Review and Analysis of Electronic Data Forensics Rules in Network Remote Survey

Yixin Zhang
Zhongnan University of Economics and Law, Wuhan 430073, China.

Abstract: With the rapid development of open network environment in China, its influence is more and more far-reaching. When it comes to the forensics in the field of investigation measures, it is mainly embodied in electronic data and its network extraction. Network extraction includes network remote inspection of evidence collection mode, from the traditional hands-on, contact type gradually to remote, non-contact type. However, in China's current judicial theory, the legal nature and definition of network remote inspection are not clear, and even the rules themselves are unreasonable or contradictory. In practice, it is mainly reflected in a series of difficult situations in application, such as improper use due to unclear concept and nature, or mixed use with other investigation measures. These will eventually lead to the non-standard and illegal electronic forensics, the loss of protection of citizens' privacy rights, and the failure of the system of investigation links. To better implement fixed and extraction of link to the network evidence investigation and necessary based on the existing system for the existing rules are more comprehensive and systematic carding and analysis, clarify the legal nature of network remote inquest and legal position of, in order to improve the network remote electronic data evidence rules in the system of inspection.

Keywords: Electronic Data; Investigation Measures; Network Forensics; Network Remote Survey

Introduction

Electronic evidence, which appears more and more frequently in criminal cases and plays an increasingly important role in the investigation of cases, has different problems in obtaining evidence because of its nature and characteristics completely different from traditional physical evidence and documentary evidence. Compared with the former, the difficulty of obtaining evidence of traditional physical evidence mainly focuses on the identification of true and false and the identification of right and wrong, while the difficulty of obtaining evidence of electronic evidence is not only reflected in the difficulty of later identification due to its easy modification, but also reflected in how to accurately locate, screen and collect the vast Internet information flow, and how to ensure the integrity and objective authenticity of the extracted electronic data.[1] Therefore, based on the transition stage of the Internet information age, it is still necessary to continue to explore the improvement of electronic data forensics

technology and the establishment of forensics rules.

In 2005 issued by the inquest and electronic computer crime scene data check rules, is the first in the history of our country of electronic data evidence systematic provisions of normative documents, among them, the field of electronic data evidence collection, examination, appraisal procedure and the provisions of the content,[2] is the beginning of the research on electronic data forensics problem in our country. Currently, China's existing important normative documents related to electronic data forensics mainly include the following two parts: First, provisions on Several Issues concerning The Collection, Extraction, Examination and Judgment of Electronic Data in Handling Criminal Cases (hereinafter referred to as Provisions on Electronic Data) issued in September 2016;The second is the Rules on Electronic Data Forensics in Criminal Cases handled by Public Security Organs (hereinafter referred to as the Rules on Electronic Data Forensics) promulgated in January 2019.According to the above two existing laws and regulations, combined with other judicial interpretations related to electronic data investigation and evidence collection, this paper makes an overall sorting and evaluation of electronic data forensics rules system in network remote investigation and related application problems of electronic data forensics and network remote investigation.

As one of the legal investigation measures expressly stipulated in the Criminal Procedure Law of Our country, there is a specific and detailed concept definition in the legal provisions. From the logical relationship, the network remote investigation should be the next concept of the investigation, and the provisions of the law for the investigation should also be applied to the network remote investigation. At the same time, the Regulations on Electronic Data and the Rules on Electronic Data Forensics have made a series of specific regulations on the practical operation methods and procedures of network remote inspection.

1. Subject of inspection

Investigation and inspection refers to the investigation of places, articles, corpses and human bodies related to crimes, so as to discover and collect all kinds of traces and articles left by criminal activities. It is stipulated in the criminal proceedings that the investigation should be carried out in principle by the investigators, and when necessary, people with specialized knowledge can be appointed or hired to conduct the investigation under the auspices of the investigators. The Electronic Data Forensics Rules further require that the remote inspection should be undertaken by the county-level public security organs, while the superior public security organs can provide technical support. For the regulation of the subject of network remote inspection, the main consideration should be the professionalism of the subject of inspection, whether it can ensure that electronic data can be collected comprehensively, timely and objectively in the whole process of inspection under legal procedures, and whether it can provide technical guarantee. All of these will be an important reliance on whether the extracted electronic evidence has integrity and legitimacy, and further improve the identity qualification and ability qualification requirements of the subject of the investigation, which is the due meaning of the network remote investigation.

2. Objects of inspection

Since the promulgation of the Amendment to the Criminal Procedure Law in 2012, electronic evidence has been officially included in the statutory types of evidence, and has become a new generation of "king of evidence" in today's Internet information age.[3] Because of its own virtual sex, massive, recoverability, multimedia and other basic characteristics of electronic data clearly different from the traditional material evidence, documentary evidence, shall not be in direct contact, its storage and read also does not depend on physical space and medium, but mainly preserved in all kinds of electronic equipment, network system, or computer system.[4] Based on this, Article 9 of the Regulations on Electronic Data clearly stipulates that the object of network remote inspection should be the remote computer information system, and Article 27 of the Regulations on Electronic Data Forensics also specifies that network remote inspection should be carried out on the remote computer information system if necessary in the process of online network extraction. It can be seen that the applicable object of network remote survey is almost no dispute to be identified as the remote computer information system in the current laws and regulations.

However, with the rapid development of the Internet and the variety of mobile electronic devices, the tool medium for people to connect and use the Internet has long been not limited to computer systems, and the scope of electronic data storage and display has been greatly expanded.Therefore, in order to meet the objective authenticity, comprehensive integrity of electronic data forensics, the applicable object of network remote inspection should be expanded to all intelligent terminal operating systems that can access the network and carry out electronic data transmission, interaction and storage, such as mobile phones and tablets.

3. Applicable conditions

Article 9 of the Regulations on Electronic Data stipulates not only the applicable objects but also the applicable conditions, that is, the premise of network remote survey must be "necessity". In other words, the application time of remote inspection in electronic data forensics program is limited, so it should be postponement. Some scholars believe that this means that remote survey can only be carried out when the purpose of extracting and collecting electronic data cannot be achieved by other conventional means.[5] Other scholars believe that this is to emphasize the need to combine application with specific situations and investigation and evidence collection.[6] This is mainly based on two considerations. One is to ensure citizens' right to privacy and information to the greatest extent by setting strict preconditions. In this way, citizens are not aware of the situation, in the process of secret investigation was unreasonable or even illegal access to private data, and even can not know, can not claim relief. Second, to better ensure the reliability and comprehensiveness of data. Electronic data evidence mainly includes two modes, respectively is "one collection" and "single extraction".[7] Some scholars think, compared with the electronic data from a storage medium on separate download extraction model of the medium itself and collect data integration mode, the data source and technical level are a better preserve data integrity and authenticity of effect, that is, if the original storage media can be directly contacted and extracted, the form of network inspection should not be given priority.[8] However, some scholars do not agree with the principle of "simultaneous extraction" consistent with the Regulations on Electronic Data and the Rules on

Electronic Data Forensics, that is, the mode of integrated collection is not only difficult in practice, but also violates the principle of proportion, and is suspected of infringing citizens' privacy and property rights. It also tries to point out that the storage of electronic data will be "distributed" from the perspective of the development of network technology.[9] In other words, even if the integrated collection mode advocated by the former view is adopted, it is difficult to continuously ensure the integrity and authenticity of evidence extracted in the development trend of The Times.

At the same time, Article 9 also stipulates that in the network remote survey, if further use of technical investigation means is needed, the examination and approval procedures shall be stricter accordingly. All of these provisions aim to protect as much as possible the rights of citizens, such as privacy and individual property rights .But the fact is, only setting these preconditions, the protection of civil rights is far from enough. Article 27 of the Rules of Electronic Data Forensics further specifies six kinds of situations that can be applied to network remote investigation. However, it is obvious that the "installation of new application programs on the remote computer system" has involved the scope of technical investigation, but more clearly reflects the suspicion of violating citizens' privacy right.

When it comes to cross-border forensics, there is also a need to consider a variety of possible violations of rights and international conventions. The Rules for Electronic Data Forensics have to some extent responded to the international criticism raised by articles 3 and 9 of the Electronic Data Regulations, [10] and have been improved accordingly. First of all, in the "electronic data sets" for public and private, domestic and overseas electronic data for boundary points, the former leads to the network remote inquest to those who have nothing to do with the case facts, citizens as well as reasonable expectation of electronic data and extract indifferently, this is without a doubt over the criminal proceedings disguised in investigation of similar measures to set up the right restrictions. The latter is likely to cause unnecessary international disputes and diplomatic risks when remote inspections are conducted to extract electronic data from overseas.[11] Second, article 3 also grants the same investigative power to the people's courts, which may violate the provision of Article 40 of the Constitution that "only the right to inspect citizens' correspondence is granted to public security organs and procuratorial organs", thus infringing citizens' freedom of communication and right to confidentiality in communication. The practice of Electronic Data Forensics rules is to further limit the object of remote inspection to domestic computer information system and electronic data publicly released abroad. Although this action eliminates the possibility of violation of part of international law, it still fails to effectively deal with the fundamental contradiction of how to protect the legitimate privacy rights of citizens in China. It also fails to eliminate the dilemma that the right of investigation, as a national sovereignty, cannot be carried out legally in other countries, so that the investigation work cannot be carried out normally.

4. Applicable procedures

In terms of application procedure, in order to prevent the abuse of inspection power, the Criminal Procedure Law clearly stipulates that the investigation personnel must hold the legal certificates approved by the relevant investigation authorities.[12] However, this regulation has little practical significance in the practice of network remote inspection, because there are no special restrictions on the place and time, and it

is often a secret investigation without the knowledge of the parties concerned. In addition, various elements and information that should appear in the follow-up inspection record are specified in detail, which is mainly for the consideration of evidence preservation.[13]

Compared with the Provisions on Electronic Data, in addition to a series of procedural rules for online extraction should also be applicable to remote inspection, the provisions that "higher public security organs should command and provide technical support when applying remote inspection to lower public security organs" are added in Articles 28 and 29 of the Rules on Electronic Data Forensics. Article 30 also introduces the system of "witness", audio and video recording. All the above are brand-new program supervision mechanisms established for the application of network remote inspection. "Making record of Network remote Inspection afterwards" is a direct transplant of the stipulation that "investigation must make record of investigation" in criminal proceedings. In cases where technical investigation is required, further stringent approval procedures are required. But in criminal proceedings in our country, technical investigation and an inquest is a parallel relationship of two kinds of legal investigation measures, both in terms of the specific legal regulation has a bigger difference, but the rules of here is the technical investigation into the remote means of inspection methods, may appear in practice both conceptual confusion, and so cannot be strictly in accordance with the applicable situation.

It should be pointed out that although the electronic Data Forensics Rules have made some progress and breakthrough in setting up the overall supervision mechanism of remote inspection procedures, there are still big defects. The supervision procedure should include pre-examination, in-process supervision and post-examination. The imperfect supervision mechanism will lead to excessive free operation space for the subject of investigation in practice, which is obviously not conducive to the protection of the privacy of the subject of investigation, the conservation of investigation and judicial resources, and the restoration of the investigation of criminal facts.

References

[1] Zhu TH, Wang YQ, "Regulation of Due Process of Electronic Data Forensics - A Review of "Public Security Electronic Data Forensics Rules", published in Soochow University Journal (Law Edition), No. 7, 2020.

[2] He JB, "Research on the Standards and Norms of Electronic Data Forensics at Home and Abroad", in "Secret Science and Technology", No. 3, 2016.

[3] Liu PX, "Basic Theory of Electronic Evidence", in Journal of the National Procuratorate, No. 1, 2017.

[4] Xie DK, "Reflection and Reconstruction of the Rules for Remote Inspection of Electronic Data Networks", Chinese Criminal Law, No. 1, 2020.

[5] Liu M, "Analysis of the Standardized Text of Public Security Electronic Data Forensics", in "Journal of People's Public Security University of China (Social Science Edition)", Vol. 1. 2021 Issue 37 Issue 4.

[6] Xie DK, "Authenticity of Electronic Data", in "Journal of the National Procuratorate", No. 5, 2017.

[7] Xie DK, "Reflection and Reconstruction of Remote Inspection Rules for Electronic Data

Networks", Criminal Law, No. 1, 2020.

[8] Zhu TH, Wang YQ, "Regulating Due Process of Electronic Data Forensics - A Review of "Public Security Electronic Data Forensics Rules", Journal of Soochow University (Law Edition), No. 7, 2020.

[9] Liang K, "Reshaping the Cross-border Remote Electronic Forensics System", Global Law Review, No. 2, 2019.

[10] Li SW, Interpretation of the Criminal Procedure Law of the People's Republic of China, China Legal Publishing House, 2018 edition, p. 10. 321.

[11] Liu HY, Editor-in-Chief: Electronic Data Forensics, Tsinghua University Press, 2016, p. 325.

[13] Zhang Y, Zhang B, "Concept Definition and Characteristic Analysis of Electronic Data Evidence", in "Journal of Hubei Police Officers College", Vol.1. September 28, 2015.