, 100 subjects were selected. The question "What do you think of the implementation of the 2016 Regulations and the 2017 Cyber Security Umbrella Law?" Respondents found it difficult to implement and needed improvement. Aiming at the difficulty of law enforcement, this article puts forward suggestions to promote the standardization of electronic forensics.

1. Introduction

At present, various forms of crimes relying on computer, Internet and other information technology as criminal tools are also emerging. Cybercrime is a new type of crime committed with the help of a network platform and the use of modern network technologies. It is characterized by rapid crime, strong concealment, difficult evidence, and difficulty in locating the perpetrator. As an independent type of evidence, electronic evidence is still in its infancy in China. The collection of electronic evidence, the methods and techniques of electronic evidence collection, and the verification and identification of electronic evidence often require certain scientific methods and judgments. Provisions. In order to make electronic evidence the basis for criminal law proving during the public prosecution stage, the legality of electronic evidence collection and its relevance to relevant facts must be examined and judged before they can be accepted. Because electronic evidence has the characteristics of general evidence in addition to its unique characteristics, it discusses the issues in judicial practice in order to provide some reference for judicial personnel in this way, and promote electronic evidence to fight for social justice and fairness aspects play a role.

According to the technical classification of electronic forensics and the framework of China's laws, the electronic forensics system can be divided into two categories: the first category is the acquisition of internal data of electronic equipment, which can

be understood as electronic computer forensics, but the computer collection here the broad concept refers not only to computers, but also to various types of electronic equipment with functions such as storage, calculation, and control [1-2]. China's "Criminal Procedure Law" legal provisions for this type of electronic evidence collection are mainly inspection, inspection and search, seizure [3]. The second type is to obtain evidence through electronic means. This type of electronic evidence collection is not clearly defined in China's criminal procedure law, but according to the method and form of evidence collection, it is generally classified as technical investigation [3-4]. The legacy of network data and the processing of personal computer data formed in the era of big data have brought technical obstacles to the recovery, extraction, restoration, preservation, collection, use, and legality confirmation of electronic evidence [5]. Mainly: the degree of electronic evidence data restoration, the legitimacy of the extraction of evidence data, the remediation of irrecoverable evidence data, the preservation of legally extracted evidence data [6]. At present, in the absence of legislation on electronic evidence in China, how to legally regulate the procedures of electronic evidence collection to achieve the reliability of electronic evidence collection [7].

This article introduces the concept of electronic evidence to complete the conceptual understanding and grasp of electronic evidence. Then on this basis, it introduces the process of electronic forensics and points out the legal risks that may exist in the process of electronic forensics. In the experimental part, a questionnaire survey method was used. In this paper, 100 subjects were selected, and statistics and analysis were performed on the implementation of relevant laws and regulations. 47% of the respondents thought that implementation was difficult and needed improvement.

2. Method

2.1 Electronic Evidence

Electronic evidence can be divided into the following three types: one is the electronic data that computer applications (word files, excel forms, images and voice, video files), computer databases, computer logs and other computer technology applications will be displayed; the second is Online electronic transmission records, voice chat records, QQ, WeChat chat information are electronic data displayed based on the widespread use of the Internet; thirdly, electronic data appearing in communication technology applications, such as information stored in communication equipment, call records, and MMS , Mobile phone positioning information[8-9].

2.2 Electronic Forensics

At present, China's electronic forensics procedures generally go through the following stages: First, the basic preparation stage of electronic forensics [10]. It involves the qualification review of the forensic subject, the implementation of forensic technology and equipment, the release of information sources and the planning ideas for the design of electronic forensics. Secondly, the preliminary implementation stage of electronic forensics. At this stage, investigators conduct forensics on devices in real space such as mobile phones and computers, as well as remote downloading and forensics of networks in virtual spaces, both forensics will secure the electronic evidence collected and seize it [11]. Third, the implementation of electronic forensics. The main operation task is to back up the electronic evidence,

save the original equipment of the electronic evidence, and then analyze and test the duplicates to extract the relevant data of the case. Finally, the stage of summary and identification of electronic forensics results. The electronic evidence passes the third stage of analysis and inspection, and reports such as the conclusion of the conclusion of the evidence collection and the record of the investigation are produced. The four stages are linked up and down, and the electronic forensics results obtained may not be finalized. If problems are found in the forensics during the analysis and inspection process, according to the degree of credibility and probabilistic power of electronic evidence, if necessary, consider restarting the second stage, which is in accordance with the provisions of the evidence collection system in our criminal procedure law [12]. Electronic evidence is the legal evidence independently provided by the new criminal procedure law, and it is a legal issue related to information technology. We should pay attention to its particularity. Now that electronic evidence has been given legal status, the electronic evidence collection system should be more standardized.

2.3 Legal Risks

(1) Lack of legislation and lack of operational guidance on the application of electronic evidence

In China's current laws and regulations, there is currently no separate "Evidence Law", which is a natural deficiency in legal origin for electronic evidence. At present, the more mature legal requirement for electronic evidence in the judicial practice is the "Electronic Signature Law", which mainly regulates the rules of transaction behavior in the field of e-commerce, and solves the problem of the evidence ability and proof power of electronic signatures, but it has not formed a complete System, the judgment standards of electronic evidence are more controversial, and the legal interpretation is often ambiguous; and the rules and regulations on the collection, preservation, review judgment, and demonstration of electronic evidence are also very incomplete.

(2) Inconsistent adoption standards for electronic evidence collection and probative power

There are inconsistent standards for the adoption of electronic evidence forensics and probative power. There is a lack of uniform standards for the use of electronic evidence in different departments. Although the Criminal Procedure Law clarifies the legal status of electronic evidence, there is no detailed regulation on how to obtain, fix, analyze, appraise, and show evidence, and the current judicial interpretation or the laws and regulations of the department have no relevant details. It is stipulated that this results in various departments processing data according to their own set of methods, such as the methods and procedures of electronic evidence inspection and identification carried out by some grass-roots public security, procuratorial, and judicial departments, which do not form a uniform standard of evidence. Electronic evidence is easy to be transformed into other traditional evidence forms under certain conditions, which makes its judgment on the value of evidence ambiguous.

3. Experiment

3.1 Research Object

In order to ensure the comprehensiveness of the research results, this experiment selected 100 survey respondents from ten industries including Internet, finance, education, construction, real estate, and manufacturing. High school, high vocational.

3.2 Research Methods

On October 1, 2016, the "Provisions on several issues concerning the collection, extraction and examination and judgment of electronic data of criminal cases" were implemented. On June 1, 2017, the cyber security law was also officially implemented. This is the first time that cyber security issues are regulated Written law, only about three years after its promulgation, the use of questionnaires can reflect the actual implementation in judicial practice.

There are eleven questions in the questionnaire. What is your age? What network products do you use frequently? What do you think is personal information? Have you experienced personal loss caused by leaking personal information on the Internet? Do you think the reason for the personal information leakage problem is serious? What do you think of the current state of network security in China? How much do you know about China's related laws on network security? What do you think of the implementation of the 2016 Regulations and the 2017 cyber security umbrella law? Do you think that privacy protection can be put in place in the current electronic data search? Do you think that the current cyber security vulnerabilities have challenged the legality boundary? Do you think What is the significance of the promulgation of the cyber security law?

4. Discussion

4.1 Experimental Results and Analysis

In response to the question "What do you think of the implementation of the 2016 Regulations and the 2017 cyber security umbrella law", the responses of respondents were collated and analyzed, and most respondents found that the implementation of cyber security regulations is still relatively in an imperfect stage. The survey results are shown in Table 1 and Figure 1:

Table 1. Experimental results

Answer	Rate (%)
In place	36
Needs to be improved	47
Not implemented	14
Other	3

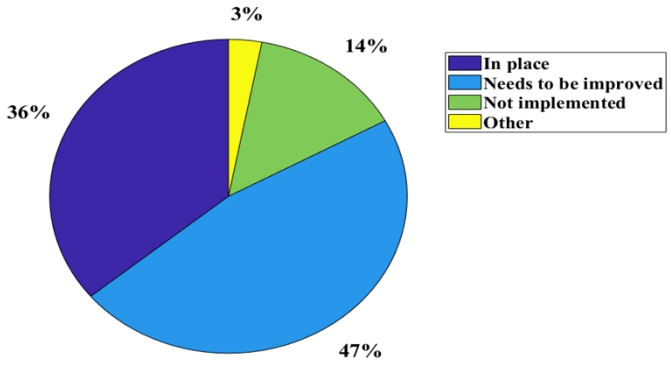

Figure 1. Experimental results

36% of the interviewees are optimistic that the implementation of the new law is better and the law is advancing with the times. 47% of the interviewees believe that the actual implementation is still gradually improving. There are four reasons for this: First, the development of electronic evidence is not mature. As a new thing, there is still a cognitive process, and everyone's consciousness has not reached a level. Due alertness and sensitivity should be strengthened. Secondly, the functions of relevant departments are not clear at the time of implementation, the supervision force is insufficient, and the coordination between the departments is not enough. It is difficult to obtain evidence in network cases, and it is also difficult to identify suspects. Third, there is a contradiction between the protection of rights and cracking down on illegal activities. The self-protection of major network operators and the monopoly of data make it difficult to detect and obtain evidence, and the real-name system under interests cannot be realized. 14% of the interviewees believe that the implementation is not in place, mainly due to the large increase in Internet cases in recent years, the legislation has clearly failed to keep up with the situation, and the regulations have lagged behind the status quo. Although new laws have been issued, there are still many problems that can be explored also many. In the specific implementation, because the real name system is not in place, almost all cyber fraud cases are operated with virtual identities, which also makes investigation and evidence collection difficult.

4.2 Recommendations for the Standardization of Electronic Forensics

(1) Develop guidelines for electronic evidence identification

Only when the standards and norms of electronic evidence forensics work are formulated, can the electronic evidence forensics work be carried out reasonably and effectively, and the forensic work can be reasonably followed. If we want to work out reasonable standards for electronic evidence collection, we must formulate perfect forensics standards for each step of the collection. Evidence identification is the beginning part of the forensic work, and it plays a very important role in the entire forensic work. It is related to the preservation, analysis and result generation of the evidence. If the identification of evidence is not carried out correctly or the identified evidence has little to do with the case, the subsequent work of evidence collection and analysis will be futile. Therefore, guiding standards should be formulated for the identification of evidence to prevent the identification from deviating from the direction of forensics.

(2) Improve the examination and identification procedures for electronic evidence

Electronic evidence shall be reviewed at the same time in accordance with the requirements of each type of evidence. Where the original storage medium exists and is convenient for transfer, it shall be transferred to the people's court in order to verify the authenticity of audiovisual materials and electronic data when necessary. Authentication of audio-visual materials and electronic data must ensure the authenticity and reliability of the sources, collection, extraction, production, storage, and identification of audio-visual materials and electronic data through various kinds of evidence to prevent them from being difficult to distinguish or unreasonable due to authenticity. The doubts of the explanation were eliminated. Judicial practice pays more attention to three principles. One is the principle of non-destructiveness, that is, not to take any action that may change the original data, such as using a write-protection device on the original hard disk when extracting data; the second is to avoid using the original evidence, such as in the hard disk copy analyze the data to protect the original data. The third is to record the operations performed. During the

forensics process, the process of extraction, preservation and transmission of evidence should be completely recorded.

5. Conclusion

"Criminal Procedure Law" is based on China's basic national conditions, and electronic evidence is confirmed by legislation as a new type of criminal evidence. It is of great significance for investigating agencies to better use scientific and technological means to punish crimes and maintain social order. The collection of electronic evidence must be based on laws and regulations. Investigating agencies use scientific evidence collection methods to discover, fix, extract, and analyze electronic evidence materials, and promote electronic evidence to play a role in fighting for social fairness and justice. Based on the domestic procedural and methodological research on electronic data evidence and electronic forensics, many norms and standards are still in the trial stage, and they need to be tested and modified in judicial practice. In particular, the specifications for the inspection and appraisal of various electronic data evidences are still in the revision period, which needs to be further studied and resolved in future work.

References

[1] Fabiola La Gamba, Giovanni Corrao, Silvana Romio. Combining evidence from multiple electronic health care databases: performances of one‐stage and two‐stage meta‐analysis in matched case‐control studies[J]. Pharmacoepidemiology & Drug Safety, 2017, 26(10):1213-1219.

[2] Bouteiller X P, Barraquand, Frédéric, GarnierGéré, Pauline, et al. Electronic appendix 2 to: No evidence for genetic differentiation in juvenile traits between Belgian and French populations of the invasive tree Robinia pseudoacacia[J]. Plant Ecology & Evolution, 2018, 151(1):5-17.

[3] Mark Conner, Sarah Grogan, Ruth Simms-Ellis. Do Electronic Cigarettes Increase Cigarette Smoking in UK Adolescents? Evidence from a 12-month Prospective Study[J]. Tobacco Control, 2017, 27(4):365-372.

[4] Ine Beyens, Amy I. Nathanson. Electronic Media Use and Sleep Among Preschoolers: Evidence for Time-Shifted and Less Consolidated Sleep[J]. Health Communication, 2018, 34(5):1-8.

[5] Jung M J, Naughton J P, Tahoun A, et al. Do Firms Strategically Disseminate? Evidence from Corporate Use of Social Media[J]. The Accounting Review, 2018, 93(4):225-252.

[6] Lori A. Catalano, Eileen Werdman. Avoiding legal risks in critical care nursing[J]. Nursing Critical Care, 2017, 12(4):30-35.

[7] Vitalii M Pashkov, Andrii A Olefir, Oleksiy Y Bytyak. Legal features of the drug advertising[J]. Wiadomosci Lekarskie, 2017, 70(1):133-138.

[8] Marko Jukić, Puljak L. Legal and Ethical Aspects of Pain Management[J]. Acta Medica Academica, 2018, 47(1):18.

[9] Abidah Setyowati, Constance L. McDermott. Commodifying Legality? Who and What Counts as Legal in the Indonesian Wood Trade[J]. Society & Natural Resources, 2017, 30(6):15.

[10] Adi Hajj-Ahmad, Severine Baudry, Bertrand Chupeau. Flicker Forensics for Camcorder Piracy[J]. IEEE Transactions on Information Forensics & Security, 2017, 12(1):89-100.

[11] David G. Reading, Ian W. Croudace, Phillip Edward Warwick. Fusion bead procedure for nuclear forensics employing synthetic enstatite to dissolve uraniferous and other challenging materials prior to LA-ICP-MS[J]. Analytical Chemistry, 2017, 89(11):6006-6014.

[12] Adam M. Olsen, Bryony Richards, Ian Schwerdt. Quantifying Morphological Features of α-U 3 O 8 with Image Analysis for Nuclear Forensics[J]. Analytical Chemistry, 2017, 89(5):3177.