A Study on The Current Status of Electronic Evidence Preservation in Internet Crime

Yuanqi Chen [1, *], Mingsi Li [2] and Yu Qiu [3]

[1] Law School, East China University of Political Science and Law, Shanghai, China

[2] Law School, China Foreign Affairs University, Beijing, China

[3] Law School, Southeast University, Nanjing, China

* Corresponding Author Email: 212125010219@ecupl.edu.cn

Abstract. This article focuses on the electronic evidence related to internet crime, exploring legal systems related to electronic evidence and legal issues related to information technology. The paper discusses the concept and characteristics of electronic evidence in internet crime, analyzes the relevant technologies and legal systems used for preserving electronic evidence in China, and highlights potential issues. Furthermore, a comparative legal study is conducted, examining the electronic evidence rules in the Anglo-American legal system and the Continental legal system, with reference to judicial cases in Japan and the United States. This analysis emphasizes the similarities and differences in electronic evidence rules and admissibility criteria. Finally, the paper proposes strategies to address the challenges faced in electronic evidence preservation in China from both a technological and systemic perspective. By addressing the arguments above, this article holds theoretical and practical significance in enhancing the legal framework and standardizing electronic evidence practices in China.

Keywords: Cybercrime; Electronic Evidence; Blockchain.

1. Introduction

In recent years, new forms of internet crime have exhibited diverse developments, with activities such as online fraud and internet gambling utilizing information technology on the rise. The evidence for such crimes often appears in the form of electronic data. Due to the inherent challenges of electronic data, such as its difficulty in preservation, complexity, and susceptibility to change, investigating new types of internet crime cases presents additional difficulties in obtaining electronic evidence compared to traditional criminal cases.

Regarding the authentication of electronic evidence, Article 50 of the Criminal Procedure Law of the People's Republic of China stipulates that materials that can be used to prove facts in a case are all considered evidence. As for the rules for obtaining electronic evidence, the "Rules for the Collection of Electronic Data in the Handling of Criminal Cases by Public Security Organs," published by the Ministry of Public Security in 2019, states in Article 6 that "collection and extraction of electronic data should be conducted by two or more investigators. When necessary, professional technicians may be assigned or hired to collect and extract electronic data under the supervision of investigators." It can be observed that China has only established departmental normative documents at the practical level and has not enacted specialized legislative regulations for the preservation and authentication of electronic evidence.

Currently, the normative standards for electronic evidence in new types of internet crime cases are not comprehensive enough. Therefore, the continuous improvement of relevant regulations regarding electronic evidence in internet crime is essential to effectively combat these emerging forms of crime and enhance judicial efficiency.

2. Overview of Electronic Evidence in Cybercrime

As computer technology continues to advance, the proportion of crimes committed using high-tech means is constantly increasing, highlighting the crucial role of electronic evidence in judicial

practice. Although there are no specific legal definitions for electronic evidence, fundamentally, electronic evidence refers to materials stored in electronic data form within devices that can be used to prove the facts of a case. Electronic data, on the other hand, is data and information stored in physical forms such as electronic or optical signals within computer systems or storage devices, primarily consisting of text, symbols, numbers, letters, and the like [1].

Based on the definitions of electronic evidence and electronic data, three characteristics can be inferred:

First, electronic data is stored in media in the form of numbers and symbols, which, compared to other evidence such as witness testimony, is more objective and precise.

Second, electronically stored evidence in data form is highly vulnerable, with risks of loss and tampering, making it inherently mutable, posing a challenge when handling electronic evidence.

Third, electronic evidence serves as a bridge between computer science and law, possessing high technological complexity, necessitating interdisciplinary expertise to engage in related work. Electronic evidence allows for convenient retrieval and analysis, saving considerable time and manpower costs. Furthermore, electronic evidence facilitates more convenient and effective cross-jurisdictional investigations and litigation, playing a significant role in the proper functioning of the judicial system and society.

3. Current Status of Electronic Evidence Collection in China

3.1. Technical Means of Electronic Evidence Collection in China

In practice, electronic evidence collection in China employs the method of directly sealing the original storage media. If it is not possible to seize the original media, electronic data may be printed, photographed, or recorded.

The sealing of the original storage media places significant emphasis on preserving the integrity of the evidence to ensure its authenticity. For instance, when electronic data is stored on a computer, and it needs to be used as evidence, the investigating authorities first consider sealing the original storage media, which is the computer itself. The investigating authorities use methods such as video recording to document the location of the original media, and then they record the entire process from sealing the computer to unsealing it and conducting examinations. This meticulous approach guarantees the continuity of electronic evidence from extraction to presentation in court.

It is evident that whether confiscating the original media or printing, photographing, or recording electronic data, the approach to handling electronic evidence still resembles the treatment of physical evidence. However, with the development of modern society and the rise of blockchain technology in the past decade, this technology aligns perfectly with the need in the judicial field for secure storage and preservation of electronic evidence.

The Opinions of the Supreme People's Court on Strengthening the Judicial Application of Blockchain, released on May 23, 2022, not only recommends that the People's Courts establish blockchain platforms but also emphasizes the need for blockchain's robust anti-tampering technology to safeguard judicial data security and the credibility of electronic evidence. Some notary offices have already launched blockchain electronic data certification platforms online, indicating that blockchain technology has significant potential for development in the field of judiciary in the future.

3.2. Legal Regulations for Electronic Evidence Collection in China

To regulate the actions of investigative agencies when extracting electronic evidence stored in electronic data form in criminal cases, relevant authorities have established corresponding documents to govern the conduct of investigative agencies.

3.2.1 Rules for the collection of electronic data in the handling of criminal cases by Public Security Organs

The Ministry of Public Security, in accordance with relevant laws such as the Criminal Procedure Law of the People's Republic of China and drawing from practical experience, has formulated the Rules for the Collection of Electronic Data in the Handling of Criminal Cases by Public Security Organs. These rules provide specific regulations on how public security organs should extract different electronic data using various methods under different circumstances. They also cover procedures related to the examination, investigative experiments, entrusted examinations, and authentication of electronic data. These rules serve as a regulatory foundation for electronic evidence collection in China.

3.2.2 Interpretation of the Supreme People's Court on the Application of the Criminal Procedure Law of the People's Republic of China

This judicial interpretation, located in Chapter IV on evidence, dedicates a specific section to the examination and authentication of audiovisual materials and electronic data. Article 93, in the manner of enumeration, first lists specific forms of electronic data, such as emails, electronic data exchanges, online chat records, blogs, microblogs, mobile text messages, electronic signatures, domain names, and more. It then, from the perspective of the "three characteristics" of evidence, namely, authenticity, legality, and relevance, provides regulations for the examination of electronic data.

Article 94, on the other hand, sets forth circumstances in which audiovisual materials and electronic data cannot serve as a basis for concluding a case. This can be regarded as a rule of unlawful exclusion for audiovisual materials and electronic data. This provision takes into consideration the authenticity and legality of evidence but does not address the situation where audiovisual materials and electronic data lack relevance to the case's conclusion. Consequently, there is a regulatory gap in Article 93, specifically in the fourth provision, which addresses the examination of the relevance between electronic data and the facts of the case and lacks subsequent guidelines on how to handle cases where no such relevance exists. In practice, it is indisputably essential to examine the relevance between electronic data and the facts to be proven and make determinations accordingly.

3.2.3 Online Litigation Rules

In the realm of electronic evidence, blockchain technology is an undeniable topic due to its capability to ensure the integrity and authenticity of evidence. The theoretical foundation of blockchain technology is robust, but its effectiveness relies closely on the relevant actors in blockchain applications. Consequently, there are corresponding legal restrictions on blockchain technology [2]. Articles 16 and 17 of the "Online Litigation Rules" stipulate that evidence uploaded to a blockchain platform by parties, if verified consistently, can be recognized by the People's Court, except when there is other evidence sufficient to overturn it. If a party has a valid reason to raise objections to the authenticity of evidence uploaded to a blockchain platform, the People's Court should make judgments based on factors such as the blockchain evidence platform itself and the process of evidence storage technology.

Although legal documents related to electronic evidence have been gradually introduced in recent years, there are still imperfections. For instance, in criminal litigation cases, some victims or their close relatives may obtain electronic evidence through their own means, such as seeking electronic experts or even hiring hackers. It is evident that there is no legal basis for either the subject's qualifications or the methods or means of evidence collection. Therefore, faced with the overwhelming wave of the information age where electronic information serves as a social medium, establishing a comprehensive electronic evidence system, specifying who can do what, outlining the legal responsibilities, and more, is a pressing necessity [3].

4. Comparative Legal Research

In today's era of technological advancement, with the proliferation of computer network crimes, the research on procedures for electronic evidence collection and preservation has become a contemporary research focus. Of course, different countries have varied legal viewpoints. This article will conduct separate studies on the evidence-related systems in different legal systems around the world:

4.1. Electronic Evidence Systems in Common Law Legal Systems (such as the United Kingdom and the United States)

In common law legal systems like those in the United Kingdom and the United States, electronic evidence is primarily governed by the best evidence rule, along with statutory provisions and case law from federal and state courts.

4.1.1 Application of U.S. Rules on Electronic Data Evidence

As of today, the United States has not enacted specific legislation governing electronic data but rather relies on a combination of statutory procedures, electronic commerce laws, and precedents from federal and state courts to constitute the applicable rules for electronic data [4]. As a representative country of the common law tradition, the United States adheres to the traditional principles of the best evidence rule and provides detailed regulations for authentication under Federal Rules of Evidence Rule 901(a). Authentication is defined as the process by which evidence is shown to be what it purports to be before it is admitted into legal proceedings or presented in court. While authentication requirements have presented challenges in securing electronic evidence, they offer reliable safeguards for establishing the authenticity of electronic evidence and preventing biases in favor of traditional forms of evidence [5].

Furthermore, in the early 20th century, the United States established rules for the exclusion of illegally obtained evidence to curb abuses of state power. These rules primarily encompass substantive and procedural aspects. Substantive rules define the scope and boundaries of illegally obtained evidence, while procedural rules specify operational procedures for excluding such evidence. These provisions are primarily aimed at preventing unlawful police conduct during evidence collection and preserving the effectiveness of the collection process.

4.1.2 Application of Electronic Data Evidence Rules in Canada

Canada has drawn guidance from the United States' legislation and practices concerning electronic data and has made innovations based on them. In 1998, Canada introduced the Uniform Electronic Evidence Act, which broke away from traditional evidence rules. This Act was the world's first dedicated legislation on electronic data, expanding the scope of electronic evidence and establishing new standards for the integrity of electronic records. It recognized that the integrity of electronic records could be maintained even when computer systems or other devices were not functioning correctly during critical moments in the evidentiary process. Concurrently, under the influence of U.S. legislation and judicial practices, Canada also applies rules on authentication, with a comprehensive classification system. Taking the Uniform Electronic Evidence Act as an example, it embodies a rigorous examination and assessment procedure for electronic data. Article 3 of this Act specifically outlines the methods for authentication of electronic data. It stipulates that the authenticity of electronic data must be supported by evidence through rulings, and the forms of authentication include oral or certified evidence. The Act also mandates that electronic data must possess authenticity and that the presentation of the original is required to achieve this purpose.

4.2. Electronic Evidence: Related Systems in Continental Legal Systems

In contrast to common law systems like those in the United Kingdom and the United States, countries following the continental legal system have not established independent legal frameworks specifically addressing electronic evidence. Instead, they typically apply relevant rules to regulate

electronic evidence within the context of case proceedings [6]. Taking Germany, a typical representative of the continental legal system, as an example, while Germany has not enacted standalone legislation governing the collection and authentication of electronic evidence, it places significant emphasis on the issue of authenticity concerning electronic evidence. However, the focus primarily lies in the content and procedures for authentication. Germany operates under an inquisitorial legal system, where judges play a prominent role in litigation proceedings. Authentication can occur not only during court investigations but also in preliminary trial procedures [7]. During court proceedings, judges in Germany have the authority to exclude evidence that lacks a clear connection to the case. Additionally, judges may question witnesses and experts during court investigations to ascertain the authenticity of the matter and its relevance to the case. After comprehensive consideration, judges make their judgments based on the authenticated evidence.

From this, it can be observed that in Germany, the emphasis on authenticating electronic data primarily pertains to the authenticity of evidence content and its relevance to the case. Final judgments are made based on a comprehensive assessment of authenticated evidence.

4.3. Case Analysis: Comparative Study of Handling Electronic Evidence in Different Legal Systems of the United States and Japan

Utilizing the case of Lorraine v. Markel American Insurance Company, which took place in the United States in 2007, we conducted a comparative study of how the legal systems of the United States and Japan handle electronic evidence. The following conclusions were drawn:

Firstly, let's provide a brief overview of the case: The plaintiff, Lorraine, had her yacht struck by lightning and received compensation from Markel American Insurance Company based on her insurance policy. However, several months later, significant additional damage to the yacht was discovered. The insurance company contended that this new damage was not caused by lightning and was outside the scope of the insurance policy. In response, the insurance company initiated a declaratory judgment action. Since this article primarily focuses on the study of the legal framework for electronic evidence, we specifically discuss the electronic evidence presented in this case, which comprises email communications between the parties' attorneys.

4.3.1 America

Regarding the electronic evidence presented by both parties in this case, Judge Grimm proposed five criteria for the admission of electronic evidence: (1) it is relevant (Federal Rule of Evidence 401); (2) it is authentic (Federal Rule of Evidence 901(a)); (3) it is not hearsay (Federal Rule of Evidence 801), and if it is, then it is subject to the requirements of the exceptions (Federal Rules of Evidence 803, 804, and 807); (4) it must comply with the "rules of original evidence", and, if it is not, then it must comply with the rules of derivative evidence (Federal Rules of Evidence 1001-1008); and (5) the probative value of the electronic evidence outweighs the likelihood that it would cause unfair prejudice, or any other factor set forth in Federal Rule of Evidence 403. And he engaged in a series of scholarly discussions, resulting in a judicial opinion. This case marked a significant departure from the longstanding practice of U.S [8]. Federal courts declining jurisdiction over "cases or controversies" lacking practical significance.

Judge Grimm's discussions on the admissibility of electronic evidence provided a pioneering approach, making this case the first to discuss the judicial acceptability of electronic data. Although the electronic evidence presented by both parties in this case was ultimately not admitted, the court's scholarly discussion of the evidence and its inclusion within the admissible category represented a significant advancement. After all, from a technical standpoint, this diverged from the requirement that judgments and motions must be supported by sworn testimony [8].

The judicial opinion on electronic evidence issued by Judge Graham has greatly facilitated the use of electronic evidence in American courts and has supported the construction of the American legal system of electronic evidence. Similarly, this case can be seen from the rule of hearsay and the best evidence rule is a great obstacle to the adoption of electronic data as evidence. To solve the "hearsay" this difficulty, the United States has developed a "business records exception", that is, the daily

business activities can be stored in the document management personnel or other qualified witnesses to provide testimony, if it can be proved that these materials are the right cut to obtain the correct way, then it can be used as evidence in court. As long as it can be proved that these materials were obtained in the correct manner, they can be used as evidence in court. At the same time to ensure the use of the best evidence rule, the United States of America on the source of electronic data to make screening, found that the best evidence is stored in the medium of 0101 original bit stream, but its need for screen display, which will break his original features, so the United States of America Electronic Evidence Act as an exception to the rule of the best evidence, and explicitly put forward the "if the data is stored in a computer or similar device, any printout or output by other visual means is 'original' if it accurately reflects the data itself."

4.3.2 Japan

In Japanese civil and criminal litigation, due to the presence of judicial discretion, expert witnesses, and printed records, as well as the diverse and unpredictable forms of electronic data, there are no specific regulations regarding electronic data used as evidence. Therefore, general examination rules pertaining to evidence are followed. In civil litigation, documents presented as evidence should be the originals or certified copies. According to this rule, electronic data recorded in media can be considered the original data, and both the storage media and printed copies can be presented to the court as quasi-documentary evidence. When required to provide necessary supplementary explanations for the evidence presented, the parties involved should actively cooperate, as failure to do so may result in unfavorable judgments by the judge exercising discretion [9].

In the case at hand, both the plaintiff and defendant submitted printed email records to the court. Under Japan's legal framework, printed records are crucial for examining electronic storage records, and therefore, email printouts can be admitted as evidence in court. If there are objections to the authenticity or reliability of the printouts, it becomes necessary to have digital evidence experts examine the underlying electronic data, and the court may summon the operator of the electronic records to testify.

4.3.3 Comparative summary

In conclusion, although the United States and Japan exhibit formal differences in their procedures and systems for recognizing electronic evidence, their substantive requirements for electronic evidence are fundamentally consistent. Materials should originate from original data, and written evidence should represent the storage media. Additionally, both jurisdictions allow testimony from the parties or other qualified individuals holding the evidence to establish its authenticity.

5. Strategies to Improve China's Electronic Access to Evidence Dilemma

5.1. Science and Technology

Preserving evidence within the blockchain can prevent tampering and deletion of evidence, thereby ensuring the reliability of the process of gathering evidence. Additionally, the immutability of the blockchain guarantees the integrity and authenticity of evidence. Furthermore, blockchain technology can provide a more efficient electronic evidence collection process. The use of smart contracts can automate the evidence collection process, reducing human intervention and errors. Moreover, blockchain possesses characteristics such as transparency and traceability, which can enhance the efficiency of evidence collection while reducing disputes and controversies. However, it still faces several challenges, including the need to improve processing speed and throughput, as well as the requirement for regulatory and legal frameworks.

5.1.1 HASH Calculation for identity verification to ensure information authenticity

In the blockchain, mutual verification between private keys, public keys, and addresses ensures the authenticity of evidence information. Each user possesses a unique binary private key generated from a random number. There exists a specific functional relationship between private keys, public

keys, and addresses. When certain evidence information is transformed into binary digests through HASH calculation and then encrypted using a private key, it generates a password. Finally, this password, along with the original information, is uploaded to the blockchain network space. In the case of subsequent verification of identity authenticity, i.e., determining whether the information record uploader and the password uploader are the same person, one simply needs to extract the information record and the password separately. When extracting the information record, it automatically transforms into a binary digest through HASH calculation. After extracting the password, a digest is obtained through decryption using the public key. Finally, the two digests are compared. If the digest generated from the information record matches the one obtained through decryption, it indicates that the private key holder is the same as the information record publisher, ensuring identity consistency [10].

5.1.2 Longest Chain Principle to prevent data tampering

Blockchain, as the name implies, is a chain formed by linking many blocks, each containing various information, such as transaction values, timestamps, random numbers, and more. Transaction values represent evidence information, and timestamps indicate the time of evidence publication. Each block calculates its HASH value based on the HASH value of the previous block and the information contained within itself. The information within a block remains unchanged except for the random number, which is mined to calculate the required HASH value. When a user correctly calculates the prescribed HASH value using the correct random number, the block is confirmed. Additionally, blockchain follows the principle of the longest chain, where only the longest chain is considered valid, and shorter chains are deemed invalid.

Consequently, if someone attempts to alter the record values within a particular blockchain block, both the record values and timestamps will change, resulting in the creation of a new block. However, this new chain will not be the longest chain and, thus, will be invalidated.

5.2. Legal System

As the digital society and legal environment continue to evolve, it is imperative to continually refine China's legal framework for electronic evidence collection. The primary objectives of this improvement should encompass the following aspects: Firstly, it is essential to clearly define the legal framework for electronic evidence collection to ensure the legality and reliability of evidence. This includes ensuring that the collection, preservation, and presentation of electronic evidence adhere to legal requirements to uphold fairness and judicial credibility. Secondly, the legal framework must keep pace with technological advancements to adapt to evolving digital technologies and communication tools. Thirdly, the legal system should emphasize privacy rights and data protection, ensuring the respect of individual privacy during electronic evidence collection while striking a suitable balance between the needs of criminal justice and privacy protection measures. This will contribute to building public trust in the electronic evidence collection process and can be manifested in the following points:

5.2.1 Establishing special regulations for electronic evidence collection

Defining standards for electronic evidence authentication, collection procedures, and evidence preservation measures to ensure the legality and reliability of the collection process.

5.2.2 Constructing an electronic evidence storage and management system

Ensuring the security and traceability of electronic evidence. This system can utilize blockchain technology to prevent tampering and deletion of evidence.

5.2.3 Adopting a warrant principle

This principle underscores the legality review of personal electronic information data to prevent unauthorized access. According to the warrant principle, law enforcement agencies must obtain court approval when obtaining personal electronic information data and clearly define the scope and purpose of the information obtained. When using the obtained personal electronic information data,

law enforcement agencies must strictly adhere to legal limitations and procedures to ensure the legal use of data and the protection of individual rights.

6. Conclusion

Cybercrime is on the rise, and electronic evidence plays a crucial role in cybercrime investigations and cybersecurity. This article has focused on electronic evidence in the context of cybercrime, analyzing the technical means and legal frameworks for electronic evidence collection in China. It has also compared these with different legal systems in other countries, highlighting the shortcomings in China's electronic evidence technology and legal provisions. Recommendations have been made to address these deficiencies.

Through the proposed improvements, China's methods of electronic evidence collection will be better suited to meet the demands of the contemporary digital society. This will promote justice and the rule of law while safeguarding the rights and freedoms of citizens. In the future, research on the application of blockchain technology and the refinement of legal regulations can provide new avenues for the acquisition and preservation of electronic evidence. These advancements can lead to more effective countermeasures against cybercriminal activities, enhanced data security, the assurance of procedural fairness, and increased judicial efficiency, ultimately saving judicial resources.

Authors Contribution

All the authors contributed equally and their names were listed in alphabetical order.

References

[1] Hong Dongying. General Introduction to Civil Procedure Law. Peking University Press, 2020.

[2] Zhu Chenyang. Review of the Admission and Admissibility of Electronic Evidence in Civil Litigation. Shanghai Law Research Collection 2023, Volume 10 - Anthology of Chinese Excellent Traditional Legal Culture. Shanghai Law Society, 2023:126-135.

[3] Pei Zhaobin. On the mode of electronic data forensics in criminal proceedings. Oriental Law, 2014(05):87-95.

[4] Liu Baochen. On the Rules of Electronic Data Evidence in Criminal Proceedings, 2022(06).

[5] Lund, Paul. An investigators' Approach to Digital Evidence. Digital Evidence and Electronic Signature Law Review, 2009,06: 220-222.

[6] Chen Jian. Study on legal issues of electronic evidence collection. Hebei University of Economics and Business, 2020(05):13-14.

[7] Qiu Aimin. Study onthe System of Authentication of Physical Evidence. Beijing Intellectual Property Press, 2013:132.

[8] Esler, Brian W. Lorraine v Markel: Unnecessarily Raising the Standard for Admissibility of Electronic Evidence. Digital Evidence and Electronic Signature Law Review, 2007, 04: 80-82.

[9] Kaneko, Hironao. "Electronic Evidence in Civil Procedure in Japan." Digital Evidence and Electronic Signature Law Review, 2008,05: 211-213.

[10] Xu Ronghong. Research on electronic evidence storage technology based on blockchain. North China University of Technology, 2022.