International Journal of World Economic Research
ISSN: 3080-9886 (Print), ISSN: 3080-9894 (Online) | Vol. 2, No. 3, 2026

Discuss the Value of Electronic Data as Evidence and The Criteria for Its Examination and Judgment

Xiaoyu Zhang

School of Law, Anhui University of Finance & Economics, Bengbu Anhui 233030, China

Abstract: In the context of digital litigation, electronic data has become the most frequently used new type of legal evidence in civil, commercial, administrative, and criminal proceedings. Relying on binary code storage, electronic data differs from traditional documentary evidence and electronic documents, possessing unique attributes such as intangibility, ease of alteration, and reproducibility. While it has evidentiary value in efficiently reconstructing case facts and optimizing the allocation of judicial resources, it also suffers from inherent defects such as irregular evidence collection and difficulties in verifying authenticity. This paper, drawing on the research findings of scholars such as Peng Chasan, Zhao Changjiang, and Zhang Xin, clarifies the legal boundaries between electronic data and electronic documents, analyzes the diverse judicial value of electronic data, constructs a complete review and judgment standard around the three dimensions of evidentiary relevance, legality, and authenticity, and proposes improvement paths based on current pain points in investigative and administrative judicial practices.

Keywords: Electronic data, Evidence review, Evidence collection regulations, Electronic documents.

1. Introduction

In 2012, my country's Criminal Procedure Law and Civil Procedure Law simultaneously added electronic data as independent legal evidence, ending its long-standing awkward position of being dependent on audiovisual materials and documentary evidence. In judicial practice, disputes over online lending, online defamation, telecommunications and network crimes, and administrative information disclosure almost always rely on chat logs, backend logs, and cloud data for case resolution. However, judicial practice has long confused the legal application rules of electronic data and electronic documents, resulting in frequent procedural flaws in the search and extraction of electronic data by investigative agencies, and highlighting the difficulty in proving the authenticity of electronic data in administrative litigation. Existing research includes Zhao Changjiang focusing on criminal evidence rules, Liu Yanjun examining investigative evidence collection from the perspective of power control, Huang Youyong conducting research specifically on administrative litigation scenarios, and Peng Chasan clarifying the fundamental conceptual differences between electronic data and electronic documents. Based on existing literature, this paper unifies the general review logic of the three major litigation systems, systematically explains the evidentiary value and review and judgment rules of electronic data, and responds to practical disputes in line with evidence law classroom theory.

2. Definition and Basic Legal Analysis of Electronic Data

Based on the judicial interpretations on electronic data issued by the Supreme People's Court, the Supreme People's Procuratorate, and the Ministry of Public Security, and the conclusions of Peng Chasan's "Comparative Study on the Legal Regulation of Electronic Data and Electronic Documents" [5], electronic data refers to a collection of binary data formed during the course of a case, stored, processed, and transmitted in digital form, capable of directly proving the facts of the case. Typical forms include social media chat logs, server operation logs, bank transfer records, and device location data. In practice, it is easily confused with electronic documents. The core difference between the two lies in their purpose of formation and their evidentiary logic: electronic documents are records kept in official and commercial activities, mainly used for internal archiving, and are only converted into evidence when retrieved afterward; electronic data, on the other hand, naturally carries factual information about the case from its inception and can be used directly as evidence without secondary conversion.

Based on Liu Yanjun's research, "A Study on Electronic Data Investigation and Evidence Collection Procedures under the Perspective of Power Control" [3], three unique characteristics of electronic data can be summarized: First, its carrier dependence, meaning it cannot be displayed independently without storage media such as mobile phones, servers, and hard drives; second, its traceless tamperability, meaning that modifications to the underlying code leave no visible trace and can only be verified through technical means; and third, its multiple copies sharing the same source, meaning that the original data, cloud backup data, and synchronized mirror data have the same evidentiary value. These characteristics directly determine that the evidentiary advantages and examination difficulties of electronic data coexist, and the logic of traditional documentary evidence examination cannot be applied.

3. The Core Judicial Value of Electronic Data as Evidence in Litigation

3.1. Objectively Reconstructing the Facts of The Case and Making Up for The Shortcomings of Traditional Evidence

Traditional verbal evidence is highly susceptible to the influence of the parties' subjective perceptions and interests, leading to false statements. Paper-based evidence is also vulnerable to destruction, alteration, and loss. In contrast,

electronic data contains metadata such as timestamps, IP addresses, and device MAC addresses. This metadata is automatically generated by the system, making human intervention extremely difficult. Sun Mingze, in his research "A Study on the Procedural Regulation of Electronic Data Collection by Investigative Agencies" [4], points out that in cybercrime cases, the rate of contradiction in verbal evidence exceeds 60%, making electronic data the only direct evidence capable of objectively reconstructing the sequence of events and the content of interactions. For example, in telecommunications fraud cases, the suspect's transfer time, login location, and chat scripts can all be completely reconstructed from the raw backend data, without relying on corroborating witness testimonies.

3.2. Balancing the Evidentiary Capacity of Public and Private Entities to Implement the Principle of Equality in Litigation

In administrative litigation, administrative organs have long held access to administrative ledgers and internal approval documents, naturally placing the opposing party at a disadvantage in terms of evidence. Huang Yongyou's "A Study on the Authenticity of Electronic Data in Administrative Litigation" [2] points out that with the widespread adoption of online government communication, administrative counterparts can retain electronic data such as text messages, dialogues on government platforms, and online application receipts themselves, without relying on the administrative organs to disclose internal documents, thus reversing the imbalance in the burden of proof in administrative litigation. In the criminal field, the entire process of electronic data evidence collection leaves a trace, which can, in turn, constrain public power. Zhang Xin's "A Study on the Legal Regulation of Electronic Data Search" [1] proposes that each step of electronic data search, seizure, and mirror extraction generates system logs, which can supervise investigative organs to prevent them from overstepping their authority to search citizens' private storage devices, thereby achieving data boundary control over public power.

3.3. Adapting to Digital Justice to Reduce Litigation Costs Throughout the Entire Process

Compared to paper evidence, which requires physical sealing, storage, and in-court transfer of the original documents, electronic data can be backed up losslessly through mirroring and hash-based solidification, with storage costs approaching zero. This also aligns with the asynchronous evidence presentation rules of online trials, allowing parties to submit solidified electronic data online for cross-examination without needing to present the original device in court. However, its inherent limitations must be acknowledged: electronic data is highly susceptible to distortion due to equipment failure, network viruses, or human deletion. Even if recovered technically, data fragmentation and corruption may occur, rendering it ineffective as evidence. This is the fundamental reason for establishing strict review standards.

4. Three-Dimensional Review and Judgment Standards for Electronic Data

Based on the general three-dimensional framework for the review of evidence and the research conclusions of six references, the review of electronic data follows a progressive review order of "relevance first, legality as a baseline, and authenticity as the core." If the preliminary review is not passed, no further verification is required.

4.1. Relevance Review: The First Hurdle for Evidence Admission

Relevance review is divided into formal relevance and substantive relevance. Formal relevance verifies the ownership of the data subject, confirming whether the account and device were used by the parties involved in the case, and excluding anonymous data without binding to the account. Substantive relevance verifies the causal relationship between the data content and the facts to be proven, distinguishing between direct and indirect relevance. For example, in private lending, transaction records are directly relevant data, while the transferor's daily consumption records are irrelevant data and should be directly excluded. Unlike electronic documents, electronic data does not require interpretation in conjunction with other materials and can be independently used to determine relevance, which is the core difference between the two review standards (Peng Chasan, 2022) [5].

4.2. Legality Review: The Core Basis for Excluding Evidence's Admissibility

The legality review focuses on the entire process of evidence collection, search, and preservation, with a key emphasis on regulating the evidence collection behavior of public authorities. First, the subject must be legal. According to Sun Mingze's research [4], the search and mirroring of criminal electronic data can only be carried out by investigators with cybersecurity qualifications; auxiliary personnel can only provide technical assistance and cannot independently conduct evidence collection. Second, the authority must be legal. Zhang Xin [1] pointed out that electronic data searches are invasive investigative measures, and internal approval procedures must be followed for searches of citizens' mobile phones and private cloud storage. Data obtained by cracking passwords or remotely accessing servers without approval is illegal evidence and should be excluded according to law. Third, preservation must be legal. After evidence collection, a mirror copy must be made simultaneously, and hash verification values must be recorded to prevent data contamination during transfer and storage. Liu Yanjun further added that the essence of legality review from the perspective of power control is to balance investigative efficiency with citizens' data privacy rights, prohibiting the excessive collection of irrelevant data under the guise of investigation [3].

4.3. Authenticity Verification: The Final Judgment of Evidentiary Value

Authenticity is the biggest challenge in electronic data examination. Huang Youyong [2] divides it into formal authenticity and content authenticity. Formal authenticity examines the data generation environment, verifying whether

the evidence collection equipment system time and network environment are abnormal, and investigating external interference such as equipment infection, system time tampering, and account theft. Content authenticity distinguishes between original electronic data and derived electronic data. Original data in the original storage medium is presumed to be authentic, requiring supplementary verification only after the opposing party raises a reasonable objection; screenshots, forwarding records, and paper printouts are derived copies and cannot be used as the sole basis for a conviction, requiring corroboration with service provider backend logs and forensic identification. Zhao Changjiang, in his research on criminal evidence rules [6], emphasizes that the standards for accepting derived electronic data in criminal proceedings are stricter than in civil and administrative proceedings, and the possibility of reasonable tampering must be excluded.

5. Current Challenges and Improvement Paths in Electronic Data Examination

5.1. Existing Judicial Dilemmas

In the context of digital justice, electronic data has become a core type of evidence in the three major types of litigation. Unlike traditional physical evidence, electronic data is characterized by its virtual nature, ease of alteration, and reproducibility, placing higher demands on the compliance of its collection, preservation, and review procedures. Currently, my country's electronic data review rules are not adequately adapted to grassroots judicial practices, exhibiting prominent problems such as inconsistent review standards, flawed evidence collection procedures, and inconsistent judgments, severely hindering the effectiveness of electronic evidence. Therefore, systematically analyzing the difficulties in judicial review and constructing targeted improvement pathways is of great significance for standardizing the application of electronic data and unifying judicial decisions.

Secondly, procedural flaws in evidence collection are commonplace, and these legal flaws are difficult to rectify afterward. The evidentiary value of electronic data highly depends on standardized evidence collection and solidification processes, but at the grassroots level, there is a prevalent mindset of prioritizing substance over procedure in case handling. In practice, the reverse evidence collection model of collecting evidence first and then supplementing approval is very common, leading to an inherent lack of procedural legality due to the pre-existing requirement for evidence collection. At the same time, the core process of synchronously solidifying hash values is often overlooked. Evidence such as chat logs, transaction records, and platform data involved in the case is not solidified and verified in a timely manner when extracted, making it impossible to lock in the original state and rule out the possibility of tampering. Such flaws constitute substantive procedural violations that cannot be corrected or explained to restore legality, ultimately leading to the exclusion of key evidence. This not only wastes judicial resources but also easily results in the inability to pursue prosecution or hold anyone accountable.

Third, the disconnect between administrative and criminal review standards leads to conflicts in similar cases. China has not yet established unified rules for reviewing electronic data across the three major litigation systems, resulting in significant differences in review standards between administrative and criminal proceedings. Administrative litigation focuses on reviewing the legality of administrative actions, with a relatively lenient review of the authenticity and procedural compliance of electronic evidence; evidence without obvious signs of tampering is generally accepted. Criminal litigation, however, adheres to the principle of procedural justice, imposing strict review standards on the evidence collection process, data preservation process, and traceability records of electronic data. This disconnect in review standards means that the same electronic evidence may be accepted in administrative cases but excluded in criminal cases, creating inconsistent judgments for similar evidence and undermining judicial uniformity and public trust in the judiciary.

5.2. Targeted Improvement of the Path

In response to the aforementioned difficulties such as ambiguous definition of concepts, irregularities in evidence collection procedures, and fragmented judgment standards, and taking into account the special attributes of electronic data and the pain points in grassroots judicial practice, while balancing procedural justice and substantive justice, a comprehensive path is constructed from three levels: conceptual standardization, source regulation, and rule unification, to promote the standardization and unification of electronic data review and application.

First, it is crucial to unify the applicable boundaries of concepts and refine the rules for accepting archived electronic documents. A clear distinction must be made between the legal attributes of original electronic data and derived electronic documents: electronic data is firsthand data generated directly and unprocessed at the time of the case, possessing stronger authenticity and relevance; archived electronic documents, on the other hand, are derived data that has been manually organized, transformed, and migrated, and thus contain inherent flaws. Judicial authorities should clarify the boundaries between the two in case-handling regulations and judgments, prohibiting the direct acceptance of archived electronic documents as original electronic data. Simultaneously, specific acceptance conditions should be established, requiring the inclusion of accompanying data entry logs, transfer records, archiving approval and migration ledgers to fully prove that the data has not been tampered with throughout the process, forming a closed-loop chain of evidence before acceptance, thus preventing the misuse of concepts from the outset.

Secondly, implement pre-procedure regulations and construct a tiered evidence collection and approval system. Abandon the passive error-correction model of post-event rectification and strengthen source control of evidence collection. Drawing on Zhang Xin's tiered approval system [1], set differentiated evidence collection thresholds based on data attributes and levels of privacy. For publicly available data online, simplify the approval process while balancing efficiency and procedural legality; for private and confidential data such as personal records, financial statements, and core corporate data, strictly enforce tiered approval and legal document issuance procedures. Simultaneously, establish mandatory procedures for hash value synchronization and solidification, full audio and video recording, and retention of evidence collection records. Clearly define that evidence not solidified in compliance with regulations or without evidence collection records is inadmissible, forcing investigators to standardize evidence

collection procedures and eradicate procedural flaws.

Finally, a tiered presumption of authenticity rule is established to unify the three major litigation discretion standards. Based on the source and controllability of electronic data, a tiered review standard is constructed to resolve conflicts in litigation standards. First, original mirror data and native server backend data, with no room for human intervention or tampering, are directly presumed authentic, simplifying formal review. Second, transaction, login, and operation logs automatically retained by platforms and government systems, relying on the system's anti-tampering mechanism, allow for a more relaxed formal review, focusing on verifying the legality of evidence collection. Third, controllable evidence such as screenshots and screen recordings taken unilaterally by parties, with low tampering costs and questionable authenticity, cannot be directly presumed authentic; it requires reinforcement through backend tracing, in-court verification, and cross-comparison. This tiered rule unifies the three major litigation review discretion standards, eliminates differences in judgments across similar cases, and maintains the uniformity and fairness of judicial application.

6. Conclusion

Electronic data is core evidence in the digital age, and its value in objectively restoring facts, balancing the gap in evidence presentation, and reducing litigation costs makes it an important supplement to traditional evidence. However, due to its easily tamper-proof and traceless nature, it cannot be reviewed using the lenient logic of traditional evidence review. Judicial review must strictly adhere to the progressive standards of relevance, legality, and authenticity, clarify the legal differences between electronic data and electronic documents, and address procedural shortcomings based on existing evidence collection regulations. It is essential to leverage the evidentiary power of electronic data while safeguarding citizens' data privacy through legality review, achieving a balance between judicial fairness and the protection of digital rights.

References

[1] Zhang, X. (2024). A study on the legal regulation of electronic data search [Master's thesis]. Jilin University.

[2] Huang, Y. Y. (2023). A study on the authenticity of electronic data in administrative litigation [Master's thesis]. Zhongnan University of Economics and Law.

[3] Liu, Y. J. (2023). Research on electronic data investigation and evidence collection procedures from the perspective of power control [Master's thesis]. Southwest University of Political Science and Law.

[4] Sun, M. Z. (2022). A study on the procedural regulation of electronic data collection by investigative agencies [Master's thesis]. Southwest University of Political Science and Law.

[5] Peng, C. S. (2022). A comparative study on the legal regulation of electronic data and electronic documents. Archives Management, (04).

[6] Zhao, C. J. (2021). Research on the rules of evidence of electronic data in criminal cases [Master's thesis]. Southwest University of Political Science and Law.