Science of Law Journal (2026)
Clausius Scientific Press, Canada

DOI: 10.23977/law.2026.050206
ISSN 2616-2296 Vol. 5 Num. 2

Analysis of the dilemma of electronic data forensics for the crime of illegal use of information networks

Xiyue Zhang

College of Humanities and Social Development, Nanjing Agricultural University, Nanjing, 210095, Jiangsu, China

Keywords: Illegal use of information network; Electronic data; Execution connection; Rules of evidence; Closed loop of the program

Abstract: As cybercrime governance enters the digital age, electronic data has become a key carrier for the connection between criminals and criminal crimes of illegal use of information and network, and the problems in the connection between relevant laws and evidence collection have become increasingly prominent. This paper examines the dilemma of the connection between execution and evidence collection of electronic data for the crime of illegal use of information networks. At the pre-trial level, the characteristics of this crime bury the problem of ambiguity in the authority to collect evidence and the mismatch of evidence form. At the in-process level, standard conflicts and procedural absences lead to the loss of electronic data in the positive connection. At the post-event level, the lack of supervision has put the data involved in the case into a situation where no one has disposed of it. To solve the dilemma, it is necessary to reconnect the mechanism from four aspects: technical regulation, evidence rules, departmental responsibilities, and accountability. This study provides practical guidance for the work of electronic data evidence collection for the crime of illegal use of information networks, and standardizes the evidence collection process, Improving the quality and efficiency of case handling can enrich the theory of the connection between cybercrime evidence and execution, and make up for the shortcomings of the current research on the connection between crime and execution.

1. Introduction

With the rapid development of information network technology, the number of cybercrime cases is constantly increasing. The crime of illegal use of information networks is a key charge for regulating preparatory acts online, and electronic data serves as the primary basis for identifying this charge and is also the core to prove the validity of this evidence. The crime of illegal use of information networks is characterized by its network nature and information dispersion, and electronic data is prone to tampering and loss. These factors have long posed obstacles to the coordination of electronic data forensics between administrative law enforcement and criminal justice.

In practice, electronic data collected by administrative agencies is often excluded from criminal proceedings due to procedural issues. When public security organs re-collect evidence, they often miss the best opportunity to do so. After the criminal procedure is concluded, the absence of a mechanism for handling electronic data related to the case makes it difficult to advance administrative

accountability work. These issues have seriously affected the effectiveness of governance over cybercrime, and the poor connection between administrative law enforcement and criminal justice has become an urgent institutional issue that needs to be addressed. The existing relevant regulations have not been specifically designed in accordance with the characteristics of this crime and the attributes of electronic data, and thus cannot effectively address the difficulties encountered in practical work.

Existing research often analyzes the coordination of execution from a macro-institutional perspective but fails to fully explore it in a targeted manner by combining the specific nature of the crime of illegal use of information networks and the unique attributes of electronic data. Currently, amidst the digital era, the digital transformation of the interface between administrative agencies and criminal justice has become an unstoppable trend of the times [1]. Therefore, this article focuses on the crime of illegal use of information networks, adopting a full-process framework encompassing pre-event, during-event, and post-event stages to analyze the issues and their causes at different stages. Drawing on comparative law experience and China's judicial practice, we propose systematic solutions from four aspects, including technical regulation and evidence rules. This article aims to identify the broken links in the evidence circulation process, provide systematic institutional improvement plans, and provide support for enhancing the governance level of cybercrime.

2. The qualitative characteristics of the crime of illegal use of information networks and the basis of electronic data forensics

2.1 Characteristics of illegal use of information networks and their impact on forensic subjects

The core qualitative characteristic of this crime is its network nature. The investigation of cybercrime and the admissibility of electronic evidence are of utmost importance. Over-reliance on technology poses multiple challenges for law enforcement agencies, including technological advancement, privacy concerns, and legislative issues [2]. Cybercrime primarily relies on electronic data as evidence, and the scattered nature of information poses a barrier to obtaining evidence. The root cause of the poor coordination in criminal justice execution lies in the fact that the barriers related to execution data have not been eliminated with the advancement of informatization [3].If the perpetrator sets up the server overseas, the administrative authority's authority is limited, and cross-border cooperation with public security is complex, it is extremely easy to miss the opportunity to obtain evidence, leading to data loss.

This crime is characterized by the dispersal of information. The website registration, server, and payment data belong to different entities, resulting in a "legitimacy paradox" for the evidence collection entity. Investigators have the authority but lack technical expertise, while technical personnel possess technical skills but lack authority, resulting in flaws in the legality of evidence collection. At the same time, there is a problem of "self-defined convergence", where law enforcement departments possess both administrative and investigative functions, leading to confusion in the evidence collection process [4, 5].

There is uncertainty in determining the illegality of this crime. Article 287-1 of the Criminal Law stipulates "using information networks to commit illegal crimes" as a constitutive requirement, which is difficult to determine in the early stages of law enforcement and affects the collection of evidence [6]. Administrative law enforcement focuses on efficiency, while criminal justice emphasizes fairness. The inconsistent standards for evidence have led to practical dilemmas: obtaining evidence according to criminal standards is prone to exceeding authority, while adhering to administrative standards is likely to result in data loss before a case is filed.

2.2 Characteristics and requirements of electronic data forensics and corresponding dilemmas

Electronic data is easy to tamper with, easy to lose and technology dependent.

Tampering leads to the principle of originality of sealing the original carrier and fixing the hash value, but the perpetrator may set the server overseas, the administrative organ has no right to access the original overseas media, and the cross-border evidence collection procedures of the public security organs are complicated, making this principle difficult to implement. Administrative evidence collection often fails to meet the requirements of the originality of criminal procedures, and when the case is transferred to the public security, most of the key data has been lost. Pei Wei believes that the first contact and subsequent processing of electronic data should be distinguished, and the behavioral guidelines for first-time contacts should be formulated to reduce the risk of evidence preservation [7].

The data retention period of network service providers is usually six months, and the perpetrator can quickly delete the data in a short period of time. The execution connection procedure includes multiple links, and the cycle is long, often exceeding the data survival window, which eventually leads to the loss of key data.

Technology dependence is another important feature of electronic data, which requires the subject of evidence collection to have corresponding technical capabilities. The technical capabilities of administrative agencies are generally weak, and they lack verification capabilities in the face of encrypted data and other situations, and lack unified normative guidelines. If technical personnel are entrusted to collect evidence, they will also face the paradox of separating evidence collection authority and technical qualifications, which will eventually lead to flaws in the authenticity of the evidence taken, which is difficult to use as a basis for concluding in criminal proceedings.

2.3 The nature of this crime corresponds to the form of electronic data

This section focuses on the three types of behaviors of this crime: establishment, release, and purpose, and clarifies their correspondence with electronic data and evidence collection requirements. Due to the insufficient adaptation of the current norms, it is easy to lose evidence and affect the connection of executions.

In the establishment-type behavior, the illegal purpose of the perpetrator's establishment of a website or group is hidden and cannot be directly identified, and it needs to be supported by metadata such as IP addresses, login logs, and registration information. However, the current regulations do not have uniform provisions on the extraction, operation, preservation and transfer of metadata, and the standards for collecting evidence are different, which are prone to deviation, damage or omission, resulting in evidence that cannot be used as a basis for conviction and sentencing.

Publishing behaviors are based on information content as the main classification standard, which is a common type of this crime. The scale of the batch is the key to determining the seriousness of the circumstances, which is directly related to the execution of the case. However, in administrative evidence collection, some subjects pursue efficiency, simplify processes, and ignore the complete collection of batch data, resulting in the lack of key evidence and restricting the effectiveness of execution connection.

The purpose of purpose-based behavior is to commit fraud and other illegal crimes, and the subjective factors are obvious, but it proves that the behavior is subjective. Purpose-based behaviors must collect data such as search records, communication records, transfer records, and abnormal behavior to support the perpetrator's subjective illegal intentions. The extraction of fixed core evidence needs to be standardized to avoid operational flaws leading to invalidation of evidence.

To sum up, the current norms are imperfect and the ability of evidence collection subjects is insufficient to exacerbate the dilemma of execution connection, and it is necessary to clarify the

evidence collection standards, refine the process, and strengthen technical support to solve the problem.

3. The positive connection subject is out of place

The misalignment of power and responsibility in the positive connection between criminal law and crime of illegal use of information network is concentrated in four aspects: conflicting evidence collection standards, poor evidence transformation, lack of early intervention, and inadequate transfer of the whole case.

3.1 Double standards and their conflicts in forensic procedures

There are significant differences between administrative law enforcement and criminal justice evidence collection standards. Administrative evidence collection emphasizes efficiency and flexible procedures; Criminal evidence collection emphasizes fairness and strict procedures. Wang Ziyu pointed out that the theory of "limited access as an exception" formed based on this difference advocates the denial of administrative evidence access to criminal proceedings in principle, which is supported by the theory of exclusivity of the subject of evidence collection and the hierarchical theory of administrative wrongdoing and criminal facts. Both show that administrative evidence should not be directly used to prove criminal facts because it does not meet the requirements of criminal procedures [8]. In practice, administrative evidence is often excluded due to the lack of original media sealing, hash value verification and other elements, and when the public security organs re-collect evidence, the data has been lost due to the easy loss characteristics, making it difficult to prosecute cybercrimes.

Comparative law research shows that Japan's "Law on Punishing the Transmission of Harmful Online Information" provides a better idea .The law recognizes that the standards for forensic collection of executions have their own emphasis, and the standardized connection is achieved through a unified electronic data evidence collection list, and the transformation of evidence is not excluded due to differences in subjects.

3.2 Legal obstacles and practical responses to evidence transformation

The legal obstacles to evidence transformation mainly stem from the difference between verbal evidence and technical evidence. In terms of verbal evidence, Article 54, Paragraph 2 of the Criminal Procedure Law clarifies that physical evidence collected by administrative organs can be used in criminal proceedings, but the legislative interpretation excludes verbal evidence. Scholars generally believe that the stability of verbal evidence is weak, administrative interrogation and criminal interrogation are different, and direct conversion may undermine procedural fairness. In terms of technical evidence, administrative appraisal reports often lack necessary elements and are difficult to meet the requirements of criminal evidence.

German theory provides reference for evidence transformation. The court can use administrative evidence as investigation material ex officio, and the evidence exclusion rule adopts a balance of interests model, which is only excluded when evidence collection seriously violates the basic rights of citizens. This mechanism not only guarantees the access of administrative evidence to ascertain the facts, but also takes the protection of basic rights as the bottom line, providing an important reference for the improvement of China's rules.

3.3 The obligation of public security organs to intervene in advance and its activation mechanism

The lack of the obligation of public security organs to intervene in advance is an important reason for the poor positive connection, which stems from the ambiguity of the system design. There is no specific guidance on the timing of intervention, and in practice, it is mostly the administrative organs asking for help and the public security organs responding passively. The authority to intervene is unclear, too narrow to standardize evidence collection, and too wide may interfere with administrative law enforcement; The feedback mechanism is unclear, and the intervention effect is difficult to sustain, which ultimately leads to lack of evidence or missed correction opportunities.

Early intervention is a necessary prerequisite for ensuring the ability of electronic data evidence and achieving smooth connection. If the public security organs do not intervene in time, it is easy to lead to the loss of evidence or procedural violations, and the case cannot be remedied after it is transferred, so it is necessary to establish an early intervention and activation mechanism from the institutional level.

3.4 Administrative law enforcement agencies' obligation to transfer the entire case

The transfer of the whole case is the legal obligation of the administrative organ to transfer the case, and it is also the basis for the comprehensive determination of the facts in criminal procedures. According to the "Provisions on the Transfer of Suspected Criminal Cases by Administrative Law Enforcement Organs", after discovering suspected criminal clues, administrative organs should transfer all materials within 24 hours, including transfer letters, investigation reports, lists of items involved in the case, inspection reports, etc.

In practice, the obligation to transfer the whole case is often in vain: some administrative organs only transfer some materials, and criminal organs cannot verify the integrity of electronic data and restore the trajectory of behavior, making it difficult to fully determine the facts. Some failed to issue written reports in accordance with regulations, the procedures were not standardized, and even the cases were downgraded, and administrative penalties were used instead of criminal prosecution. In order to reduce the risk of accountability, administrative organs tend to terminate their own procedures or selectively transfer them, resulting in a breakdown in the positive connection between executions.

4. The reverse connection procedure is disconnected

The break of the forward connection makes a large amount of electronic data impossible to enter the criminal process, and the disconnection of the reverse connection will also leave the matters involved in the case unpaid after the criminal process is concluded. When the act does not constitute a crime, whether the administrative illegality is eliminated and how to deal with the electronic data involved in the case are all issues that must be solved in reverse connection.

4.1 Administrative violations after non-prosecution and acquittal verdicts

After the conclusion of the criminal procedure, the case enters the post-event link of reverse connection. The first question is whether the perpetrator who is not prosecuted or acquitted should bear administrative responsibility.

According to the system design, if the procuratorate makes a decision not to prosecute and finds that administrative punishment is necessary, it shall submit a procuratorial opinion and transfer the case materials, including electronic data materials, to the administrative organ. After the court renders

an acquittal verdict, if it finds it necessary to pursue administrative responsibility, it may transfer data materials through judicial recommendations. From the perspective of the system, electronic data could have been provided through administrative disposal. But in practice, this connection practice is not ideal. In the cases where the procuratorate did not prosecute, a large number of cases did not submit procuratorial opinions, and the electronic data was not filed with the case without entering the administrative procedure. After the court's acquittal verdict, there is no rigid constraint on the formulation, issuance and adoption of judicial recommendations, and there are no mandatory requirements for administrative organs to receive electronic data and how to process data. In some cases, it is difficult to transfer electronic data across regions due to the staggered jurisdiction of different jurisdictions.

The time and space blocking of off-site jurisdiction has led to the failure of some illegal acts that should have been punished to enter administrative procedures. As a result, the electronic data involved in the case was also stranded at the terminal of the criminal procedure, neither received nor disposed of. The criminal procedure has ended, the administrative procedure cannot be initiated, the electronic data has fallen into a management vacuum in the aftermath, and the connection between execution and execution has been broken again.

4.2 Obligation to subsequently dispose of electronic data involved in the case

After the administrative accountability procedure is initiated, the electronic data involved in the case will enter the administrative link from the criminal procedure. The standardized disposal of electronic data involved in the case is the core link of the operation of administrative accountability procedures. The data may contain illegal information, and if left untreated, the illegal website or group may continue to operate; If data involving privacy is not handled properly, it may infringe on the legitimate rights and interests of citizens. At present, there is a lack of standardization in data disposal in the reverse connection. There is no clear time limit and list requirements when handing over, and judicial organs often only transfer data carriers, without verification information such as extraction records and hash values, and administrative organs cannot verify the authenticity of the data. There is no obligation to verify after receipt, and no one checks whether the data is complete and tampered with. There is a lack of operational standards for classified disposal, and harmful data is prone to results such as shelving and not deleting and arbitrarily destroying, which seriously affects data quality.

Known laws provide for the collection and extraction of electronic data in criminal proceedings. However, it is not clear how the data will be transferred to the administrative organ in reverse after the conclusion of the criminal procedure, what verification information must be attached to the transfer, and how to complete the verification with the help of external forces when the administrative organ's technical capabilities are insufficient. The three links of handover, reception, and classification and disposal all lack standards that can be followed. Therefore, it is necessary to establish whole-process constraints from the above three links to ensure that the data source is traceable, the content is controllable, and the disposal is verifiable.

4.3 Supervisory functions of procuratorial organs

The implementation of the above links needs to be guaranteed by the supervision of the procuratorial organs. Article 27 of the Administrative Punishment Law clarifies that procuratorial organs shall submit procuratorial opinions and transfer administrative organs to administrative organs for handling cases that do not pursue criminal responsibility in accordance with the law but should be given administrative punishment.

However, in practice, this function has not been effectively performed, and cases are often

terminated directly after non-prosecution, and there is a lack of follow-up on the transfer of electronic data and the disposal of administrative organs. The proportion of procuratorial opinions put forward by procuratorial organs in non-prosecution cases nationwide is less than 30%, and the binding force of opinions is weak, and the phenomenon of administrative organs not giving feedback and not handling is widespread.

5. Optimization of evidence collection governance and responsibility mechanism

5.1 Embedding of technical regulations

To solve the dilemma of electronic data forensics, it cannot only rely on institutional constraints, but also requires technical means to be embedded in the whole process.

First of all, it should be uniformly equipped with evidence collection tools that meet national standards, and operation logs should be automatically generated and attached to the case. Data can be introduced into the blockchain for storage, and the advantages of blockchain to ensure the transparency, authenticity, and integrity of each transaction can be used, and the hash value can be written into the judicial blockchain during evidence collection, fundamentally preventing evidence tampering [9]. Secondly, relevant departments such as the administration and justice should jointly formulate metadata extraction specifications, clarify the scope and format of extraction of IP addresses, registration information, etc., and solve the problem of difficulty in proving intent due to the lack of metadata. Just as analyzing computer memory requires delving into its running process to detect malicious hijacking, electronic data forensics must also delve into its "operating process" and internal structure to discover hidden facts [10]. Finally, a cross-platform forensic list system should be implemented, requiring platforms to provide data with integrity checkpoints to solve the problem of data fragmentation caused by information fragmentation. The embedding of technical means can make the whole process of data flow traceable and ensure the authenticity of evidence from the source.

5.2 Unification of evidence rules

The conflict in the standards for forensic collection stems from the fact that too much emphasis is placed on the subject of evidence collection rather than the content of the evidence collection, resulting in administrative evidence being excluded due to procedural defects and re-collection of evidence due to data loss. The way to solve this problem lies in establishing a unified review standard centered on the quality of evidence. At the level of review standards, whether the evidence is collected by the administrative organ or the public security organ, as long as the evidence collection procedure is legal, the verified hash value is consistent, the original media is sealed intact, and the extraction record is complete and can be used in criminal proceedings. At the level of specialized evidence, evidence such as inspection reports issued by administrative organs can be accepted within an appropriate range after reviewing the scientific qualifications and methods of the appraisal institution; At the bottom line guarantee level, evidence of serious procedural violations should still be excluded, retaining the last line of defense for rights protection. This rule not only eliminates standard conflicts, but also avoids data loss caused by repeated forensics.

5.3 Coordination of departmental responsibilities

The root cause of problems such as the absence of early intervention, the transfer of the whole case to be vacant, the difficulty of initiating administrative accountability, and the lack of standardization of data disposal lies in the unclear responsibilities and poor connection of the main body of each link.

The list of responsibilities of each link can be standardized. At the level of positive connection, the public security organs will be present within 24 hours to guide the collection of evidence for cases involving overseas or massive data, and directly extract key evidence when necessary. At the reverse connection level, the judicial organ shall hand over the data and list of the competent administrative organ at the same level within 15 days after the non-prosecution or acquittal verdict, attach the extraction record and hash value, and perform the relevant obligations of evidence processing; At the level of disposal specifications, the administrative organs verify the integrity of the data and feedback the disposal within seven days after receiving it, promptly delete harmful data, desensitize and treat private data, and standardize and seal neutral data, so as to reduce the problem of retention of harmful data and information. Through the coordination of the responsibilities of various departments, a full-process circulation mechanism will be formed from data generation to disposal.

5.4 Improvement of accountability mechanism

The long-term absence of supervision in the reverse connection, the low proportion of procuratorial opinions, and the common lack of feedback and handling by administrative organs are rooted in the fact that there are no rigid constraints on responsibilities and no consequences for inaction, and it is necessary to strengthen accountability. At the level of supervision mechanisms, procuratorial organs establish tracking ledgers to supervise the complete transfer of data by criminal organs and the disposal of administrative organs in accordance with the law, so as to ensure that there is follow-up in all links. At the level of accountability means, if the public security organs do not reply within the time limit or are improperly disposed of, preemptively formulate and issue procuratorial suggestions to supervise and correct them, and if necessary, file administrative public interest litigation, and transfer the public security organs to the supervision organs for accountability if they do not transfer them in a timely manner and cause evidence to be lost, so as to solve the problem of inaction without consequences. At the level of assessment and incentives, the handling of administrative organs should be moved or downgraded into the law enforcement performance appraisal, and the reverse connection work should be included in the scope of case evaluation by procuratorial organs. Rigid accountability makes the connection between execution and execution from procedural idling to effective closed loop.

6. Conclusion

This study combines the theory of criminal composition and the theory of procedural connection, and takes the before, during, and after as the analysis framework to systematically investigate the dilemma of electronic data forensics for the crime of illegal use of information networks. From the perspective of the theory of criminal composition, the uncertainty and preparatory characteristics of the network, illegality determination and preparatory characteristics of this crime bury the problems of ambiguous evidence collection authority and mismatch of evidence forms at the beginning of law enforcement. From the perspective of procedural connection theory, the characteristics of crime at the pre-event level, the standard conflict and transformation obstacles at the in-process level, and the supervision vacuum at the post-event level are superimposed on each other, resulting in the loss or exclusion of electronic data in the whole process of execution connection.

At the level of comparative law, by drawing on Japan's unified evidence collection list model and Germany's evidence access mechanism for weighing interests, it is further confirmed that the core of the connection between execution lies in the unification of evidence standards and the closed loop of the responsibility system. The research shows that to solve the dilemma of connecting the execution of electronic data evidence collection and execution of this crime, it is necessary to promote coordinated promotion from four dimensions: technical regulation, evidence rules, departmental

responsibilities, and accountability. Technical regulation is embedded in the whole process of evidence collection to ensure the authenticity of evidence from the source; The rules of evidence establish quality-centered review standards and eliminate standard conflicts and barriers to transformation. The list of departmental responsibilities clarifies the tripartite responsibilities of the complete transfer of public security organs, standardized disposal by administrative organs, and supervision of the whole process by procuratorial organs. The accountability mechanism is implemented with a rigid accountability guarantee system, realizing a benign closed loop in the procedural and substantive aspects of execution connection.

References

[1] Qian, G. F., & Sun, P. Q. (2023). On the collaborative governance model of administrative and criminal enforcement in electronic data investigation and forensics. Network Security Technology & Application, (8), 138–140.

[2] Jain, R., & Sonowal, B. (2025). Analyzing the procedure for investigation in cybercrime and admissibility of electronic evidence. In M. Chawki & A. Abraham (Eds.), Cybercrime unveiled: Technologies for analysing legal complexity (pp. 265–289). Springer. https://doi.org/10.1007/978-3-031-80557-8_12

[3] Guo, H. (2023). New paths for the connection and governance of administrative law enforcement and criminal justice in telecom and network fraud crimes. China Legal Science, (12), 95–101.

[4] Xie, D. K. (2018). Subject of electronic data forensics: Between legality and technical legitimacy. Global Law Review, 40(1), 83–99.

[5] Ma, H. S. (2023). The application of electronic administrative evidence in cases involving the connection between administrative and criminal proceedings. Network Security Technology & Application, (4), 151–153.

[6] Zhang, Z. T. (2024). Institutional dilemmas and solutions for the transformation of administrative law enforcement evidence into criminal evidence. Comparative Law Review, (4), 118–132.

[7] Pei, W. (2019). Research on the connection of electronic evidence rules before and after criminal filing: From the perspective of the procedural nature of electronic data evidence. Contemporary Law Review, 33(2), 114–126.

[8] Wang, Z. Y. (2026). How can administrative evidence be admitted into criminal procedure: Theoretical reinterpretation from the perspective of the connection between administrative and criminal justice. Law Science Magazine, 47(1), 155–171. https://doi.org/10.16092/j.cnki.1001-618x.2026.01.009

[9] Sonowal, B., & Jain, R. (2025). Securing evidence in digital forensics using blockchain. In L. M. Patnaik, G. T. Raju, & N. H. Prasad (Eds.), Advances in data science and artificial intelligence: Proceedings of ERCICA 2024, Volume 1 (pp. 395–408). Springer. https://doi.org/10.1007/978-981-96-4430-8_28

[10] Kävrestad, J., Birath, M., & Clarke, N. (2024). Memory analysis. In Fundamentals of digital forensics (pp. 205–210). Springer. https://doi.org/10.1007/978-3-031-53649-6_18