Education and Social Work
ISSN Print: 3079-515X
ISSN Online: 3079-5168
https://doi.org/10.63313/ESW.9075

An Empirical Analysis and Systematic Reconstruction of the Exclusionary Rule for Illegal Electronic Evidence

Yangyang Liu
Anhui University of Finance and Economics, Bengbu 233030, China
Email: 851311512@qq.com

How to cite this paper: Liu, Y. Y. (2025). An Empirical Analysis and Systematic Reconstruction of the Exclusionary Rule for Illegal Electronic Evidence. Education and Social Work, 2(2), 42-51. ISSN Print: 3079-515X; ISSN Online: 3079-5168.
https://doi.org/10.63313/ESW.9075
Published: 2025-07-08

Abstract

China's exclusionary rules for illegal electronic evidence face dual challenges in the digital era: insufficient normative supply and operational dysfunction in practice. By integrating Liu Pinxin's "Derivation-Data-Acquisition" evidence system theory, Zhang Zetao's empirical findings on administrative procedures substituting for investigations, Wang Zhiyong's logic distinguishing evidence admissibility from probative value, Hou Dongliang's conceptualized exclusion criteria, He Yue's blockchain regulatory solutions, and Han Xu's quantitative judicial practice research, this study reveals that current rules fail to address the unique characteristics of electronic evidence. This results in only a 3% exclusion rate for illegal electronic evidence in judicial practice, accompanied by structural biases such as "prioritizing authenticity over legality," "circumventing criminal regulations through administrative procedures," and "replacing procedural review with technical authentication." The study proposes a threefold improvement approach: (1) establishing a specialized rule system of "illegality-non-remediability-unified exclusion" at the normative level; (2) creating a dual-axis review model of "rights infringement degree-technical compliance" at the standard level; and (3) enhancing the "judicial alliance chain" technology and evidence coordination mechanism between administrative and criminal procedures at the procedural level. This integrated research provides normative solutions for amending the Criminal Procedure Law that combine theoretical innovation with practical needs.

Keywords

Illegal electronic evidence; exclusionary rules; administrative-criminal evidence convergence; blockchain forensics; typological standards; evidentiary capacity

1. The Disconnect Between Norms and Practice: The Real Dilemma of Illegal Electronic Evidence Exclusion

1.1. Systematic deficiencies and ambiguous application in legislative

norms

Article 56 of China's Criminal Procedure Law limits the application of the exclusionary rule for illegal evidence to testimonial evidence and physical or documentary evidence. The exclusion of electronic data can only be indirectly addressed through the defect remediation rule in Article 27 of the Electronic Data Provisions, resulting in a normative gap characterized by "unclear legal text—fragmented judicial interpretations—technical departmental regulations." Liu Pinxin points out that this formalistic interpretive stance has led to the widespread academic view that "the exclusionary rule does not cover electronic data." However, internationally, a "convergence theory" consensus has emerged, advocating the unified exclusion of electronic and traditional evidence. While China's practice tacitly aligns with this trend, it lacks normative confirmation. Han Xu's empirical study of 125 judicial documents revealed that electronic data was excluded in only four cases, all based on "questionable authenticity" rather than "procedural violations," reflecting a formalistic tendency in rule application.

The deeper contradiction lies in the normative disregard for the "systemic" nature of electronic evidence. Liu Pinxin's "derivative-data-acquisition" system theory demonstrates that the admissibility review of electronic evidence must encompass the complete chain of "derivative evidence (expert opinions)—data corpus—acquisition records." However, current rules focus solely on formal defects in the data corpus, lacking systematic regulation over the legality of derivative evidence and the legitimacy of acquisition procedures. For example, in a case involving infringement of citizens' personal information, the investigative authority failed to seal the hard drive or include signatures for forensic submission. Although the court excluded the data, it did not simultaneously exclude the 520,000 pieces of information derived from it, violating the inherent requirement of "holistic exclusion for electronic evidence systems, including both trunk and branches".

1.2. Procedural Avoidance Mechanism for the Connection Between Administrative and Criminal Evidence

Through an investigation of 108 "two-law convergence" cases, Zhang Zetao found that 87% of cases involving electronic evidence exhibited the phenomenon of "substituting administrative procedures for criminal investigations." A typical example is extracting mobile phone data through detention and interrogation under the Police Law to circumvent the search warrant requirement stipulated in Article 138 of the Criminal Procedure Law. This procedural conversion creates three systemic loopholes:

First, administrative evidence collection permits "single-officer operations" and "post-hoc corrections," conflicting with the "dual-officer collection" and "procedural rigidity" requirements of criminal litigation.

Second, blockchain and other technical storage methods are used to conceal pre-chain procedural violations. For instance, in a fraud case, electronic data ex-

tracted without a proper record was admitted as evidence after blockchain storage, effectively replacing "procedural legality" scrutiny with "technical authenticity."

Third, the standards for converting administrative evidence are ambiguous. In a smuggling case, investigative authorities extracted server data under the guise of administrative seizure and later directly used it as criminal evidence, bypassing the exclusionary rule for illegally obtained physical evidence.

He Yue further revealed that the application of "judicial + consortium chain" technology exacerbates the concealment of procedural circumvention. When investigative authorities store evidence on private blockchain platforms, they selectively upload data "favorable for conviction" while omitting video records or operation logs exposing "procedural violations." As a result, courts can only examine the technical authenticity of "post-chain data" but cannot trace the legality of "pre-chain procedures." This "technical black box" effect shields 76% of administratively converted electronic data from legality reviews, creating what Hou Dongliang described as a paradoxical practice where "technically illegal electronic data is legitimized."

2. Theoretical Deconstruction: The Underlying Causes of the Failure to Exclude Illegal Electronic Evidence

2.1. Cognitive Bias and Systematic Deficiencies in the Theory of Evidential Attributes

Current evidence theory exhibits a structural imbalance in grasping the "technical-legal" dual attributes of electronic evidence. Liu Pinxin's proposed "derivative-data-acquisition" evidence system theory demonstrates that the examination of electronic evidence's admissibility should cover the complete chain of "derivative materials (expert opinions) - data corpus - acquisition records." However, existing rules merely treat it as a digital extension of traditional physical evidence, overlooking the unique characteristics of electronic data throughout its "generation-storage-transmission-extraction" lifecycle. For instance, in a case involving infringement of citizens' personal information, investigative authorities failed to seal the original hard drive medium and lacked inspection signatures. Although the court excluded the data corpus, it did not simultaneously exclude the expert opinions derived therefrom, violating the inherent requirement of "holistic exclusion of both primary and secondary evidence systems" for electronic evidence.

This theoretical cognitive bias has led to a judicial practice tendency of "emphasizing data content while neglecting acquisition procedures." As Wang Zhiyong pointed out, courts often misclassify admissibility issues such as "unqualified expert opinions" as "rectifiable defects," confusing the fundamental distinction between admissibility and probative value.

A deeper contradiction lies in the conflict between the "virtual nature" of electronic evidence and traditional evidence theory. Liu Pinxin emphasizes that the separable nature of electronic data's carrier and content makes its "ancillary information data"

(e.g., operation logs) and "associated trace data" (e.g., IP addresses) crucial for legality review. Yet, existing rules still adhere to the "static custody chain" theory for physical evidence. This resulted in a fraud case where WeChat chat screenshots were admitted based on "consistent hash values," while the procedural violation of failing to transfer the original medium was ignored. Such theoretical lag prevents the effective regulation of electronic evidence's distinctive "dynamic and tamper-prone" features under current frameworks.

2.2. Institutional Loopholes and Value Conflicts in the Coordination of Administrative and Criminal Procedures

China's "dualistic integration" model of administrative violations and criminal offenses has created systemic conditions for procedural circumvention. Zhang Zetao's empirical study of 108 "two-law convergence" cases revealed that 87% of cases involving electronic evidence exhibited "substitution of criminal investigation with administrative procedures." A typical example involves public security organs extracting mobile phone data through detention and interrogation under the Police Law, thereby circumventing the search warrant requirement under Article 138 of the Criminal Procedure Law. This institutional loophole in procedural conversion manifests in three aspects: First, administrative procedures permit "single-officer evidence collection" and "post-hoc rectification," fundamentally conflicting with the "dual-officer evidence collection" and "procedural rigidity" requirements of criminal litigation. Second, Article 51 of the Administrative Case Procedure Rules allows procedural defects to be rectified through "situation statements," effectively undermining the strict procedural controls of criminal litigation. Third, functional overlap between public security organs' public order and criminal investigation departments led to a telecom fraud case where investigative authorities obtained call records under the guise of administrative investigation and directly used them as criminal evidence, bypassing the exclusionary rule for illegal evidence.

The essence of this procedural disjunction lies in the value conflict between "efficiency priority" and "rights protection." He Yue's comparative law research highlights that foreign jurisdictions generally balance electronic evidence efficiency and rights protection through "judicial warrant doctrine," such as the dual-review mechanism for mobile data established in the U.S. Riley case. In contrast, China's Electronic Data Evidence Rules lack judicial review requirements for measures like "network remote inspection" and "online extraction," resulting in 82% of electronic evidence collections bypassing judicial approval. Zhang Zetao further exposes how unchecked discretionary power between administrative law enforcement and criminal investigation enables a "procedural circumvention" practice—exemplified by a smuggling case where investigative authorities first extracted server data under administrative seizure and later directly used it as criminal evidence, violating procedural justice principles in substance.

3. Systematic Reconstruction: The Path to Perfecting the Exclusionary Rule for Illegal Electronic Evidence

3.1. Legislative level: Establishing specialized exclusion rules for electronic evidence

Liu Pinxin proposed in "On the Exclusion of Illegal Electronic Evidence" that the exclusion of electronic evidence should follow a triaxial logic: the input axis of "investigative subject—procedure—formal illegality," the linkage axis of "irremediable defects," and the output axis of "holistic exclusion within the evidentiary system." Accordingly, Article 56 of the Criminal Procedure Law could be amended to include a dedicated provision: "Where the collection of electronic data violates statutory procedures, potentially severely compromising judicial fairness without possibility of rectification or reasonable explanation, such evidence shall be excluded; derivative products of electronic data (e.g., expert opinions, inspection records) whose authenticity is compromised due to procedural violations shall also be excluded."

This provision requires clarification in three dimensions:

1. Legalization of the Input Axis : Statutorily defining exclusion prerequisites—such as "unqualified investigative subjects (e.g., auxiliary police conducting solo evidence collection)," "procedural violations of technical standards (e.g., failure to use write-blocking devices)," and "formal defects (e.g., unsigned witness statements)"—distinguishing them from traditional physical evidence formality reviews.

2. Substantiation of the Linkage Axis : Aligning with Article 28 of the "Electronic Data Rules," explicitly categorizing scenarios like "unsealed original storage media" or "absence of synchronized audiovisual recordings"—which render authenticity unverifiable—as "irremediable" conditions, precluding corrective measures.

3.Systematization of the Output Axis :Incorporating the "derivative-data-collection" system theory to mandate synchronized review of electronic data, derivative expert opinions, and investigative records. For instance, in a case involving infringement of personal information, where unsealed hard drive data was excluded, the resulting 520,000-entry forensic analysis derived therefrom should likewise be excluded.

3.2. Standard level: Establishing a typological exclusion system

Absolute Exclusion Category: Evidence Collection Infringing on Constitutional Rights. Regulatory Basis: According to Article 40 of the Constitution, which protects freedom of communication, evidence obtained through remote network examination without a judicial warrant or by malicious software interception should be excluded, regardless of its authenticity. As Liu Pinxin noted, the U.S. has incorporated computer searches into the scope of inadmissible evidence under the Fourth Amendment, and China can adopt this constitutional exclusion logic, deeming electronic evidence collection that severely infringes on privacy and communication rights as illegal. Practical Example: In a case involving a casino operation, the inves-

tigative authorities obtained the suspect's mobile phone chat records by implanting a Trojan program without a technical investigation permit. This evidence should be absolutely excluded due to violating the procedural requirements of Article 150 of the Criminal Procedure Law.

Discretionary Exclusion Category: Serious Procedural Violations but Not Infringing on Basic Rights. Judgment Standard: Wang Zhiyong emphasized in "How to Prevent the Abuse of the Rule of Excluding Illegal Evidence in Criminal Trials" that it is necessary to distinguish between admissibility and probative value. For actions such as extracting electronic data without witness participation or a single police officer operating the evidence collection equipment, the court should comprehensively consider the degree of procedural violation and whether it affects the authenticity of the evidence. For example, in a pyramid scheme case, investigators extracted server data alone, but the blockchain certification proved the completeness of the operation process, allowing for discretionary correction.

Correction and Acceptance Category: Technical Defects' Procedural Remedies. Scope of Application: Limited to formal defects listed in Article 27 of the "Regulations on Electronic Data," such as "missing signatures on records" and "storage media not labeled with information," and corrections must not exceed the original evidence range. In the empirical study of Han Xu, regarding a fraud case, the WeChat chat record extraction record lacked the investigator's signature. However, after the synchronous audio and video recordings were supplemented, it became credible. Prohibitive provisions: For fundamental violations such as' the evidence collection entity lacks qualifications 'or' technical standards are not followed, 'it is forbidden to rectify these issues with' situation explanations.' For example, electronic data extraction led by auxiliary police officers cannot be legitimized through post-facto recognition.

3.3. Program level: Improving administrative-criminal coordination and technical regulation

(1) Rigid Control of Subject Qualification

Implementation Standard: Zhang Zetao's empirical research revealed that 87% of procedural circumvention cases involve administrative personnel leading evidence collection. Therefore, it must be clarified that administrative evidence collectors must possess criminal investigation qualifications, and auxiliary police or market regulatory personnel are prohibited from independently participating in electronic data extraction. In a certain smuggling case, customs officials independently extracted data from the involved server, resulting in the absolute exclusion of this evidence due to the illegitimacy of the subject.

Exception: For publicly available data legally collected by administrative agencies (e.g., business registration information), conversion can be made under Article 54 of the Criminal Procedure Law, but additional conditions such as "dual-witness pres-

ence" and "full-process audio-video recording" must be applied.

(2) Dual Review of Procedural Conversion

Prosecutorial Review: During the prosecution review stage, the prosecutorial authority must conduct a dual review of "legality + technicality" on administrative evidence collection procedures. As Han Xu noted, for chat records extracted during administrative investigations, in addition to reviewing the form of the extraction record, the technical department must be commissioned to verify the data integrity check value.

Retroactive Warrant Correction: For electronic data already extracted during administrative procedures, procedural defects can be corrected post-criminal case filing through a "retroactive warrant," provided the emergency circumstances stipulated in Article 15 of the Electronic Data Collection Rules are met.

4. Guidelines for the Application of Rules in Judicial Practice

4.1. Deconstruction of Judicial Logic in Typical Cases

1. Absolute Exclusion Case: Procedural Violation Infringing Fundamental Rights

In the case of "Qvod Company Distributing Obscene Materials for Profit," the investigative authority failed to prepare a seizure record when impounding the servers, and the transfer process lacked witness signatures. According to Liu Pinxin's "Systematic Exclusion" theory, the electronic data stored on these servers and the derived expert opinions should all be excluded. This is because the evidence collection process severely violated Article 12 of the "Electronic Data Forensics Rules," rendering the data source untraceable and constituting an "irremediable defect" scenario.

2. Discretionary Exclusion Case: Coexistence of Technical Flaws and Procedural Violations

In a telecommunications fraud case, the investigative authority extracted the suspect's mobile chat records using blockchain-based evidence preservation, but the preservation platform lacked national certification. The court, referencing He Yue's technical regulatory framework, ruled on one hand that the preservation technology's compliance was insufficient, while on the other hand, it verified that the extraction procedure complied with Article 9 of the "Electronic Data Provisions." Ultimately, the court exercised discretion to allow the admission of the evidence after the investigative authority supplemented the platform's certification credentials.

3. Remedial Admission Case: Procedural Remedy for Formal Defects

In a gambling operation case from Han Xu's empirical research, investigators extracting backend data from a gambling website failed to document the integrity check value in the record. The court, applying Article 27 of the "Electronic Data Provisions," required the investigative authority to supplement the hash value calculation records. After verification confirmed consistency with the original data, the court permitted remedial admission of the evidence.

4.2. Standard level: Establish a typological exclusion system

According to Zhang Zetao's correlation analysis between procedural violations and rights infringement, illegal electronic evidence is categorized as follows:

Absolute Exclusion Category: Evidence obtained through investigative actions that violate constitutional rights, such as remotely inspecting citizens' communication data without judicial warrants or extracting electronic evidence through torture. Such actions directly contravene Article 40 of the Constitution regarding the protection of communication freedom and must be excluded regardless of the evidence's authenticity.

Discretionary Exclusion Category: Situations involving severe procedural violations without infringing fundamental rights, such as extracting electronic data without witness participation or by unqualified personnel. Courts must comprehensively assess the "severity of the violation" and its "impact on judicial fairness." For example, in cases where investigators extract mobile phone data alone without violating privacy rights but breach the mandatory "two-person evidence collection" requirement without possibility of rectification, discretionary exclusion should apply.

Rectifiable Admission Category: Technical defects (e.g., missing signatures on records, unsealed storage media) that can be admitted after rectification or reasonable explanation. However, fundamental violations like "illegitimate evidence-collecting entities" cannot be rectified.

4.3. Program level: Improving administrative-criminal coordination and technical regulation

1.Standardizing the Legality Review of Administrative Evidence Conversion Implement Zhang Zetao's procedural control recommendations for the connection between administrative and criminal evidence, clarifying in judicial interpretations:

Substantive Requirements : Administrative evidence collectors must possess criminal investigation qualifications. Auxiliary police and administrative personnel are prohibited from independently participating in electronic data extraction, with evidence obtained in violation being absolutely excluded.

Procedural Requirements : During the administrative investigation phase, the extraction of electronic data must be accompanied by the creation of an extraction record compliant with the Electronic Data Extraction Rules

, detailing technical standards, witness information, etc. Evidence lacking critical elements cannot be converted into criminal evidence.

Review Requirements : During the review for prosecution, procuratorial organs must conduct a "secondary legality review" of the administrative evidence collection process. Electronic data obtained in violation of special laws such as the Data Security Law and the Personal Information Protection Law

must be excluded, even if it complies with administrative procedures.

2.Establishing a Dual Authentication Mechanism of "Technical Self-Verification +

Legal Verification" Incorporating He Yue's blockchain technology regulatory framework, the following should be implemented in judicial practice:

Pre-Chain Review : When investigative authorities extract electronic data, they must simultaneously record the evidence collection process on video. The hash value of the video must be stored on the blockchain along with the data itself. Evidence without video recording or missing video hash values shall not be admitted.

5. Conclusion: The Redefinition of Procedural Justice in the Digital Age

The reconstruction of exclusionary rules for illegal electronic evidence is, in essence, a redefinition of procedural justice in criminal litigation in the digital age. From Liu Pinxin's "integrated exclusion theory" revealing the systemic characteristics of electronic evidence, to Zhang Zetao's empirical research warning of risks in circumventing administrative procedures; from Wang Zhiyong's theoretical deconstruction clarifying the boundaries between evidentiary competence and probative value, to Hou Dongliang's typological standards providing a practical operational framework; from He Yue's technical regulatory approach balancing technology and the rule of law, to Han Xu's quantitative research exposing judicial practice deviations—six major academic works collectively point to one core proposition: only by deeply integrating the technical attributes of electronic evidence with the procedural values of criminal litigation can a modern evidentiary rule system be constructed that ensures both rights protection and governance efficacy. Future amendments to the Criminal Procedure Law should build upon this foundation, explicitly establishing the independent exclusionary status of electronic data in regulations, creating dual dimensions of rights and technology in standards, and improving the linkage control between administrative and criminal procedures—making the exclusionary rules for illegal electronic evidence both a "firewall" against unlawful evidence collection and a "guardian" of judicial fairness in the digital era. This represents not merely a technical upgrade of evidentiary rules, but a significant evolution of criminal rule-of-law civilization in the digital age.

References

[1] Liu Pinxin. On the Exclusion of Illegal Electronic Evidence [J]. Tsinghua Law Journal, 2025, 19(03): 74-88.

[2] Zhang Yunfeng. Research on the Application of Evidence Exclusion Rules in Criminal Defense [J]. Legal System Vision, 2025, (06): 88-90.

[3] Wang Runtian. The Application of the Exclusionary Rule for Illegal Electronic Evidence [J]. People's Procuratorial Semimonthly, 2023, (17): 75-76.

[4] Hou Dongliang, You Yi. On the Improvement Path of the Exclusionary Rule for Illegal Electronic Evidence [J]. Journal of Shenyang University of Technology (Social Science Edition), 2023, 16(05): 475-480.

[5] Zhang Zetao. On the Ineffectiveness of the Exclusionary Rule for Illegal Evidence in Criminal Procedure—A Perspective on Procedural Risks in the Connection Between Administrative and Criminal Evidence [J]. Tribune of Political Science and Law, 2019,

37(05): 67-80.

[6] Yang Jun. On the Evidential Attributes and Regulation of WeChat Information [J]. Journal of Huaibei Normal University (Philosophy and Social Sciences Edition), 2018, 39(01): 24-29.

[7] Wang Jinglong. Rectifying the Name of the "Exclusionary Rule for Illegal Evidence" [J]. Journal of Gansu University of Political Science and Law, 2017, (03): 43-61.

[8] Hu Ming, Wang Lin. Electronic Evidence Collection in Criminal Cases: Rules, Practices, and Improvements—An Empirical Analysis Based on Judicial Documents [J]. Journal of Political Science and Law, 2017, 34(01): 79-89.

[9] Chen Ruihua. A Theoretical Interpretation of the Exclusionary Rule for Illegal Evidence [J]. Evidence Science, 2010, 18(05): 552-568.

[10] Xi Wei: "Several Reflections on China's Electronic Evidence System," in Chinese Criminal Science, 2020, No. 6, p. 138.

[11] Min Chunlei: "An Analysis of the Scope of Application of the Exclusionary Rule for Illegal Evidence," in Journal of Law Application, 2015, No. 3, p. 11.

[12] Yang Yuguan, Guo Xu: "On the Scope of Illegal Evidence," in Lanzhou Academic Journal, 2015, No. 6, p. 157.