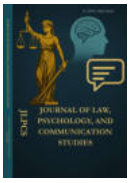
PANORAMA SCHOLARLY GROUP

Journal of Law, Psychology, and Communication Studies (JLPCS)



Research on the Legitimacy and Procedural Efficiency Challenges in Electronic Data Examination

Renyong Liu[a, *]

[a]*Sichuan Police College, LuZhou, 610000, China*

ARTICLE INFO

Keywords:
Electronic data
Judicial practice
Legitimacy
Procedural efficiency
Standardization

DOI: *https://doi.org/10.63802/jlpcs.V2.I1.81*

ABSTRACT

With the rapid advancement of information technology, electronic data has become increasingly integrated into all aspects of social life and judicial practice. As a new type of evidence, electronic data plays a crucial role in criminal, civil, and administrative proceedings. Yet, its application raises profound challenges concerning legality, procedural efficiency, and standardization. This paper explicitly situates itself within procedural law, evidentiary reform, and judicial governance, highlighting its dual contribution to theory and practice. Methodologically, it adopts literature review, comparative analysis, case studies, doctrinal research, and selected empirical data. The study identifies three core challenges: insufficient legal legitimacy of examination procedures, procedural inefficiency caused by technological and institutional fragmentation, and the absence of nationwide technical standards. Drawing on international experiences—particularly from the United States, the European Union, ASEAN, and selected Asian jurisdictions—the paper proposes a framework to enhance legality, efficiency, and cross-border cooperation. The findings enrich the discourse on procedural justice in the digital age and provide targeted recommendations for strengthening China's evidentiary system and smart court development.

1. Introduction

The rapid development of information technology has deeply transformed contemporary social life, with electronic data now permeating almost every domain—from personal communication, online payments, and commercial transactions to government administration and public governance. Against this backdrop, electronic data has gradually evolved into a critical source of evidence in judicial practice. In criminal proceedings, particularly in cases of cybercrime and telecommunication fraud, traditional physical and documentary evidence often fails to capture the full picture of criminal conduct. Only through the examination of chat logs, digital financial records, IP addresses, and emails can investigative authorities reconstruct the factual matrix of the crime (Casey, 2011; Wang, 2019). Similarly, in civil disputes involving electronic contracts, online transactions, and intellectual property infringement, electronic data frequently constitutes the decisive evidence determining case outcomes (Mason & Seng, 2017).

Despite its growing importance, the use of electronic data in judicial proceedings continues to face considerable challenges concerning legality, reliability, and procedural fairness. First,

* Corresponding author. e-mail: yun.pei.mnl@eac.edu.ph

electronic data is characterized by its replicability, susceptibility to tampering, and fragility, which cast doubts on its authenticity and integrity. Ensuring lawful collection and examination remains a fundamental concern (Liu, 2020). Second, tensions persist between judicial authorities and litigants during the examination process. While law enforcement agencies rely heavily on specialized technical departments, the qualification of examiners and compliance with statutory procedures are not uniformly guaranteed. Conversely, litigants often lack the technical capacity to challenge expert conclusions, placing them in a disadvantaged position during litigation (Zhang, 2021). Third, the globalization of data flows further complicates the issue, as much electronic data is stored on overseas servers. This creates jurisdictional and procedural obstacles for domestic courts in accessing and authenticating cross-border evidence (Goodison, Davis, & Jackson, 2015).

Furthermore, the procedural complexity of electronic data examination undermines judicial efficiency. Variations in examination tools and technical standards across regions lead to inconsistencies in outcomes, sometimes prolonging case adjudication and jeopardizing the predictability of judicial decisions. Such inefficiencies conflict with broader policy objectives in China aimed at optimizing the business environment and enhancing judicial efficiency (Chen, 2022).

Therefore, a systematic inquiry into the legality and normalization of electronic data examination is not only of theoretical significance but also of practical necessity. From the perspective of procedural law, this research clarifies the evidentiary positioning of electronic data; from the perspective of evidentiary reform, it proposes pathways for standardization and legitimacy; and from the perspective of judicial governance, it explores institutional innovations that reconcile efficiency with fairness. Practically, the establishment of standardized procedures for the collection, preservation, examination, and admissibility of electronic data can simultaneously enhance judicial fairness, reduce examination delays, and safeguard the procedural rights of litigants (Zhou, 2020). Ultimately, such reforms are essential to reconciling the goals of fairness and efficiency within judicial practice.

2. Research Overview

2.1. Current status of international research

2.1.1. The United States: Integration of Statutory and Case Law

The United States, as one of the earliest jurisdictions confronted with large-scale cybercrime, has accumulated extensive experience in the regulation and examination of electronic data. Its approach is characterized by a combination of statutory provisions and case law development.

First, U.S. federal law has explicitly recognized the evidentiary status of electronic data since the late twentieth century. The Federal Rules of Evidence (FRE), particularly Rule 901, set forth requirements for the authentication of evidence and have been widely applied to electronic evidence (Federal Rules of Evidence, 2019). Over time, federal and state courts have refined these standards through numerous judicial decisions, gradually forming an interactive framework of "rules complemented by case law" (Kerr, 2005).

Second, U.S. practice emphasizes the procedural legality and verifiability of electronic evidence examination. Law enforcement agencies are required to ensure that each stage of data extraction, preservation, transmission, and examination is traceable. The doctrine of "chain of custody" obliges investigators to maintain detailed records, thereby minimizing risks of tampering and strengthening evidentiary reliability (Casey, 2011).

Third, the adversarial nature of U.S. proceedings guarantees the rights of litigants to challenge examination results. Parties and their attorneys may question the methodologies employed and even appoint independent technical experts to assist during trial. This adversarial design promotes transparency and enhances the credibility of digital forensics (Mason & Seng, 2017).

Finally, the U.S. judiciary has actively responded to emerging technological challenges such as cloud computing, social media data, big data analytics, and deepfake technologies. Judicial interpretations and professional guidelines—including the Department of Justice's Electronic Evidence Guide and the Federal Rules of Civil Procedure on e-discovery—offer practical mechanisms for the retrieval and examination of such data (Goodison, Davis, & Jackson, 2015).

2.1.2. The European Union: Emphasis on Unified Legislation and Cross-Border Cooperation

In contrast to the United States, the European Union (EU) must reconcile diverse national judicial systems among its member states. Consequently, the EU focuses on harmonized legislation and regional cooperation.

First, the EU has established a unified legal framework for electronic evidence. The proposed E-Evidence Regulation and instruments under the Budapest Convention on Cybercrime enable judicial authorities of member states to request data directly from service providers across borders, bypassing traditional mutual legal assistance procedures (European Commission, 2018). This framework enhances efficiency in handling transnational cases.

Second, the EU attaches great importance to the protection of fundamental rights. In line with the Charter of Fundamental Rights of the European Union, the General Data Protection Regulation (GDPR) imposes strict requirements on the collection, storage, and use of personal data. Balancing crime control with privacy protection is thus a distinctive feature of the EU's regulatory approach (Biasiotti, Cannataci, & Turchi, 2018).

Third, the EU promotes the unification of technical standards through institutions such as Eurojust and Europol. These bodies support the development of standardized methods for electronic data examination to facilitate mutual recognition and information-sharing across borders (Christakis, 2020).

2.1.3. Other Jurisdictions: Japan and South Korea

Beyond the United States and the EU, countries such as Japan and South Korea have also made significant progress in this field.

Japan has gradually incorporated provisions on electronic evidence into its Code of Criminal Procedure and relevant judicial interpretations. It emphasizes transparency in evidence collection and procedural safeguards for defendants (Shionoiri, 2019).

South Korea, meanwhile, has adopted a collaborative model in which police and prosecutorial authorities share responsibilities in electronic data examination. More recently, Korean authorities have explored the application of blockchain

technology to enhance the integrity of data preservation (Kim, 2021).

Overall, foreign jurisdictions generally stress the legality, procedural justice, and technical reliability of electronic data examination. Through a combination of legislation, case law, and institutional cooperation, they have developed relatively mature frameworks. These experiences provide valuable references for China in refining its own system of electronic data examination.

2.2. Current status of Chinese research

Compared with foreign jurisdictions, China started relatively late in building its system of electronic evidence examination. Nevertheless, significant progress has been made, particularly since the 2012 amendment of the Criminal Procedure Law which explicitly recognized electronic data as a statutory form of evidence (NPC, 2012). Scholarly attention and judicial practice have increasingly focused on the legitimacy, technical feasibility, and procedural safeguards of electronic data examination.

2.2.1. Institutional Developments

China's Criminal Procedure Law (Articles 48 and 63) defines electronic data as an independent category of evidence. In response, the Supreme People's Court (SPC), the Supreme People's Procuratorate (SPP), and the Ministry of Public Security (MPS) have issued several judicial interpretations and departmental regulations. These documents set forth general requirements for the collection, preservation, and review of electronic data (SPC, SPP & MPS, 2016).

However, institutional shortcomings remain evident:

Lack of unified standards – Different regions and forensic institutions often adopt divergent methods of examination and reporting formats, undermining the authority and comparability of results (Zhou, 2020).

Unclear examiner qualifications – While specialized departments exist within police and prosecutorial organs, certification and supervision of third-party forensic institutions remain insufficient. Consequently, courts sometimes hesitate to recognize their conclusions as authoritative (Liu, 2020).

Low procedural transparency – Defendants and litigants face limited opportunities to participate in or challenge examination processes, weakening the adversarial balance of litigation (Zhang, 2021).

2.2.2. Academic Research

Chinese scholars have concentrated their research on three major areas:

Legitimacy of procedures – Many legal scholars emphasize that electronic data must satisfy the "three elements" of evidence law—legality, authenticity, and relevance. Research indicates that unlawful collection or examination procedures will severely undermine admissibility (Chen, 2022).

Technical approaches – Collaboration between legal scholars and information technology experts has produced proposals to enhance the integrity of electronic data. Suggested methods include the adoption of blockchain-based preservation systems and reliable timestamp mechanisms to ensure data immutability (Huang & Li, 2019).

Procedural safeguards – Scholars highlight the necessity of strengthening litigants' participatory rights, particularly through the use of technical experts or "expert assistants" in trial proceedings. These measures are seen as essential for ensuring transparency and adversarial balance (Wang, 2019).

2.3. Practical Challenges

Despite legal recognition and academic advancement, several practical obstacles persist in China's judicial practice:

Insufficient technical capacity – Many grassroots judicial organs lack advanced equipment and qualified personnel, resulting in heavy reliance on higher-level authorities or external institutions (Sun, 2020).

Cross-border evidence barriers – Given that much data is stored on foreign servers, Chinese courts must rely on complex and often ineffective international judicial assistance mechanisms. This significantly delays evidence collection (Liu, 2020).

Lagging legal frameworks – With the emergence of new technologies such as deepfake videos and AI-generated content, existing legal provisions are inadequate to address authenticity and admissibility concerns (Chen, 2022).

In sum, while China has made notable progress in the institutionalization of electronic data examination, it continues to face substantial gaps in standardization, transparency, and technical capacity. Bridging these gaps will require drawing on international experiences while tailoring reforms to China's specific judicial and technological context.

3. Research Methodology

To analyze the legality, efficiency, and standardization of electronic data examination in judicial practice, this study adopts a multi-method approach. The use of complementary methods ensures that the conclusions are both theoretically grounded and practically relevant.

3.1. Literature Review

The literature review method serves as the foundation of this research. By systematically collecting and examining domestic and international studies on electronic evidence and digital forensics, the study identifies theoretical debates, research trajectories, and unresolved issues (Casey, 2011; Mason & Seng, 2017). This process clarifies the research background and highlights the necessity of addressing gaps in China's existing framework. Through the literature review, this paper situates the discussion within broader scholarly discourse and establishes a basis for comparative and normative analysis.

3.2. Comparative Analysis

Given the highly technical and transnational nature of electronic data, comparative analysis is essential for evaluating different institutional responses. The study contrasts China's current system with established practices in the United States, the European Union, Japan, and South Korea. Such comparisons reveal both deficiencies in China's regulatory framework and potential lessons that can be selectively adapted to the domestic context (Kerr, 2005; Christakis, 2020).

3.3. Case Study Method

Case analysis enables the study to explore how theoretical and legal issues manifest in practice. As electronic data increasingly appears in high-profile cases—ranging from telecommunication fraud and financial crimes to intellectual

property disputes—the examination of actual judgments and enforcement practices highlights recurring challenges. By analyzing representative cases, this research demonstrates how electronic data examination influences judicial outcomes, thereby providing empirical support for theoretical arguments (Goodison, Davis, & Jackson, 2015).

3.4. Doctrinal (Normative) Analysis

Doctrinal analysis, a core method in legal research, examines the consistency and rationality of relevant legal provisions. This study analyzes statutory provisions such as the Criminal Procedure Law and judicial interpretations by the SPC, SPP, and MPS to assess whether current norms adequately regulate the examination of electronic data (SPC, SPP & MPS, 2016). This method highlights gaps in China's legal framework and forms the basis for proposing reforms.

3.5. Empirical Approach

Where available, this study draws upon empirical data from judicial reports, law enforcement statistics, and academic surveys to assess the actual implementation of electronic data examination. Empirical evidence provides an objective measure of issues such as delays in examination, inconsistencies in forensic conclusions, and resource disparities between regions (Sun, 2020; Zhou, 2020).

4. Results and Discussion

4.1. Theoretical Foundations of Electronic Data Examination

4.1.1. Concept and Characteristics of Electronic Data Examination

(a) Concept: In the era of digitalization and networking, electronic data has become a crucial form of evidence widely applied in criminal, civil, and administrative proceedings. To verify its authenticity and legality, judicial practice has developed a specialized procedural activity—electronic data examination. Electronic data examination refers to the process whereby qualified forensic institutions or technical experts, in accordance with statutory procedures and technical standards, analyze the generation, storage, transmission, and content of electronic data in order to reach scientific conclusions that can be used as references in judicial decision-making (Mason & Seng, 2017).

The primary objective of electronic data examination is to confirm whether electronic data is genuine and complete, and whether it has been altered or damaged during its lifecycle. Unlike ordinary evidence collection, examination is essentially a procedural activity aimed at validating authenticity through scientific methods (Casey, 2011).

(b) Relationship with Digital Forensics and Data Authentication

Relation to evidence collection – Electronic evidence collection refers to the process of retrieving and preserving data. Its purpose is to safeguard the original state of evidence. Examination, however, occurs after collection and focuses on verifying authenticity. Thus, the two stages are sequential and complementary (Liu, 2020).

Relation to broader forensic identification – Data forensics may include broader tasks such as intellectual property verification or financial analysis. Electronic data examination represents a more specific application within judicial proceedings, emphasizing procedural legality and admissibility (Wang, 2019).

Interconnection – Together, evidence collection, forensic analysis, and examination form a chain of custody ensuring lawful origin, authenticity, and evidentiary weight of electronic data.

(c) Characteristics

Electronic data examination demonstrates four major features:

Technical dependence: It relies heavily on tools such as hash verification, metadata analysis, and log examination (Casey, 2011).

Legal framework: Despite technical reliance, the ultimate function is evidentiary; thus legality determines admissibility (SPC, SPP & MPS, 2016).

Procedural nature: Examination must follow statutory protocols, such as being conducted by qualified institutions and producing verifiable reports.

Disputability: Because electronic data is replicable and tamperable, conclusions are frequently challenged by litigants, requiring strong procedural safeguards (Zhang, 2021).

4.1.2. Evidentiary Status of Electronic Data

(a) Application of the Three Evidentiary Elements

Legality – Evidence must be lawfully collected by authorized bodies without violating privacy or communication rights. Examination must be conducted by certified experts under lawful procedures (Chen, 2022).

Objectivity – Data automatically generated by servers or platforms, such as logs or transaction records, reflects real activities. Yet fragility and susceptibility to tampering undermine objectivity, necessitating rigorous examination (Huang & Li, 2019).

Relevance – Electronic data must have a logical nexus with the disputed fact. Examination helps establish reliable causal connections.

(b) Statutory Recognition in Chinese Law

Article 56 of China's Criminal Procedure Law explicitly recognizes electronic data as an independent category of evidence. The Provisions on Several Issues Concerning the Collection, Extraction, Examination and Judgment of Electronic Data in Handling Criminal Cases (2016) further detail preservation of original media, duplication and verification, and procedural records (SPC, SPP & MPS, 2016).

However, in civil proceedings, despite recognition of electronic data as evidence, the lack of detailed procedural norms results in significant judicial discretion and inconsistency.

4.1.3. Theoretical Controversies

Despite legal recognition, theoretical disputes persist in both academia and practice.

(a) Authenticity Verification

Tamperability – Unlike physical evidence, digital data can be copied and altered with minimal traces (Casey, 2011).

Instability – Hardware failures, cyberattacks, and transmission errors undermine reliability.

Opaque tools – Proprietary forensic software may lack transparency, creating a "black-box" problem where judges and litigants must rely solely on experts (Zhou, 2020).

(b) Examiner Qualifications

Institutional disparities – Many forensic institutions differ in competence and lack uniform certification.

Personnel limitations – Examiners often possess technical expertise but insufficient legal training, leading to procedural errors (Sun, 2020).

Limited defense participation – Current rules inadequately guarantee the right of litigants to appoint independent experts or request re-examination (Zhang, 2021).

(c) Procedural Deficiencies

Procedural flaws, even where conclusions appear accurate, may result in exclusion of evidence:

Absence of complete chain-of-custody records.

Lack of independent supervision during examination.

Insufficiently detailed reports, failing to explain methodologies and limitations (Chen, 2022).

4.2. Legitimacy Issues in Judicial Practice of Electronic Data Examination

Electronic data has been formally recognized as an evidentiary category in China's legal framework. However, its use in judicial practice continues to face significant legitimacy challenges. The legitimacy of electronic data examination is critical because it determines whether such evidence can be admitted into proceedings and whether it carries sufficient probative value. Current debates in China focus on three major aspects: the legitimacy of examining bodies, the legality of examination procedures, and the admissibility of examination results.

4.2.1. Legitimacy of Examining Bodies

(a) Public Security Organs

In criminal cases, electronic data examination is often conducted by the technical departments of public security organs. While this ensures efficiency and reduces costs, it raises concerns regarding neutrality and independence.

Dual role dilemma: Public security organs function both as investigators and examiners, creating risks of bias and undermining the objectivity of conclusions (Zhang, 2021).

Lack of external oversight: Defense lawyers and litigants rarely have opportunities to observe or challenge examinations conducted internally, thereby limiting transparency (Chen, 2022).

(b) Procuratorates

As supervisory organs, procuratorates occasionally conduct independent examinations to review evidence obtained by police. Although this may counterbalance investigative bias, procuratorates themselves act as prosecutorial authorities, which complicates their claim to neutrality. Moreover, their technical capacity and resources remain limited compared to public security organs (Wang, 2019).

(c) Third-Party Forensic Institutions

Independent forensic and technical institutions can, in principle, enhance neutrality. Their advantages lie in independence and professional specialization. However, in practice:

Certification systems for third-party institutions are inconsistent, and courts often doubt the authority of their reports (Liu, 2020).

Regional disparities mean such institutions are concentrated in metropolitan areas, while rural regions remain underserved (Sun, 2020).

High costs and long processing times reduce accessibility and efficiency (Zhou, 2020).

(d) Coordination Challenges

The coexistence of multiple examining bodies generates conflicts of authority: public security organs possess resources but lack neutrality; procuratorates have supervisory roles but remain part of the prosecution; third-party institutions are neutral but lack credibility. Establishing clear divisions of responsibility and mutual checks is necessary to ensure legitimacy.

4.2.2. Legality of Examination Procedures

The procedural dimension of electronic data examination is decisive for its admissibility. Any procedural flaw may lead to exclusion, regardless of the substantive accuracy of conclusions.

(a) Data Extraction

Law requires the preservation of original storage media or creation of verified duplicates (SPC, SPP & MPS, 2016). Yet in practice:

Screenshots or printouts are sometimes admitted without underlying databases, breaking the evidentiary chain.

Failure to conduct audiovisual recording during extraction undermines verifiability.

Use of commercial software with undisclosed algorithms reduces transparency (Casey, 2011).

(b) Data Preservation

Preservation must ensure integrity and prevent tampering. Problems include:

Incomplete sealing and recordkeeping of storage devices.

Lack of encryption during storage or transmission.

Limited participation of litigants, resulting in low transparency (Zhou, 2020).

(c) Data Transmission

In cross-regional or transnational cases, data transmission presents risks. Without proper hash verification or encryption, courts struggle to confirm consistency between transmitted and original data (Goodison, Davis, & Jackson, 2015).

(d) Examination Process

Procedural flaws during examination include:

Methods inconsistent with national or industry standards.

Reports lacking detailed explanations of methodologies.

Courts often deny requests for re-examination on efficiency grounds, undermining defense rights (Chen, 2022).

4.2.3. Legitimacy of Admissibility and Judicial Review

The ultimate purpose of examination is to provide admissible evidence. Courts face persistent challenges in evaluating examination reports.

(a) Judicial Review Standards

Courts in China generally assess reports based on:

Legitimacy of the body (whether qualified institutions conducted the examination).

Procedural legality (whether collection and preservation followed statutory requirements).

Scientific reliability (whether technical methods are verifiable and replicable).

Reasonableness of conclusions (whether findings logically relate to case facts).

Failure to meet these criteria often leads to reduced probative weight or exclusion.

(b) Boundary Between Technical and Legal Judgment

Courts sometimes overly rely on technical conclusions, risking the substitution of judicial judgment with expert opinion (Mason & Seng, 2017).

Judges often lack technical literacy to critically assess methodologies, leading to uncritical acceptance.

Divergent conclusions from different institutions create uncertainty in judicial determinations (Liu, 2020).

(c) Lack of Unified Standards

The absence of nationwide standards for admissibility leads to inconsistencies across courts and regions. Potential reforms include:

Developing unified examination protocols and report templates.

Strengthening adversarial procedures to allow cross-examination of experts.

Establishing independent technical advisory teams to assist judges (Christakis, 2020).

4.3. Dilemmas of Procedural Efficiency in Electronic Data Examination

While legitimacy remains a core concern in the examination of electronic data, efficiency poses equally significant challenges in judicial practice. Procedural efficiency, in this context, refers to the ability of electronic data to be admitted into proceedings within a reasonable cost, timeframe, and degree of accessibility. However, technological barriers, limited judicial resources, and the increasing diversity of case types often undermine efficiency. These inefficiencies not only delay trials but also increase judicial costs and potentially compromise the fairness of adjudication.

4.3.1. Technical Complexity

(a) Limitations of Hardware and Technical Conditions

Electronic data examination relies heavily on advanced forensic equipment, such as data acquisition devices, forensic workstations, write-blockers, and mobile device unlocking tools. However, these devices are expensive and require constant upgrading. Many grassroots judicial organs struggle to maintain sufficient hardware capacity (Liu, 2020).

For example, in a theft case handled by a county-level court, investigators were unable to extract data from a suspect's smartphone due to the absence of decryption equipment. Instead, they relied on screenshots, which the court ultimately dismissed for lack of originality and completeness. Such cases demonstrate how insufficient hardware directly reduces efficiency (Sun, 2020).

(b) Software Compatibility and Updates

Electronic data often comes from diverse platforms—social media, email servers, encrypted communication tools, or cloud storage. Each platform has unique formats and encryption systems, requiring specialized software. Frequent software updates and encryption upgrades further exacerbate incompatibility, rendering existing forensic tools obsolete.

The Qvod (KuaiBo) case, for instance, involved multiple storage formats and encryption mechanisms, requiring months of technical effort to decode and verify data. This prolonged the adjudication process and illustrates how software incompatibility creates serious efficiency bottlenecks (Chen, 2022).

(c) Cross-Platform and Cross-Border Obstacles

In cybercrime and transnational cases, relevant data is often stored on servers across multiple jurisdictions. Extracting such data requires both technical expertise and international cooperation.

In an online gambling case, most transaction data was hosted on overseas servers. Chinese investigators could only obtain partial chat logs, while the core transaction databases remained inaccessible due to jurisdictional barriers. Consequently, courts relied on incomplete evidence, resulting in partial convictions (Zhou, 2020). This highlights how cross-border barriers undermine both efficiency and completeness.

4.3.2. Insufficient Judicial Resources

(a) Lack of Specialized Personnel

Electronic data examination requires professionals who are proficient in both technology and law. However, such interdisciplinary experts remain scarce. In many regions, ordinary police officers or clerks with limited training must conduct examinations, leading to inefficiencies and quality concerns (Wang, 2019).

In a contract fraud case, for example, email communications were presented as evidence. Due to limited expertise, examiners only provided screenshots without tracing server codes or transmission paths. The defense successfully challenged the evidence as potentially forged, weakening the prosecution's case (Zhang, 2021).

(b) Lengthy Examination Cycles

The process of data extraction, preservation, verification, analysis, and reporting is time-consuming. In large-scale cases involving terabytes of data, examination may take months or even years. According to the Supreme People's Court's 2022 Annual Report, the average forensic cycle for electronic data cases nationwide reached 3.5 months, while complex cases such as large-scale financial fraud required more than one year. Data from Beijing Internet Court further shows that approximately 42% of cases were delayed due to difficulties in obtaining or authenticating electronic evidence (Liu & Zhang, 2023).

The Ezubao financial fraud case is illustrative: more than 900,000 investors and massive volumes of transaction data

required forensic examination, which lasted over a year. This not only delayed the trial but also monopolized scarce forensic resources, leaving other cases pending (Goodison, Davis, & Jackson, 2015).

(c) Lack of Unified Standards

Different regions and institutions often adopt varying technical standards and reporting formats, resulting in inconsistent conclusions. In one personal information infringement case, two different jurisdictions reached conflicting findings on the same dataset due to divergent methodologies. Ultimately, the case was remanded, significantly prolonging litigation (Liu, 2020).

4.3.3. Challenges from Diverse Case Types

(a) Telecommunication Fraud

Telecommunication fraud often involves dispersed data such as instant messaging logs, virtual payments, and anonymous accounts. The use of anonymization and encryption technologies complicates data retrieval. In a "pig-butchering" scam case, only partial records could be obtained, leading to limited convictions despite large financial losses (Chen, 2022).

(b) Financial Crimes

Financial crime cases involve complex transaction chains embedded in banking and payment systems. Examining such data requires advanced analytical tools. In one securities manipulation case, examiners analyzed tens of millions of records over several months, significantly delaying adjudication (Zhou, 2020).

(c) Intellectual Property and Civil Disputes

In civil cases involving copyright infringement or electronic contracts, courts face additional challenges. For example, in Youku v. Baidu Netdisk, the plaintiff alleged storage of infringing video files. Given the volume of user data and privacy concerns, courts could only partially admit data, failing to capture the full extent of infringement (Huang & Li, 2019).

5. Normative Pathways for Standardizing Electronic Data Examination

The challenges of legality and efficiency identified in previous chapters demonstrate the urgent need for a standardized framework to govern electronic data examination in judicial practice. Standardization not only enhances evidentiary legitimacy but also reconciles fairness with efficiency, thereby strengthening the credibility of judicial decisions in the digital era. Drawing on international experiences while considering China's institutional realities, this chapter proposes five normative pathways: institutionalizing examining bodies, unifying procedural rules, establishing technical standards, strengthening rights protection, and developing cross-border cooperation mechanisms.

5.1. Institutionalizing Examining Bodies

First, it is essential to establish a clear division of responsibilities among public security organs, procuratorates, and third-party forensic institutions.

Public security organs should primarily undertake preliminary examinations due to their resources and technical capacity.

Procuratorates should perform a supervisory role to review the legality of examinations.

Independent forensic institutions should be empowered to provide neutral and authoritative opinions, especially in cases of dispute.

To ensure authority, a national certification system for third-party institutions should be introduced, similar to accreditation mechanisms in the U.S. and EU (Mason & Seng, 2017). This would enhance credibility while promoting checks and balances between investigative and supervisory bodies (Zhang, 2021).

5.2. Unifying Procedural Rules

Second, procedural rules governing extraction, preservation, transmission, and examination must be unified nationwide. Current inconsistencies undermine both fairness and efficiency.

The Provisions on Electronic Data in Criminal Cases (2016) provide a partial framework, but similar standards should extend to civil and administrative litigation.

Standardized protocols for audiovisual recording, chain-of-custody documentation, and re-examination rights should be codified to reduce regional disparities (SPC, SPP & MPS, 2016).

Adopting unified rules would also facilitate judicial predictability, allowing litigants to anticipate how electronic data will be assessed across jurisdictions (Chen, 2022).

5.3. Establishing Technical Standards

Third, technical standards for examination must be clearly defined. This requires:

1. Standardized forensic methodologies—including hash verification, metadata analysis, and blockchain-based preservation mechanisms—to ensure consistency and replicability (Huang & Li, 2019).

2. Uniform report templates—mandating disclosure of methods, principles, and limitations—to increase transparency and enable effective cross-examination (Casey, 2011).

3. Regular updates to reflect technological developments, such as artificial intelligence and deepfake detection (Christakis, 2020).

A unified set of technical standards would strengthen the scientific reliability of examinations and reduce conflicts between expert opinions.

5.4. Strengthening Procedural Rights

Fourth, procedural rights of litigants must be enhanced to ensure adversarial balance.

Right to participate: Defendants and their lawyers should be allowed to observe examinations and raise objections during the process (Wang, 2019).

Right to appoint experts: Courts should facilitate the participation of independent technical experts or "expert assistants" to assist parties in cross-examination (Zhou, 2020).

Right to re-examination: Requests for re-examination should not be denied solely for efficiency reasons, particularly in cases where examinations directly determine liability (Liu, 2020).

By institutionalizing these rights, courts can ensure that examinations are not merely technical processes but also subject to adversarial scrutiny, reinforcing procedural justice (Chen, 2022).

5.5. Developing Cross-Border Cooperation Mechanisms

Finally, given the globalization of data flows, international cooperation is indispensable.

Treaty-based frameworks: China could strengthen engagement with the Budapest Convention on Cybercrime or develop bilateral treaties to facilitate direct requests to foreign service providers (European Commission, 2018).

Judicial diplomacy: Regional cooperation with ASEAN or neighboring jurisdictions could provide pragmatic solutions for data hosted in foreign servers (Goodison, Davis, & Jackson, 2015). At present, China's cooperation with ASEAN remains limited to police-level data sharing, with no judicial-level fast-track for electronic evidence. In practice, requests for cross-border data often take more than six months, in stark contrast to the EU's E-Evidence Regulation, which allows intra-EU requests to be fulfilled within 10–30 days. Establishing a "Belt and Road Judicial Data Exchange Platform" could significantly shorten collection time and improve mutual recognition of digital evidence (OECD, 2023).

Technical collaboration: Shared platforms for forensic tools and training could help bridge disparities in technical capacity. Moreover, joint development of AI-based forensic tools with ASEAN partners could enhance both efficiency and credibility of examinations.

Such mechanisms would reduce the delays and uncertainties currently plaguing cross-border data acquisition.

Author Contribution

Renyong Liu was solely responsible for the conception, design, research, and writing of this paper. The author conducted all literature reviews, case analyses, and comparative studies independently. No other individuals contributed to the intellectual content or drafting of the manuscript.

Compliance with Ethical Standards

This research does not involve human subjects, clinical trials, or personally identifiable data. All sources used are publicly available academic and legal materials. The study complies fully with academic ethical norms and does not require IRB approval.

Funding

This research received no specific grant from any funding agency in the public, commercial, or not-for-profit sectors.

Competing Interest declaration

The author declares no competing interests.

Acknowledgments

None

References

1. Biasiotti, M. A., Cannataci, J., & Turchi, F. (2018). Balancing privacy and security in the digital era: The European approach to electronic evidence. *Computer Law & Security Review, 34*(2), 289–302.
2. Casey, E. (2011). *Digital evidence and computer crime: Forensic science, computers, and the internet* (3rd ed.). Academic Press.
3. Chen, R. (2022). The procedural legitimacy of electronic evidence in China's judicial practice. *Peking University Law Journal, 34*(2), 145–163.
4. Christakis, T. (2020). Cross-border access to electronic evidence: The European Union's e-evidence proposal and its impact on fundamental rights. *Journal of Cyber Policy, 5*(1), 1–20.
5. European Commission. (2018). *Proposal for a regulation on European production and preservation orders for electronic evidence in criminal matters*. COM(2018) 225 final.
6. Federal Rules of Evidence. (2019). *Federal rules of evidence*. United States Courts.
7. Goodison, S. E., Davis, R. C., & Jackson, B. A. (2015). *Digital evidence and the U.S. criminal justice system: Identifying technology and other needs to more effectively acquire and utilize digital evidence*. RAND Corporation.
8. Huang, J., & Li, X. (2019). Blockchain-based preservation of electronic data: Legal feasibility and technical design. *Tsinghua Law Journal, 13*(4), 112–129.
9. Kim, S. (2021). Blockchain for digital evidence preservation: A South Korean perspective. *Asian Journal of Law and Society, 8*(1), 121–140.
10. Kerr, O. S. (2005). Searches and seizures in a digital world. *Harvard Law Review, 119*(2), 531–585.
11. Liu, H. (2020). Electronic evidence in China: Current practice and future directions. *Journal of East Asia and International Law, 13*(2), 423–444.
12. Liu, R., & Zhang, Y. (2023). Artificial intelligence and electronic evidence in China's judiciary. *Journal of Law and Technology, 15*(2), 45–63.
13. Mason, S., & Seng, D. (Eds.). (2017). *Electronic evidence* (4th ed.). Institute of Advanced Legal Studies, University of London.
14. NPC (National People's Congress). (2012). *Criminal Procedure Law of the People's Republic of China* (Amended 2012).
15. OECD. (2023). *Cross-border access to electronic evidence: Global challenges and policy options*. OECD Publishing.
16. Shionoiri, K. (2019). The development of electronic evidence in Japanese criminal procedure. *Keio Law Review, 96*(3), 55–72.
17. SPC, SPP, & MPS (Supreme People's Court, Supreme People's Procuratorate & Ministry of Public Security). (2016). *Provisions on several issues concerning the collection, extraction, examination and judgment of electronic data in handling criminal cases*.
18. Sun, Q. (2020). The shortage of forensic resources in Chinese courts: An empirical analysis. *China Legal Science, 38*(3), 211–229.
19. Wang, Y. (2019). The legitimacy dilemma of electronic data evidence and its judicial regulation. *China Criminal Law Review, 11*(2), 98–115.
20. Zhang, L. (2021). Procedural safeguards in electronic data examination: Challenges and reforms. *Journal of Comparative Law, 45*(1), 76–94.
21. Zhou, M. (2020). Procedural justice in digital evidence examination: Problems and countermeasures. *Peking University Law Review, 22*(4), 67–83