Science of Law Journal (2024)
Clausius Scientific Press, Canada

DOI: 10.23977/law.2024.030425
ISSN 2616-2296 Vol. 3 Num. 4

Research on the problem of electronic data forensics of the crime of assisting in the commission of fraudulent activities through electronic means

Wenqing Chen[1], Zihan Wang[2,*]

[1]School of Humanities, Donghua University, Shanghai, China
[2]School of Law, East China University of Political Science and Law, Shanghai, China
[*]Corresponding author: 1502414027@qq.com

Keywords: Crime of Assisting in the Commission of Fraudulent Activities through Electronic Means; Electronic Data; Technical Investigation; Forensic Measures

Abstract: With the rapid development of the Internet, cybercrime activities have become increasingly rampant, in which the crime of assisting in the commission of fraudulent activities through electronic means has become a hot issue in judicial practice. At present, the electronic data forensic procedures for the crime have the phenomena of the nature of forensic measures being unclear, the quantification of the electronic data involved in the case, and the presentation of electronic data in paper form, which leads to problems such as the authenticity and legitimacy of the electronic data being difficult to question, and difficulties in forensics. Based on this, on the basis of the existing evidentiary rules, the nature of electronic data forensic measures and the key to distinguishing types of evidence should be clarified, the protection of personal information should be strengthened, and the methods of proof should be enriched, so as to solve the practical problems.

1. Introduction

With the development of information network technology, information sharing has become more frequent, convenient and widespread. However, the convenient and hidden nature of such networks has been exploited by law-breakers, making citizens' personal information extremely accessible, and crimes can be committed through remote manipulation, greatly reducing the cost of crime. This has led to the transfer of traditional forms of crime such as fraud and theft to cyberspace, and the frequent occurrence of cybercrime in recent years.

The crime of assisting in the commission of fraudulent activities through electronic means (hereinafter referred to as ‘Attempt and aiding or abetting’) is a new offence under the Amendment (IX) to the Criminal Law, which mainly refers to the perpetrator who knows that another person uses the information network to commit a crime and provides technical support for the crime such as Internet access, server hosting, network storage, communication transmission, etc., or provides advertisements and promotions, Payment and settlement and other illegal assistance. This offence significantly reflects the characteristics of crowdedness, with the type of evidence mainly focusing on electronic data and the volume of data being huge. It is worth noting that the number of

prosecutions for the offence of ‘Attempt and aiding or abetting’ throughout the year of 2021 has jumped to the third place of all criminal cases, becoming the primary offence in the criminal chain of telecommunication network fraud, and covering almost all aspects of telecommunication network fraud such as the acquisition of information, technical support, provision of venues, promotion and attraction, and payment and settlement.

Compared with traditional evidence, the core evidence of the crime - electronic data, with virtual, science and technology, vulnerability, massive, dependence and other significant features. Due to these characteristics of electronic data, its forensic process needs to rely on specialised extraction technology, forming a different forensic model from traditional physical evidence. At the same time, the complexity of electronic data also raises the issue of balance between the protection of personal information and the fight against crime. Therefore, procedural constraints on the forensic process of electronic evidence are particularly important. However, at present, no independent approval procedures have been designed for the examination and extraction of electronic data, which requires evidence legislation and judicial practice to be adjusted and improved accordingly in the light of the characteristics of electronic data.[2]

2. Sorting out the rules of electronic data forensics

In the Criminal Procedure Law amended in 2012, electronic data was formally listed as a new type of evidence. Subsequently, in order to regulate the forensic process of electronic data, the Supreme People's Court, the Supreme People's Procuratorate, and the Ministry of Public Security (MPS) jointly issued the Provisions on Several Issues Concerning the Collection and Extraction of and Examination and Judgement on Electronic Data for Handling Criminal Cases (hereinafter referred to as the ‘Electronic Data Provisions’) in 2016, whereas the MPS issued the Rules of Public Security Organs Handling Electronic Data Forensics Rules for Criminal Cases (hereinafter referred to as the Electronic Data Forensics Rules).

With regard to forensic measures, Article 9 of the Electronic Data Rules lists in detail the ways of electronic data forensics, ranging from broad online extraction, to remote investigation, to network technology investigation, forming a hierarchical system. However, in Article 9 of the Public Security Electronic Data Rules, although there are references to the procedures of search, seizure and attachment in the Criminal Procedure Law, among the electronic data forensic measures designed therein, apart from the network technology investigation which has a strict approval procedure, the other measures do not achieve a comprehensive and effective convergence with the provisions of the Criminal Procedure Law. It is worth noting that Article 27 of the Public Security Electronic Data Rules reaffirms the concept of online extraction of electronic data as a superordinate concept for remote investigation, but the second paragraph of Article 33 seems to regard network technology investigation as a common technical support for both. The rights guarantee part is reflected in Articles 4, 52 and 58, which all emphasise the confidentiality obligations of judicial organs, require the timely destruction of irrelevant data, and explicitly prohibit the disclosure of citizens' information, so as to ensure that the right to know of the right holders of the original carriers of electronic data is safeguarded.

In terms of the exclusion of electronic data, Article 27 of the Electronic Data Provisions follows the same line of thought as the review of traditional physical evidence, explicitly stating that electronic data with procedural flaws that cannot be remedied shall not be used as the basis for a case. Article 28 further provides for exclusionary circumstances affecting the authenticity of electronic data. In addition, the Provisions on Procedures for Handling Criminal Cases by Public Security Organs promulgated by the Ministry of Public Security in 2020 also clarified the issue of reviewing the legality of electronic data on a macro level from the perspective of exclusion of

illegal evidence. As there are differences in the procedural settings of different electronic data forensic measures, the choice of forensic measures at the investigation stage will directly affect the determination of the legality and authenticity of electronic data.

3. Judicial status of electronic data forensics in 'Attempt and aiding or abetting'

With the rapid progress of Internet technology, cases of the crime have presented significant new features. First of all, the volume of data involved in the case has expanded dramatically, the participants in the case are spread across multiple geographic regions, and the criminal ability of individuals has increased significantly, covering all aspects of the criminal chain from information collection, publicity and diversion, technical support to venue provision, payment and settlement. Not only has the amount of data that can be manipulated by individuals surged, but criminal activities facilitated online have also reached an unprecedented scale. In addition, the types of electronic data are changing rapidly with technological innovation, and a large amount of new types of evidence are emerging, yet these emerging areas have not yet been perfected at the legislative level, and the courts are overwhelmed in dealing with them. Under the big data environment, the storage, transmission, modification and deletion of electronic data have become exceptionally convenient, which puts higher requirements on judicial organs and case handlers, who are not only required to be proficient in the relevant technology, but also need to be equipped with a large amount of professional equipment to meet the challenges.

In a nutshell, the high incidence and special nature of 'Attempt and aiding or abetting', combined with the objective difficulties faced by electronic forensics, as well as the lagging nature of laws and regulations and the limitations of judicial technological capacity[3], together constitute the current situation of the difficulty of forensics work in the crime.

3.1. Vague nature of evidentiary measures and violation of citizens' fundamental rights

When discussing 'Attempt and aiding or abetting', we have to face the problem of the ambiguous nature of the evidence collection measures. Take the seizure measures as an example, although the 'electronic data provisions' clearly 'to seize the original storage media as the principle, to the scene of separate extraction as an exception, to print, photograph, video and other ways of fixing as a supplement' of the principle of evidence collection, but the data show that, in practice, the direct extraction, inspection and investigation of electronic data without prior seizure of the situation is quite common. This shows that the case officers tend to seize, inspection and other measures as a whole method of application, rather than subdividing its nature. Currently, China's e-discovery measures and their implementation procedures for the crime show a more lenient trend, such as online network extraction and remote inspection, which, despite possessing the characteristics of traditional mandatory investigative measures, lack the statutory conditions of necessity and have relatively lax approval procedures.

With the evolution of the times, the scope of citizens' rights and interests such as the right to personal information and the right to privacy are expanding. Especially in the meta-universe and other emerging technologies, the boundaries between the virtual and real worlds have become blurred, and some scholars have even proposed that citizens have the right of independent virtual network personality, which covers the maintenance and realisation of personality independence, equality, dignity and freedom. The various types of information in the virtual space of the internet, as an important component of personal information rights and privacy rights, must be processed with the explicit written consent of the individual or fulfill the obligation of disclosure under legal circumstances.

The e-discovery measures for the crime are a violation of citizens' rights to personal information

and privacy in two main ways: First, the technical level of infringement. In practice, the investigation and evidence collection technicians sometimes directly use illegal procedures to capture the evidence involved in the case, experts pointed out that the network environment, the use of legal means of evidence collection similar to hacking technology has become easier. Second, infringement on the means level. With the help of network technology, round-the-clock and endless network monitoring has become possible, and the extraction of sensitive personal information such as social software chat logs and IP addresses also involves such issues.[5]

3.2. The quantification of the electronic data involved in cases and the burden of justice resulting from the taking of evidence on a case-by-case basis.

In the case of 'Attempt and aiding or abetting', electronic data are proliferating at an unprecedented rate, creating a trend towards quantification. This astronomical volume of data poses a great challenge to judicial workers, making it difficult for them to complete their forensic, examination and analysis work in a short period of time, making it impossible for them to accurately judge the nature, content and quantity of the data involved in the case, and thus affecting the accuracy of the conviction and sentence.

In judicial practice, although most judicial workers still adhere to the traditional principle of 'taking evidence one by one, should be taken as much as possible', but in the face of the massive amount of electronic data, the implementation of this principle appears to be incompetent. This problem is further exacerbated by the differences in technical capabilities between the public security authorities and the procuratorial authorities. Although the public security organs have accumulated a wealth of experience and means of investigation and evidence collection, the procuratorial organs still face enormous difficulties in examining massive amounts of evidence, which undoubtedly leads to an excessive consumption of judicial resources.

Cybercrime cases in China often use the element of amount as the core criterion, and the rigid implementation of the principle of comprehensive evidence collection will bring about a series of problems. First, it will lead to difficulties in identifying the number of victims and in obtaining evidence; second, it will be difficult to accurately count the number of offences, and the nature of the content involved will be difficult to identify; and third, the burden of justice will become unusually heavy. With the increased investment in cybercrime governance, cybercrime cases have become an increasingly important part of judicial work. This means that we need to devote more manpower, material resources and time to these cases. However, if we devote exponentially more energy and financial resources to evidence-gathering, the processing time for other types of cases will inevitably be compressed, and at the same time the litigation period will be lengthened, thus reducing the overall efficiency of judicial work.

3.3. Electronic data presented in the form of paper, difficult to ensure the authenticity of the evidence

In the field of e-discovery, data are presented in a variety of forms, covering five common forms of presentation, such as CD-ROMs, USB flash drives, photographs, screenshots, and verified written opinions. However, the specific definition of a screenshot, i.e., whether it is an electronic screenshot that is directly verified online or whether it is printed through a paper version of a screenshot, has not yet been clearly defined. However, in the judicial practice of the case of the crime of assisting in the commission of fraudulent activities through electronic means, most of the data after e-discovery is converted into a written document for display at the time of transfer and presentation. Based on the procuratorate's current method of presenting electronic evidence, which is not comprehensive, both the prosecution and defense prefer to convert it into paper documents for written transmission and

presentation.

The choice of paper documents as the presentation form of electronic data does, to a certain extent, solve the problem of the original carrier being large and not portable, simplifying the process of presenting electronic data and thus improving the efficiency of cross-examination. However, from the point of view of the best evidence rules, the probative power of the original electronic data compared to the paper-based electronic data is more powerful. In addition, the collecting process of some electronic data lacks sufficient evidence to prove its legitimacy and authenticity, which further highlights the importance of original electronic data.

If the paper-based electronic data lacks corresponding records of the extraction process, then the integrity of the electronic data provided by the prosecution will not be effectively verified, and it will be difficult for the defense to raise objections to the electronic data. In addition, scholars have also pointed out that part of the encrypted electronic data can not be screenshot or printed and other operations for paper display, over-reliance on paper documents in the form of display may lead to the lack of this part of the electronic evidence in the court process of cross-examination, can not constitute a complete chain of evidence, thus affecting the quality and fairness of the case trial.[4]

3.4. Inefficient mechanisms for cross-border evidence collection and dubious legality

At the fifth meeting of the United Nations Intergovernmental Expert Group on Cybercrime in 2019, participating experts reached a basic consensus that the issue of cross-border e-discovery will be key to China's future governance of new types of cybercrime.

With regard to the collection of electronic evidence in cross-border cybercrime cases, China's current laws have set up two main paths: one is through requests for criminal judicial assistance, and the other is to conduct online network extraction, remote network survey and technical investigation on the basis of remote e-discovery regulations. However, from the observation of China's criminal investigation practice, these two paths are faced with the challenges of a single way of evidence collection, a long period of time and great difficulty, and cannot effectively meet the actual needs of the current investigation work. In addition, the inefficiency of judicial assistance requests conflicts with the timeliness of e-discovery requirements, which may lead to an increased risk of tampering with or deletion of original evidence, at the same time the lengthy and inefficient request program also provides criminal suspects with the opportunity to remove unfavorable evidence, making unilateral cross-border evidentiary modes such as "public security hacking" an unavoidable choice.

Such cross-border unilateral evidence collection not only threatens the security of national sovereignty, but may also undermine the legitimacy of evidence. In order to safeguard the sovereignty of cyberspace, countries have taken legal measures to localize data storage and strictly limit outflow. For example, in 2012, the European Union introduced the EU General Data Protection Regulation, which set an industry standard for global online data protection, and then countries have introduced laws to move closer to it.

In the Beijing Declaration, the position of "opposing unilateral sanctions" and "long-arm jurisdiction" and "respecting the judicial sovereignty of all parties" was clearly stated. Due to the intersection of the dual criminality principle, the principle of state sovereignty, and the rights of the individual, cross-border crime crackdowns often face many policy obstacles, resulting in slow progress. The National Cyberspace Security Strategy released in 2016 also emphasizes that cyberspace sovereignty is an important component of national sovereignty, and that unilateral cross-border evidentiary acts such as "public security hacking" without the authorization and informing of other countries may constitute an infringement of the sovereignty of other countries. The legitimacy and probative value of electronic data obtained through such acts will be questioned, and the question of whether they can be used as evidence in criminal proceedings, and in particular their

crucial role in the overall case, remains a topic of endless debate in the academia.

4. Recommendations for Improving Electronic Data Forensics

4.1. Legislation should clarify online network extraction as an investigative technique

In the Electronic Data Forensics Rules, network online extraction of electronic data applies to both publicly available electronic data and electronic data on remote computer information systems in the territory. It is noteworthy that network survey, as a subordinate concept of network online extraction, is regarded as a technical means. However, the execution of the survey as a legally prescribed investigative measure is not accompanied by a strict approval process. In Article 37 of the Electronic Data Forensics Rules, the freezing of electronic data is clearly defined as a mandatory investigative measure and the necessity of prior approval is emphasized, aiming to protect the procedural rights and interests of the investigated person while guarding against the abuse of investigative power. However, no corresponding approval mechanism has yet been established for the online extraction of electronic data, and if it is independently regarded as an investigative measure, it undoubtedly increases the risk of abuse of power. In addition, the current Electronic Data Forensics Rules have not made clear definitions and provisions on whether electronic data forensic measures are included in the scope of technical investigation, and the approval subjects and procedures for most major forensic measures. Therefore, clarifying online network extraction as an investigative technique is an issue that needs to be urgently addressed in the legislation.

4.2. Judicial clarity on paper-based electronic data is needed

In the current judicial practice, paper-based presentation of electronic data is still dominant, however, in order to comply with the trend of digitalization, it is particularly important to improve the rules for the use of paper-based electronic data to ensure a smooth transition.

First, the standardization of the evidence collection process must be strengthened. For example, in the process of electronic data extraction, the judicial authorities should ensure that they have complete seizure lists, detailed electronic data survey and inspection records, and precise electronic data extraction lists. These documents should contain detailed records of the personnel, time, place and object of electronic forensics, as well as the identity of the producer and the equipment used in the production process. In addition, in order to ensure the originality and authenticity of the evidence taken, multiple authentication means such as fingerprint authentication and algorithmic verification should be comprehensively used.

Secondly, the basic model of e-discovery should be further optimized. A complete electronic data not only contains the carrier itself, but should also cover evidence of identity, evidence of conduct and ancillary information related to it. Therefore, in the evidence collection process, special attention should be paid to avoiding the omission of any important ancillary information, in order to ensure the integrity and reliability of electronic data.

4.3. Procedures need to be further focused on the protection of personal information

During improving the e-discovery procedures in cases of the crime of assisting in the commission of fraudulent activities through electronic means, the Personal Information Protection Act should be more closely aligned, and differentiated treatment should be implemented for the data involved in the case, in order to effectively safeguard citizens' rights to personal information and privacy. In particular, in the process of reviewing and extracting data involving semi-public and unpublicized data, it is necessary to operate strictly in accordance with the law and with prudence. Pursuant to

article 28 of the Personal Information Protection Law, basic notification obligations must be fulfilled with respect to sensitive information such as biometrics, religious beliefs, specific identities, medical and health care, financial accounts, whereabouts and trajectories, even when legally necessary for the processing of criminal cases.

However, in view of the complexity and specificity unique to cybercrime cases such as the crime of assisting in the commission of fraudulent activities through electronic means, the fulfillment of the notification obligation on a case-by-case basis may face a dilemma similar to that of obtaining evidence on a case-by-case basis, thus affecting the efficiency of the handling of the case. Therefore, we need to further refer to the relevant provisions of Articles 18, 30 and 35 of the Personal Information Protection Law, combining the fulfillment of the obligation to inform with the construction and improvement of the mechanism of typed sampling and evidence collection, in order to achieve flexibility and efficiency in the handling of cases, and to ensure that the judicial process can be carried out smoothly while citizens' personal information is protected.[6]

4.4. Strategically enriching forensic methods for massive evidence

Some scholars have suggested adopting a "snowball"[1] sampling strategy, which begins with an established sample group and relies on its referral or searching practices to gradually expand the sample size. However, this method lacks of rigor and is more suitable as a tool for preliminary exploration. Therefore, it should be utilized with caution in judicial practice. To make up for the non-randomness defect of this sampling method, scholars went on to propose the chain-tracing sampling method, i.e., screening data from the existing data chain and tracing other sample data through the network of relationships.

In 2016, the Opinions on Several Issues Concerning the Application of Law in Handling Criminal Cases of Telecommunications Network Fraud and Other Criminal Cases, jointly issued by the Supreme People's Court, the Supreme People's Procuratorate, and the Ministry of Public Security, stipulated that sampling evidence could be used in handling cases of telecommunication network fraud, but did not address the specifics. Until 2022, Article 22 of the Opinions on Several Issues Concerning the Application of Criminal Procedure in Handling Information Network Cases clearly regulated the sampling method, which was an adjustment made by the legislator based on the dilemma of judicial practice, and it has a certain value of application for cases involving many victims, and the innovative practice of classifying and retrieving massive electronic data according to the amount of value makes it in the handling of cybercrime cases. The innovative practice of categorizing and searching massive electronic data according to its value makes it particularly useful in handling cybercrime cases in an efficient and streamlined manner.

Some scholars also advocate replacing sampling with the bottom-line proof method, i.e., setting benchmarks such as the number of crimes and the amount of money, and, after the benchmarks have been met, estimating the excess in order to assess its seriousness. The bottom-line proof method now has a legal basis, such as the Opinions on Several Issues Concerning the Application of Law in Handling Criminal Cases Involving Telecommunications Network Fraud and Other Cases issued in 2021, which set the standard for the number of criminal objects for the crime of assisting in the commission of fraudulent activities through electronic means to alleviate the forensic pressure on the judiciary caused by the huge amount of data. The method requires the collection of only electronic data sufficient to support the criteria for conviction and aggravation of punishment, which neither lowers the standard of proof for criminal offenses nor requires the acquisition of all electronic data, and the extraction and review of remaining evidence can be terminated once the statutory criteria have been met, thus realizing a balance between efficiency and fairness.

5. Conclusion

This paper discusses the challenges and problems of electronic data forensics in judicial practice for the crime of assisting in the commission of fraudulent activities through electronic means, pointing out the current difficulties of the nature of forensic measures being unknown, the quantization of electronic data, the presentation of forms of paper, and the resulting dilemma of the authenticity and legitimacy of electronic data being hard to prove. In response to these problems, this paper puts forward a clear nature of electronic data forensic measures, strengthen the protection of personal information, enrich the method of evidence and other recommendations. Looking to the future, with the continuous development of network technology, cases of assisting in the commission of fraudulent activities through electronic means will present a more complex and changeable situation, the requirements of electronic data forensics will also be more stringent. Therefore, further improving the rules and systems for the forensics of electronic data and enhancing the scientific and effective forensics technology are important measures for safeguarding judicial justice and maintaining the security of cyberspace.

References

[1] Geng Leilei.(2010). A discussion on 'Snowball' sampling method. China Statistics(08),57-58.
[2] PAN Yuede.(2024). Research on the Legal Governance of the Crime of Helping Information Network Criminal Activities. The Primary People's Court of Tiexi District of Anshan City(03),43-50.
[3] WU Xiao-min; JIA Shuo.(2022). Collection of Electronic Evidence in Cross-Border Cybercrime Investigation. Journal of Guangxi Police College(02),46-52.doi:10.19736/j.cnki.gxjcxyxb.2022.0205.
[4] Chen Hongbing. (2022). 'Pocketization' Corrections of Crimes of Helping Cybercrime. School of Law, Southeast University (02),127-135. doi:10.16339/j.cnki.hdxbskb.2022.02.017.
[5] Yang Xuan. (2022). On the Improvement to the Remote Evidence Collection System of Criminal Electronic Data. A Dissertation Submitted for the Degree of Master.https://link.cnki.net/doi/10.26917/d.cnki.ganhu. 2022.000211doi:10. 26917/d.cnki.ganhu.2022.000211.
[6] Sun Mingze. (2020). Research on the procedure regulation of electronic data collection by investigation organ. Southwest University of Political Science and Law.https://link.cnki.net/doi/10.27422/d.cnki.gxzfu. 2020.000566doi: 10.27422/d.cnki.gxzfu.2020.000566.