

Article

A Study on the Coordination of Electronic Evidence in Environmental Criminal Proceedings

Baihe Wang^{1,*}
¹ School of Law, Southwest Petroleum University, Chengdu, China

* Correspondence: Baihe Wang, School of Law, Southwest Petroleum University, Chengdu, China

Abstract: Against the backdrop of digital transformation in environmental crime governance, electronic evidence plays a pivotal role at the interface between administrative law enforcement and criminal justice. This paper examines the legal, technical, and practical challenges in transferring electronic evidence between administrative and criminal proceedings in environmental cases. Legal issues include discrepancies in admissibility standards, ambiguous definitions of evidence attributes, and the absence of cross-border collection rules. Technical challenges involve difficulties in authenticity verification, inconsistent forensic examination standards, and data-sharing barriers. Practical shortcomings such as passive administrative referrals and outdated review methods further compound these problems. To address these, the study proposes a "form-substance" two-tier evidence review model, a judicial recognition procedure for environmental monitoring data, and an interdepartmental blockchain-based evidence storage and sharing platform, shifting evidence coordination from reactive conversion to preventive collaboration. The mechanism requires three-dimensional synergy among legal rules, technological empowerment, and institutional innovation, transcending sectoral law boundaries to establish an inclusive and rigorous evidence transfer system. This approach drives environmental governance from reactive response to preventive governance, enhancing both governance effectiveness and judicial fairness.

Keywords: coordination between administrative and criminal environmental enforcement; electronic evidence; evidence coordination mechanism; conversion of administrative and criminal evidence

1. Introduction

1.1. Challenges in Environmental Crime Governance and the Importance of Coordination between Administrative and Criminal Proceedings

In recent years, environmental crimes in China have become increasingly frequent and sophisticated. In 2021, there were 132,800 cases of environmental violations in China, but only 1,868 cases involving suspected environmental crimes were transferred to criminal authorities, highlighting the prominent phenomenon of "substituting fines for criminal prosecution." Under traditional governance models, administrative and judicial authorities have been disconnected in the stages of evidence collection, transfer, and review, making it difficult to secure convictions in complex environmental crime cases due to poor evidence coordination. For example, in the 2019 "Case of Shandong Qingyuan Petrochemical Co., Ltd. Evading Regulatory Oversight by Tampering with Online Monitoring Data," although administrative authorities had preliminary evidence of data anomalies, they were unable to promptly refer the case for criminal investigation due to doubts about the data's legitimacy and the lack of rules for converting administrative evidence into criminal evidence. As a result, the company continued to discharge pollutants illegally for several months, causing severe environmental pollution. As a key link in bridging administrative oversight and criminal justice, the coordination between administrative and criminal proceedings centers on establishing an efficient evidence transfer mechanism. This ensures that electronic evidence obtained during administrative

Received: 17 April 2026

Revised: 10 June 2026

Accepted: 23 June 2026

Published: 30 June 2026



Copyright: © 2026 by the authors. Submitted for possible open access publication under the terms and conditions of the Creative Commons Attribution (CC BY) license (<https://creativecommons.org/licenses/by/4.0/>).

investigations can be effectively converted into the basis for determining guilt in criminal proceedings, thereby preventing delays in enforcement caused by duplicate evidence collection or disputes over the legality of evidence.

1.2. The Central Role of Electronic Evidence in Environmental Law Enforcement and Justice

Electronic evidence has become the "core evidence" in environmental cases. In cases involving environmental pollution, electronic evidence-such as online monitoring data, electronic transaction records, and production equipment operation logs from polluting enterprises-can precisely record the time of pollution occurrence, the types of pollutants, and the discharge volumes, providing crucial clues for establishing the facts of the crime. For example, in the "Case of Excessive Pollutant Discharge by a Dyeing and Printing Factory in Yangzhou, Jiangsu," real-time wastewater discharge data obtained by environmental protection authorities through an online monitoring system, combined with the enterprise's electronic production ledgers, clearly demonstrated the fact that the enterprise had been discharging pollutants in excess of standards for an extended period, serving as key evidence for conviction and sentencing in the criminal proceedings. With the widespread application of the Internet of Things (IoT) and big data technologies in the field of environmental monitoring, the volume and significance of electronic evidence will continue to grow; its authenticity, integrity, and legality are directly linked to the fair adjudication of environmental cases.

2. Current Status and Legal Basis for the Integration of Electronic Evidence in Environmental Administrative and Criminal Proceedings

2.1. Legal Framework and Institutional Foundation

2.1.1. Provisions on the Interface between Administrative Law and Criminal Law

Article 54, Paragraph 2 of China's Criminal Procedure Law established, for the first time at the legal level, the legal basis for the conversion of administrative evidence into criminal evidence. It permits evidence materials-such as electronic data, physical evidence, and documentary evidence-collected by administrative agencies during law enforcement to be directly admitted into criminal proceedings. However, this provision uses the catch-all phrase "and other evidence materials" without clearly defining the specific characteristics of electronic evidence, leading to ambiguous review standards in practice. In 2016, the "Two Highs and One Ministry" issued the "Provisions on Several Issues Concerning the Collection, Extraction, and Review of Electronic Data in Criminal Cases" (hereinafter referred to as the "Provisions on Electronic Data"), which further refined the rules for obtaining electronic evidence. These provisions require adherence to the principle of "priority of the original storage medium" and set forth specific regulations regarding the collection procedures and integrity verification of electronic data. Article 75 of the 2021 "Interpretation of the Supreme People's Court on the Application of the Criminal Procedure Law of the People's Republic of China" emphasizes that administrative electronic evidence must undergo a legality review to confirm that the collection procedures comply with administrative regulations before it can be used as the basis for a ruling. These provisions establish a basic framework for the integration of administrative and criminal evidence, but gaps in this integration still exist. For example, the discrepancy between the "preponderance of evidence" standard used in administrative proceedings and the "beyond a reasonable doubt" standard in criminal proceedings has led to a large amount of electronic evidence being excluded due to procedural defects.

2.1.2. Special Legislation in the Environmental Field

Compared to traditional types of evidence, the specialized and technical nature of electronic evidence in environmental crimes necessitates specific legislative support. Articles 17 and 42 of the Environmental Protection Law establish the legal foundation for the environmental monitoring system, granting the competent ecological and environmental authorities the right to collect monitoring data and clarifying

enterprises' obligation to truthfully report pollution discharge data, thereby providing a direct basis for the collection of electronic data (such as online monitoring data and pollution discharge records) in administrative law enforcement. Article 12 of the 2016 "Interpretation of the Supreme People's Court and the Supreme People's Procuratorate on Several Issues Concerning the Application of Law in Handling Criminal Cases of Environmental Pollution" (hereinafter referred to as the "Environmental Criminal Interpretation") explicitly stated for the first time that monitoring data collected by environmental protection authorities and their affiliated monitoring agencies during administrative law enforcement may be directly used as evidence in criminal proceedings. This broke through the limitations of traditional types of evidence and established the admissibility of environmental monitoring data as criminal evidence [1]. However, these special legislative provisions still contain ambiguities regarding transitional rules. For example, the "Environmental Protection Law" does not explicitly stipulate the legal status of data from third-party monitoring agencies, leading to doubts in practice regarding the evidentiary validity of self-monitoring data collected by enterprises. Although the "Interpretation on Environmental Criminal Cases" recognizes the evidentiary capacity of monitoring data, it does not specify detailed review standards; for instance, there are no concrete provisions regarding the compliance of automatic monitoring equipment installation or the integrity of the data transmission process, resulting in judicial rulings relying on the judge's discretion.

2.2. Practical Models for the Admissibility of Electronic Evidence

2.2.1. Conversion Pathways for Environmental Monitoring Data

In environmental law enforcement, the conversion of monitoring data primarily proceeds through a dual-track system of "administrative collection-judicial review." Administrative agencies obtain data through on-site sampling, real-time transmission from automated monitoring equipment, and testing by third-party institutions. If a case involves suspected criminal activity, the data is transferred to judicial authorities along with the case, and the latter review its admissibility and probative value. For example, in the "Shandong Qingyuan Petrochemical Excessive Discharge Case," pollution discharge data captured in real time by environmental protection authorities via online monitoring equipment—after undergoing hash value verification and comparison with on-site samples—was transferred to public security organs as core evidence and was ultimately deemed valid evidence in the criminal proceedings. According to Article 12 of the "Interpretation on Environmental Criminal Cases," such data does not require re-examination and may be used directly as criminal evidence, provided that certain requirements are met, including "lawful collection procedures, compliant equipment calibration, and traceable data sources."

In practice, the admissibility of monitoring data faces a two-fold review: first, a legality review in administrative proceedings—such as the qualifications of sampling personnel and equipment calibration records; second, a review of authenticity and relevance in criminal proceedings—such as whether the data fully reflects key facts like the duration of pollution and changes in concentration. For self-monitoring data provided by enterprises, judicial authorities typically require supplementary comparison reports from third-party institutions or supervisory records from administrative agencies to enhance its credibility.

2.2.2. Three Models of Electronic Evidence Collection Measures

China's amended Criminal Procedure Law of 2012 classified electronic data as a statutory category of evidence but did not establish specific rules for its collection, extraction, and review and assessment tailored to its unique characteristics. In 2016, the "Two Highs and One Ministry" issued the "Provisions on Several Issues Concerning the Collection, Extraction, and Review and Assessment of Electronic Data in Criminal Cases," and in 2018, the Ministry of Public Security issued the "Rules for the Collection of Electronic Data by Public Security Organs in Criminal Cases." These two normative documents are of great significance in regulating the collection, extraction, and review

and evaluation of electronic data by public security and judicial organs in criminal cases. Some of the review and evaluation rules from the "Provisions on Electronic Data" have been incorporated into judicial interpretations of the Criminal Procedure Law, and the documents also stipulate distinctive provisions, such as the three models for the investigation and collection of electronic data.

2.2.3. "Integrated Collection" Model

"Integrated collection" of electronic data refers to the simultaneous collection of electronic data and its original storage medium for the purpose of establishing the facts of a case in litigation. This model has clear advantages: it complies with the requirements of the original document or best evidence rule, helps ensure the authenticity and integrity of electronic data, and since it involves the collection of physical objects-allows for the application of traditional experience in collecting physical evidence, resulting in lower technical barriers and fewer specialized knowledge requirements. However, it also has drawbacks. In practice, investigators may easily exceed the limitations of the relevance rule; when collecting electronic data relevant to a case, they may inadvertently collect a large amount of irrelevant data, thereby expanding the scope of interference with or infringement of citizens' fundamental rights.

2.2.4. "Separate Extraction" Model

The "separate extraction" model for electronic data leverages the characteristics of data-namely, its replicability, low cost, and unlimited number of copies-to extract electronic data separately from its original storage medium (such as USB drives, hard drives, or optical discs) for use in establishing the facts of a case during litigation. This model aligns with the relevance rule for evidence, enabling the precise collection of data relevant to the case while avoiding excessive interference with citizens' rights. If the integrity and authenticity of the data are properly safeguarded, the extracted electronic data possesses the legal effect of a deemed original and also complies with the original document or best evidence rules. However, during the extraction and copying process, factors such as equipment malfunctions, technical defects, and intentional tampering can easily lead to data loss or incompleteness. Compared to traditional physical evidence, where authenticity is safeguarded through the creation of written records and video recordings to establish a "chain of custody," electronic data-due to its vast volume and susceptibility to modification-requires the use of specific technical measures to ensure the authenticity and integrity of the data during the collection process.

2.2.5. "Conversion Collection" Model

The "conversion collection" model collects electronic data through methods such as screen recording, screen capture, and printing, and is relatively common in judicial practice. This model does not collect the data or the original storage medium itself, but rather transfers the evidentiary information contained in the data to other media, such as electronic devices, storage media, paper, or photographs. It has a low technical barrier; ordinary individuals can perform the operation using a cell phone or computer, and it aligns with the relevance rule for evidence. However, this model conflicts with the best evidence rule, is prone to data incompleteness, makes it difficult to obtain ancillary data crucial for proving the authenticity of the evidence, and often leads to disputes over the classification of evidence types. When determining the type of evidence, the original form in which the evidence was generated should be the determining factor; for example, a screenshot of electronic data printed on paper should still be classified as electronic data, rather than documentary evidence.

The "Regulations on Electronic Data" clearly define the statutory order of priority for the three modes of evidence collection: "integrated collection" takes precedence; when that is not feasible, "separate extraction" is used; and only when the first two are impractical is "conversion collection" employed-thereby ensuring the authenticity and integrity of electronic data. However, in judicial practice, "conversion collection" (such as printing electronic data onto paper) is the most widely used method because it facilitates

submission, storage, and transfer. In light of this, when the Criminal Procedure Law is amended again, it is necessary to incorporate well-established investigative and evidentiary measures and review rules for electronic data.

3. Major Challenges in the Seamless Integration of Electronic Evidence Across Environmental and Criminal Proceedings

3.1. Challenges at the Legal Level

3.1.1. Inconsistent Standards for Admissibility of Administrative and Criminal Evidence

There are significant differences between administrative procedures and criminal proceedings regarding the standards for admitting evidence, and this discrepancy constitutes the core obstacle to the transfer of electronic evidence. In terms of legality review, the requirements of the two systems differ markedly. In criminal proceedings, the legality review of electronic evidence covers three aspects: "legality of the entity," "legality of the procedure," and "formal legality." "Legitimacy of the entity" requires that the entity collecting evidence must be an investigator or an authorized law enforcement officer. However, third-party monitoring agencies commonly found in administrative procedures-such as testing companies commissioned by enterprises-often lack the qualifications for criminal evidence collection, and the data they provide is therefore typically excluded outright. Regarding "procedural legitimacy," criminal proceedings stipulate that detailed written records must be prepared during the collection of electronic evidence, the entire process must be audio and video recorded, and key stages must be signed by witnesses; Administrative procedures, on the other hand, place greater emphasis on efficiency and often simplify the documentation process, resulting in the omission of critical details. For instance, electronic data collected by administrative agencies through non-coercive means-such as pollution discharge records voluntarily provided by a company-may be excluded by judicial authorities on the grounds of "procedural defects" because procedures required in criminal proceedings, such as "two-person enforcement" and "full-process video recording," were not followed. There are also differences in the standards for assessing relevance. In administrative proceedings, evidence need only preliminarily prove the existence of a violation; criminal proceedings, however, impose stricter requirements, demanding a complete chain of evidence that excludes reasonable doubt. For example, while an administrative agency may impose an administrative penalty based solely on data showing excessive emissions during a single time period, criminal proceedings require a closed chain of evidence formed by combining data from multiple sources-such as continuous monitoring data, operating logs of emission control equipment, and pollutant transmission pathways.

These differences result in a "secondary review" dilemma for a large volume of administrative evidence during its conversion. Even if the data itself is authentic, it may be rejected solely because the procedure does not meet the requirements of criminal proceedings, thereby creating a vicious cycle of "low transfer rates-even lower adoption rates." At the same time, "tiered" review standards require the supplementation of a large amount of derivative evidence during the conversion of administrative evidence. This not only increases judicial costs but may even lead to the loss of critical data due to the passage of time.

3.1.2. Ambiguity in Defining Types of Electronic Evidence

Article 50 of China's Criminal Procedure Law lists "electronic data" as an independent category of evidence, but its definition is merely summarized as "data stored, processed, and transmitted in digital form." It fails to clarify the criteria distinguishing it from traditional forms of evidence, such as audiovisual materials and documentary evidence, leading to two core issues in practice: disputes over the determination of attributes and confusion regarding classification.

First, the overlap between technical media and forms of proof leads to misclassification. For example, water quality data generated by environmental protection agencies through online monitoring systems is often classified as "documentary evidence"

by judicial authorities when submitted in the form of paper reports, overlooking the essential characteristics that its original medium is an electronic system and that the data generation relies on algorithmic calculations. This classification logic, which prioritizes "form over substance," obscures the core attributes of electronic data—namely, its "technological dependency" and "tamperability"—thereby marginalizing technical safeguards such as hash value verification and blockchain-based evidence preservation during judicial review. Second, there is a legislative gap regarding the legal status of new forms of electronic evidence. With the emergence of technologies such as blockchain-based evidence preservation, smart contract data, and AI-generated reports, the traditional framework for classifying evidence struggles to accommodate these new forms. For example, emissions data preserved via blockchain is stored in the form of code on a distributed ledger, combining the technical characteristics of "electronic data" with the content-verification function of "documentary evidence"; its admissibility as evidence depends on the judge's discretion. In a "certain cross-border carbon emissions trading data fraud case," the court of first instance classified blockchain-based evidence as "electronic data" and required an examination of the on-chain node consensus mechanism; the appellate court, however, classified it as "documentary evidence" and examined only its formal authenticity, leading to differing rulings in the same case. Theoretical disputes center on the divergence between the "medium-determinism" and "function-distinction" theories: the former holds that any information stored on an electronic medium constitutes electronic data, while the latter argues for classification based on the method of proof—if evidence relies on textual expression (such as electronic contracts), it should be classified as documentary evidence. This divergence often leads to the omission of reviews of ancillary information related to electronic data in judicial practice due to misclassification, thereby affecting the assessment of evidentiary completeness.

Furthermore, confusion regarding the classification of converted evidence has sparked disputes over its admissibility. When administrative agencies convert WeChat chat logs into screenshots or print out web page information, such "converted evidence" is often mistakenly classified as "audiovisual materials" or "documentary evidence," overlooking its original nature as electronic data.

3.1.3. Lack of Regulations on Reverse Transfer

Compared to the relatively well-established rules governing forward linkage (the conversion of administrative evidence into criminal evidence), reverse linkage (the conversion of criminal evidence into administrative evidence) suffers from significant legal gaps. This makes it difficult for electronic evidence generated in criminal proceedings to effectively inform administrative procedures, thereby weakening the ability to regulate legal liability across the entire chain. China's *Administrative Penalties Law* only contains a general provision in Article 27 regarding the "offset of fines and confiscated property" rule; it does not address core issues such as whether criminal electronic evidence can be directly used as administrative evidence, the conversion procedures, or the review standards. In practice, the system primarily relies on fragmented regulations issued by various departments, which fail to distinguish between evidence types, leading to three prominent problems:

First, the lack of a mechanism for mapping evidence types creates obstacles to conversion. "Electronic data" obtained in criminal proceedings is often forced to conform to traditional evidence categories in administrative proceedings due to incompatible classification systems. For example, an enterprise's encrypted wastewater discharge database extracted by public security organs during a criminal investigation is often erroneously classified as "audiovisual materials" or "documentary evidence" in administrative proceedings because the *Administrative Litigation Law* does not explicitly recognize the independent status of "electronic data." This results in the probative value of its associated technical information (such as hash value verification records and data extraction logs) being stripped away. Second, the inversion of legality review standards leads to a diminished evidentiary effect. Criminal proceedings apply a "strict exclusion"

standard when reviewing the legality of electronic evidence, but administrative procedures do not explicitly state whether the conclusions of criminal reviews can be directly accepted. If criminal evidence is partially excluded due to procedural defects (such as incomplete witness signatures), there is a lack of legal guidance on whether administrative agencies may independently admit the lawful portions of such evidence based on the "preponderance of evidence" standard. Third, gaps in procedures for evidence custody and transfer create a gap in accountability. Current regulations do not specify how the original storage media containing electronic evidence should be transferred to administrative agencies after the conclusion of criminal proceedings, nor whether technical verification reports must accompany such transfers. In some cases, due to requirements for archiving criminal case files, administrative agencies must undergo complex inter-departmental approval procedures to obtain electronic evidence; in some instances, physical damage to storage media or data overwriting has even rendered critical evidence unusable. The absence of a system for reverse integration essentially reflects a one-way mindset in the design of evidentiary rules across administrative and criminal procedures. As "high-quality evidentiary resources" formed under stricter standards of proof, the reasonable utilization of criminal evidence in administrative proceedings can not only improve law enforcement efficiency but also avoid the secondary burden on enterprises caused by duplicate evidence collection. However, the current legislative gap means that in practice, evidence transferred from criminal to administrative proceedings often faces the dilemma of "requalification." There is an urgent need to establish systematic rules covering evidence type matching, tiered recognition of legality, and the allocation of custody responsibilities.

3.2. Technical Challenges

3.2.1. Challenges in Ensuring the Authenticity of Electronic Evidence: Risks of Tampering and Loss

The digital nature of electronic evidence exposes it to the dual risks of "ease of tampering" and "difficulty in tracing origins," and there is a significant gap between the current application of technical safeguards and judicial requirements. Unlike the physical stability of traditional physical evidence, electronic data can be tampered with through technical means without leaving a trace, such as modifying backend data in pollution discharge ledgers or deleting critical log files. Even when hash verification technology is employed, operational loopholes such as "backdated verification values" and "improperly sealed storage media" still exist in practice—a certain chemical company concealed its long-term tampering of online monitoring data by forging hash verification records, a practice that was only exposed during a criminal investigation when a third-party technical agency recovered the original data. Furthermore, the widespread adoption of cloud computing and distributed storage technologies has led to evidence being scattered across multiple servers. If not promptly secured, such evidence is prone to loss due to data overwriting or physical server damage. For example, in "a certain cross-border pollution case," the implicated enterprise deleted emission data stored in the cloud; because cross-border evidence preservation procedures were not initiated in a timely manner, the critical data could not be recovered. The core contradiction in technical safeguards lies in the disconnect between the technical standards for "administrative collection" and "criminal review." In administrative proceedings, the collection of electronic evidence often relies on companies' self-inspections or rudimentary technical tools, lacking the "end-to-end audit trail" and "tamper-proof verification" required for criminal litigation. For example, environmental protection authorities used unencrypted devices to extract electronic data without simultaneously recording operation logs, resulting in judicial authorities being unable to verify the integrity of the data collection process; ultimately, the evidence was excluded on the grounds of "doubt regarding its authenticity." In theory, blockchain evidence preservation technology can ensure data integrity through distributed ledgers; however, in practice, due to insufficient technical investment by administrative agencies, only 12% of environmental enforcement cases utilize this

technology. Furthermore, since cross-departmental on-chain collaboration mechanisms have yet to be established, the evidentiary validity of such preservation is frequently called into question.

3.2.2. Inconsistent Standards for the Appraisal of Environmental Monitoring Data

The specialized and technical nature of environmental monitoring data makes establishing consistent assessment standards a significant challenge. Currently, multiple sets of technical specifications coexist in China's environmental monitoring sector: the "Regulations on Environmental Monitoring Quality Management" issued by the Ministry of Ecology and Environment emphasize the "five characteristics" of data collection (representativeness, accuracy, precision, completeness, and comparability), while the Ministry of Justice's "Technical Specifications for Judicial Appraisal of Environmental Damage" focus on pollutant composition analysis and the determination of causality; the two differ in sampling methods and data validation procedures. For example, in water quality monitoring, data results obtained through "rapid testing methods" (such as on-site measurements using portable devices) used in administrative procedures may differ from those derived from the "standard laboratory methods" required in criminal proceedings, leading to contradictions involving "dual determinations" of the same monitoring data in administrative and criminal proceedings.

The lack of uniform standards is also evident in the qualifications of forensic institutions and the format of reports. In administrative proceedings, monitoring data may be issued by third-party institutions with CMA certification, whereas criminal proceedings tend to rely on reports from judicial forensic institutions registered with judicial administrative departments, resulting in some monitoring reports that meet administrative standards being excluded due to insufficient qualifications [2]. Furthermore, differences in data recording requirements across various regulations—such as administrative reports emphasizing data results, while criminal forensic evaluations require the inclusion of original spectra and calibration records—result in the need to supplement evidence with a large volume of technical materials during the evidence conversion process. In some cases, the connection between evidence cannot be established due to the loss of original data [3].

The root cause of this divergence in standards lies in the value divide between an "administrative regulatory orientation" and a "judicial evidentiary orientation": administrative procedures prioritize efficiency and permit the use of expedient technical means to quickly secure evidence; criminal proceedings emphasize rigor and require that technical methods meet the admissibility standards for scientific evidence. Theoretical debates center on the "judicial transformative effect of technical specifications"—namely, whether administrative technical standards can serve directly as the basis for criminal forensic analysis. Some scholars advocate establishing a "two-tier certification mechanism," whereby administrative standards serve as preliminary evidence, and technical details undergo substantive review in criminal proceedings through the expert assistant system; however, in practice, judges—due to limitations in their technical understanding—often directly exclude monitoring data on the grounds of "inconsistent standards," leading to "difficulties in judicially admitting specialized technical evidence." [4]

3.2.3. Technical Barriers to Data-Sharing Platforms

The delayed development of cross-departmental data-sharing platforms has exacerbated the "technological silos" phenomenon in the integration of electronic evidence between environmental administrative and criminal enforcement. Currently, although departments such as environmental protection, public security, and the procuratorate have established information-sharing platforms for the "coordination between administrative and criminal justice" (such as the National Information Platform for the Coordination of Administrative Law Enforcement and Criminal Justice), the platforms' functions are limited to tracking case transfer processes. They provide insufficient support for core requirements such as real-time sharing of electronic evidence, technical

verification, and cross-system compatibility, which manifests primarily in three major technical obstacles

3.2.4. Heterogeneous Systems Make Data Mutual Recognition Difficult

Data storage formats, encryption standards, and metadata specifications vary across departments. For example, monitoring data from environmental protection departments follows the format specified in *HJ 493-2009 Technical Guidelines for Water Quality Sampling*, while the criminal investigation systems of public security organs require compliance with **GA/T 116-2013 Specifications for the Storage Format of Electronic Data in Forensic Science**. The two standards differ in terms of timestamp precision and data validation fields, resulting in the need for manual format conversion when transmitting electronic data across systems-or even automatic rejection by the judicial system due to missing fields. During the initial operation of a provincial "Coordination Between the Two Laws" platform, 60% of the transferred data was returned by public security authorities as "incomplete in form" because the environmental protection department had failed to include the "device calibration time" field in its monitoring data.

3.2.5. Technical Conflicts between Security Measures and Privacy Protection

Judicial authorities require security verifications-such as blockchain-based evidence preservation and digital signatures-when sharing electronic evidence, while administrative agencies, out of concern for data confidentiality, impose strict restrictions on the remote transmission of original storage media. For example, in a "pollution case at a certain chemical industrial park," environmental protection authorities, fearing the disclosure of corporate trade secrets, refused to grant the procuratorate access to the raw data interface of the online monitoring system, providing only anonymized summary reports. This prevented judicial authorities from reviewing the underlying logic of the data, forcing them to rely on secondary sampling and delaying the resolution of the case. This contradiction between "excessive security protection" and "effective evidence sharing" is, at its core, a technical tug-of-war between data sovereignty and judicial efficiency.

3.2.6. The Lack of Standardized Technical Specifications Creates a Disconnect

The current absence of a unified "Standard for the Exchange of Electronic Environmental Criminal Evidence Data" results in an "authentication vacuum" regarding the technical attributes of evidence (such as hash value verification methods and storage medium preservation standards) during cross-procedural transfers. Furthermore, portable monitoring devices widely used in grassroots law enforcement cannot directly integrate the electronic data they collect into criminal evidence management systems because their data interfaces are not included in the judicial certification system; this requires manual entry, which carries a risk of errors. The deeper impact of these technical barriers is also reflected in the safeguarding of the integrity of the chain of evidence and the efficiency of judicial review. Due to the lack of unified technical interoperability standards, inter-agency collaboration often faces issues such as "incompatible evidence formats" and "difficulty in tracing technical details." For example, server logs from a company obtained by public security authorities through remote forensic examination were challenged by the defense during court cross-examination on the grounds of "temporal logical inconsistencies" because they did not comply with the environmental protection department's "Time Synchronization Specifications for Monitoring Equipment," resulting in discrepancies between the data timestamps and the monitoring equipment's records. Such technical flaws may trigger a chain reaction of doubts regarding the authenticity of the entire chain of evidence and may even lead to the exclusion of key evidence.

Theoretically, these technical barriers to data sharing reflect a deep-seated contradiction between "digital governance" and "the legal standardization of evidence." The integration of administrative and criminal enforcement in environmental cases requires electronic evidence to be traceable, tamper-proof, and mutually recognized

across systems at the technical level; however, current laws do not provide clear guidance on the technical implementation pathways. For example, Article 142 of the Criminal Procedure Law requires that electronic data be "properly preserved," but fails to define the technical standards for "proper preservation," leading to disagreements between administrative and judicial authorities regarding the responsibility for evidence preservation. In a pollution case, the environmental protection department stored electronic data on a standard server without creating a mirror backup, resulting in data loss due to a server failure. Ultimately, criminal liability could not be pursued due to the "loss of evidence."

In practice, technical barriers have also given rise to the inefficient phenomenon of "secondary evidence generation." To meet the technical review requirements of criminal proceedings, administrative agencies often need to reprocess already-collected electronic data—such as commissioning third-party institutions to re-verify hash values or supplement metadata records. This not only increases law enforcement costs but may also introduce new risks of tampering during the processing. According to judicial statistics from a certain province, in environmental crime cases in 2023, supplementary investigations due to incompatible data formats accounted for 37% of cases, extending the average case processing time by 45%. In summary, the three major technical challenges—insufficient authenticity safeguards, fragmented forensic standards, and barriers to data sharing—are essentially the result of a mismatch between the characteristics of digital technology and traditional rules of evidence. Addressing these issues requires not only technological innovation but, more importantly, clear legal regulations governing specific technological applications, thereby creating a dual-drive model of technology empowerment and rule adaptation.

3.3. Obstacles at the Practical Level

3.3.1. Passive Evidence Transfer by Administrative Agencies and the Widespread Phenomenon of "Substituting Fines for Criminal Prosecution"

The reluctance of administrative agencies to transfer evidence is the key bottleneck hindering practical coordination. Influenced by factors such as local protectionism and performance evaluation mechanisms, environmental protection departments tend to "downgrade" cases involving suspected criminal offenses, resulting in a large volume of electronic evidence remaining stuck in administrative proceedings. The 2021 *Report on the Development of Environmental Justice in China* indicates that, among all environmental administrative penalty cases nationwide, only 4.7% were referred to the criminal justice system; furthermore, among the referred cases, as many as 35% were returned for supplementary investigation due to insufficient evidence.

A deeper examination of the root causes reveals irrationalities in the administrative performance evaluation system. Currently, in some regions, administrative performance evaluations place excessive emphasis on economic indicators and short-term benefits—such as case closure rates and the fulfillment of fine quotas—which places significant pressure on law enforcement officers. To protect departmental interests and individual performance metrics, some law enforcement officers, even when sufficient evidence of criminal activity is discovered, may opt for administrative penalties on the grounds of "insufficient evidence" out of concern that transferring a case to criminal prosecution will negatively impact their performance evaluations. This results in a large volume of electronic evidence remaining stuck in administrative proceedings. Local protectionism is also a significant factor. Under the current system, local administrative agencies are highly dependent on local governments for funding and personnel. In pursuit of short-term economic growth, some local governments adopt a protective stance toward polluting enterprises, interfere with the enforcement actions of environmental protection departments, and demand that enterprises suspected of criminal activity be "treated leniently." Under these circumstances, environmental protection departments find it difficult to perform their duties independently and impartially, and are unable to promptly and effectively refer suspected criminal cases to the criminal justice system.

Although the "Measures for the Coordination of Administrative Law Enforcement and Criminal Justice in Environmental Protection" stipulate the standards and procedures for case transfers, they lack binding enforcement mechanisms. Insufficient oversight and accountability for administrative agencies' case transfers have further exacerbated this problem. For example, the "criminal priority" principle has been distorted in practice to mean "waiting until criminal proceedings are concluded before imposing penalties," resulting in the loss of timeliness in administrative penalties and an inability to curb environmental violations in a timely manner. The phenomenon of "substituting administrative penalties for criminal prosecution" not only severely undermines the deterrent effect of the law and disrupts the chain of evidence in the coordination between administrative and criminal enforcement but also increases the difficulty of judicial review due to the untimely collection and improper storage of electronic evidence. Some enterprises take advantage of the time lag in administrative referrals to delete critical data from their servers, making it difficult for judicial authorities to reconstruct the full picture of the illegal acts.

3.3.2. "Paper-Based Review" of Electronic Evidence Weakens Its Evidentiary Value

In practice, the phenomenon of "paper-based review" of electronic evidence severely undermines its probative value and integrity. Judicial officials, often lacking specialized knowledge in reviewing electronic evidence, convert electronic data into paper form for review, thereby overlooking the dynamic nature and technical dependency of electronic evidence. In the "Case of a Certain Enterprise's Illegal Dumping of Hazardous Waste," electronic transport records submitted by the environmental protection authorities were printed as paper documents. The judge reviewed only the signatures and content of the paper documents, failing to examine metadata such as the original storage location and modification logs of the electronic data. As a result, the fact that the enterprise had tampered with the transport route went undetected, leading to a lenient sentence.

The root cause of this reliance on paper-based review lies in the conflict between "traditional evidence-based thinking" and the "characteristics of digital evidence." Traditional evidence review emphasizes the formal authenticity of written materials, whereas the authenticity of electronic evidence depends on technical verification and dynamic correlations. For example, a printed electronic contract cannot reflect the digital certificate verification process that occurred at the time of signing, and a screenshot of a web page cannot show the original path of link redirection. The absence of this critical information may lead to misjudgments regarding the relevance and authenticity of the evidence. Furthermore, the process of converting evidence to paper form is prone to operational errors—such as format conversion errors and data truncation—which further undermine the credibility of the evidence.

In theory, the "best evidence rule" for electronic evidence requires that the original storage medium or an electronic copy be provided as a priority. However, in practice, due to technical limitations (such as a lack of electronic evidence presentation equipment in some lower-level courts) and established review practices, paper-based review remains the dominant approach. This method of review not only fails to fully leverage the probative value of electronic evidence but may also lead to miscarriages of justice. For example, in a case involving environmental monitoring data, rounding errors in a paper report led to data discrepancies, causing the judge to make an erroneous ruling and affecting the fair adjudication of the case.

3.3.3. Lack of Oversight of Environmental Monitoring Agencies Casts Doubt on Data Credibility

Regulatory loopholes in environmental monitoring agencies pose a significant threat to the credibility of electronic evidence. Currently, China's environmental monitoring market features a "multi-entity, multi-tiered" structure, including agencies subordinate to government departments, third-party commercial organizations, and corporate self-monitoring departments; regulatory mechanisms struggle to cover all entities. The lack of oversight is also reflected in the inadequacy of mechanisms for tracing the quality of

monitoring data. Once a data dispute arises, it is difficult to identify the source of the problem (e.g., during sampling, analysis, or transmission), making it impossible to effectively hold parties accountable. In theory, as key evidence for determining environmental crimes, environmental monitoring data should be subject to a strict quality control system to ensure its scientific validity and reliability. However, in practice, the lack of oversight significantly undermines the evidentiary value of monitoring data, rendering it unable to meet the requirements of judicial proceedings.

In summary, practical obstacles-including the reluctance of administrative agencies to transfer evidence, the "paper-based review" of electronic evidence, and the lack of oversight over monitoring agencies-severely hinder the efficiency and quality of the integration of electronic evidence in environmental criminal proceedings. These issues not only reflect inadequate implementation of institutional measures but also highlight the disconnect between technology and the law in practical application; they urgently require resolution through institutional improvements, technological empowerment, and strengthened oversight.

4. Pathways to Improving the Integration of Electronic Evidence in Environmental Criminal Proceedings

4.1. Institutional Optimization: Clarifying Legal Rules

4.1.1. Unifying Evidence Admissibility Standards: Expanding the Scope of Application of Article 54 of the Criminal Procedure Law

To resolve the discrepancies between administrative and criminal evidentiary admission standards, Article 54, Paragraph 2 of the Criminal Procedure Law should be amended to clarify special admission rules for electronic evidence and expand the scope of "evidence materials, etc." This would directly incorporate electronic evidence collected in administrative proceedings in accordance with statutory technical specifications-such as monitoring data compliant with the "Regulations on Environmental Monitoring Quality Management"-into the criminal litigation evidence system, thereby reducing redundant reviews. At the same time, a "negative list" system should be established to explicitly exclude electronic evidence obtained illegally (such as internal corporate data stolen through hacking) or in serious violation of technical specifications (such as data obtained using uncalibrated monitoring equipment), thereby ensuring a balance between the legality and reliability of evidence. In terms of specific implementation, drawing on the "principle of data minimization" regarding data collection in the EU's General Data Protection Regulation (GDPR), administrative agencies are required to clearly inform the parties concerned of the purpose, scope, and method of use when collecting electronic evidence, thereby safeguarding their rights to be informed and to object, and extending procedural legitimacy to the administrative stage [5]. For environmental monitoring data, specialized admission rules should be established to specify technical standards-such as data sampling methods, transmission encryption standards, and retention periods-to ensure the consistency of data across administrative and criminal proceedings. In theory, unified admissibility standards help establish a "seamless" evidence conversion mechanism, reduce the exclusion of evidence due to differing standards, and improve the efficiency of litigation. In practice, however, a balance must be struck between administrative efficiency and judicial fairness to avoid compromising evidence quality through overly lenient standards. For example, while data from enterprises' self-monitoring may be admitted in criminal proceedings, it must be accompanied by third-party witnessing or technical verification reports to enhance its credibility.

4.1.2. Establishing a "Two-Stage Review" Model for Electronic Evidence: Formal Review + Substantive Review

To overcome the arbitrariness in the review of electronic evidence, a "two-stage review" model should be established, combining the strengths of formal and substantive reviews. During the formal review stage, the focus is on examining the legality of the electronic evidence's source, its formal integrity, and its technical relevance; this stage is

handled by the case filing division or a specialized technical review team. If the electronic evidence passes the formal review and proceeds to the substantive review stage, the collegiate bench will examine the authenticity of the data, the strength of its probative value, and its relevance to the core facts of the case, applying the "beyond a reasonable doubt" standard. In environmental crime cases, the formal review may require administrative agencies to submit electronic evidence accompanied by materials such as an extraction description of the original storage medium, hash value calculation records, and calibration certificates for data collection equipment, to ensure the clarity of the evidence's source and the legality of the procedures. During the substantive review, judges may utilize the expert assistant system to interpret the technical principles and analytical methods behind monitoring data, thereby enhancing the professionalism and scientific rigor of the review. The advantage of the "two-stage review" model lies in bringing the technical review forward, improving the efficiency of evidence screening, and avoiding the waste of judicial resources caused by a large volume of invalid evidence during the substantive review. At the same time, the participation of expert assistants in the substantive review enhances judges' understanding of and ability to evaluate complex technical evidence, thereby ensuring the fairness of the review results.

4.1.3. Establishing an "Accreditation" Procedure for Environmental Monitoring Data

Given the complexity and technical nature of environmental monitoring data, an "accreditation" procedure should be established to clarify the evidentiary weight of such data in the transition from administrative to criminal proceedings. The Ministry of Ecology and Environment, in conjunction with the Ministry of Justice, should formulate uniform standards for the accreditation of monitoring data, covering aspects such as the certification of monitoring agencies, standardized sampling methods, encryption requirements for data transmission, and standardized report formats. Monitoring data collected by administrative agencies must undergo the "accreditation" procedure before it can be transferred as criminal evidence. The validation procedure may adopt a "self-declaration plus random spot-check" approach, whereby monitoring agencies periodically submit self-declarations regarding data quality and undergo random spot checks by regulatory authorities. Judicial authorities may directly accept data that has passed validation, thereby reducing the burden of review; data that fails validation must undergo re-evaluation or be supplemented with additional evidence. The theoretical basis for establishing this validation procedure lies in enhancing the credibility of monitoring data and reducing uncertainties in judicial review through unified technical standards and quality control systems. This not only helps resolve the current issue of inconsistent monitoring data standards but also strengthens monitoring agencies' sense of responsibility, encouraging them to operate in a standardized manner. However, in practice, attention must be paid to cost control and ensuring fairness in the accreditation process to avoid increasing the administrative burden or creating risks of rent-seeking behavior due to excessive scrutiny. To this end, an open and transparent accreditation process should be established, and a third-party oversight mechanism should be introduced to ensure the fairness and objectivity of accreditation results.

4.2. *Technology-Driven Empowerment: Strengthening the Validity of Evidence*

4.2.1. Application of Blockchain Evidence Preservation and Integrity Verification Technologies

Blockchain evidence preservation technology provides reliable safeguards for the authenticity and integrity of electronic evidence through means such as distributed ledgers and hash encryption [6]. In the coordination between administrative and criminal enforcement in environmental protection, blockchain evidence preservation technology should be promoted. Administrative agencies should be required to simultaneously record evidence on the blockchain when collecting electronic evidence (such as pollution discharge data and monitoring reports) to ensure that the data is tamper-proof and traceable. For example, environmental protection departments can utilize blockchain technology to establish an "Environmental Evidence Preservation Platform," uploading

monitoring data, law enforcement records, and other information to the blockchain in real time to form an tamper-proof chain of evidence. At the same time, by integrating integrity verification technology, electronic evidence is provided with dual safeguards. At every stage of data collection, transmission, and storage, hash values are calculated and recorded; data integrity is verified by comparing these hash values. If a discrepancy in hash values is detected, it can be determined that the data may have been tampered with. For example, when public security authorities receive electronic evidence transferred by environmental protection departments, they recalculate the hash values and compare them with the records on the blockchain to ensure the data has not been altered during the transfer process. In theory, the combination of blockchain evidence preservation and integrity verification technology can effectively address the issues of electronic evidence being easily tampered with and difficult to trace, thereby enhancing the credibility of the evidence. However, in practical application, challenges such as high technical costs and inadequate technical infrastructure in some regions remain. To overcome these issues, the government should increase investment in blockchain technology research and development, promote collaboration among industry, academia, and research institutions, and reduce the cost of technology implementation; at the same time, it should accelerate the upgrading of technical equipment in grassroots judicial organs to enhance their capacity to review blockchain evidence.

4.2.2. Unifying Standards for the Appraisal of Electronic Evidence

To address the issue of inconsistent standards for the examination of environmental monitoring data, the Ministry of Ecology and Environment and the Ministry of Justice should jointly formulate a unified "Technical Specifications for the Examination of Environmental Electronic Evidence," clearly defining technical standards and operational procedures for stages such as sampling, analysis, and examination. For example, detection methods for different pollutants in water quality monitoring should be standardized (such as uniformly adopting national standard analytical methods), and the calibration cycles and methods for monitoring equipment should be standardized to ensure the accuracy and comparability of data. Regarding the qualifications of appraisal institutions, a unified certification system should be established to clarify the entry requirements, qualification approval procedures, and periodic assessment mechanisms for environmental electronic evidence appraisal institutions, thereby ensuring their professional competence and impartiality. To standardize the format of forensic reports, regulations should stipulate that reports must include a detailed description of the forensic process (e.g., sampling methods, use of instruments and equipment), data analysis results (e.g., pollutant concentrations, composition), quality control measures (e.g., calibration records, blank sample test results), and the basis for the forensic conclusions, thereby enhancing the standardization and readability of the reports. At the same time, a mutual recognition mechanism for assessment reports has been established; administrative and judicial authorities should mutually recognize assessment reports that comply with uniform standards to avoid duplicate assessments. Unified assessment standards help eliminate discrepancies in the interpretation of monitoring data between administrative and criminal proceedings and improve the admissibility rate of evidence. From a theoretical perspective, this serves as a key technical foundation for effectively linking electronic environmental evidence across administrative and criminal proceedings, ensuring the consistency and reliability of technical evidence across different procedures. However, in practical implementation, it is necessary to coordinate the interests and technical preferences of different departments, strengthen publicity and training on the standards, and ensure that assessment institutions, as well as law enforcement and judicial personnel, accurately understand and implement the standards.

4.2.3. Establishing an Interdepartmental Environmental Evidence Sharing Platform

To break down technical barriers to data sharing, a cross-departmental environmental evidence-sharing platform should be established to integrate data resources from departments such as environmental protection, public security,

procuratorates, and courts, thereby enabling real-time sharing and collaborative review of electronic evidence. This platform should possess the following core functions: a unified data standard interface that is compatible with the data storage formats and encryption standards of different departments to enable seamless data transmission; the introduction of blockchain technology to encrypt and archive shared data, ensuring the traceability of data sources and the tamper-proof nature of content; Establish an intelligent review system to automatically compare the technical parameters of electronic evidence and issue early warnings for data anomalies. During platform development, the principles of "security, efficiency, and convenience" should be followed, and a layered architecture should be adopted to ensure data security. For example, access permissions should be configured for different departments: environmental protection agencies can upload monitoring data and law enforcement records; public security authorities have the authority to retrieve and review relevant evidence; and procuratorates and courts can conduct in-depth analysis and make determinations regarding the admissibility of evidence. At the same time, cloud computing technology should be utilized to enable distributed data storage and efficient processing, thereby improving the platform's operational efficiency. In terms of practical application, the cross-departmental environmental evidence-sharing platform has already been piloted in some regions and has achieved significant results.

4.3. Institutional Innovation: Improving the Coordination Process between Administrative and Criminal Proceedings

4.3.1. Establishing a "Dual-Track Referral" Model: Parallel Administrative Penalties and Criminal Proceedings

To address the issues of administrative agencies' reluctance to refer cases and the practice of "substituting administrative penalties for criminal prosecution," a "dual-track referral" model should be established, allowing administrative penalties and criminal proceedings to proceed in parallel without conflict. When environmental protection authorities discover cases suspected of environmental crimes, they should issue administrative penalty decisions in accordance with the law while simultaneously initiating criminal referral procedures, thereby avoiding delays in sanctioning illegal acts due to waiting for criminal proceedings. The core of the "dual-track referral" model lies in clarifying the boundaries and coordination between administrative and judicial powers [7]. Electronic evidence collected by administrative agencies during the administrative penalty process may serve as leads or supplementary evidence in criminal proceedings; evidence obtained by judicial authorities during criminal investigations may also be shared with administrative agencies to refine administrative penalty decisions. At the same time, a referral feedback mechanism should be established, requiring public security organs to promptly inform environmental protection authorities of case filing and investigative progress upon receiving referred cases, thereby ensuring that administrative agencies have the right to be informed about the subsequent handling of cases. From a theoretical perspective, the "dual-track referral" model aligns with the dual values of administrative efficiency and judicial fairness, effectively preventing both the misuse of administrative penalties as substitutes for criminal penalties and the failure to prosecute guilty parties. However, in practical implementation, clear rules must be established for handling the overlap between administrative and criminal penalties to avoid double punishment of the parties involved. For example, fines already paid as part of administrative penalties should be offset against criminal fines; administrative penalty measures, such as orders to suspend production for rectification, should be coordinated with criminal coercive measures (such as restraining orders) to ensure consistency in the application of the law.

4.3.2. Strengthening the Supervisory Functions of Procuratorial Organs: Early Intervention and Substantive Review

As legal supervisory bodies, procuratorates should play a more active supervisory role in the coordination of electronic evidence between administrative and criminal

environmental enforcement. A mechanism for early intervention by procuratorates should be established; during the administrative investigation and evidence-gathering phase, procuratorates may dispatch dedicated personnel to intervene early and provide guidance on the collection, preservation, and safekeeping of electronic evidence to ensure that the evidence meets the requirements of criminal procedure. During the review and prosecution stage, procuratorial organs should strengthen their substantive review of electronic evidence, examining not only the legality, authenticity, and relevance of the evidence but also paying close attention to technical details (such as methods for analyzing monitoring data and the calibration status of electronic devices). For evidence that raises questions, they should require administrative or investigative agencies to provide supplementary explanations or conduct re-examinations. At the same time, a communication mechanism should be established between the procuratorate and forensic institutions; where necessary, forensic experts should be invited to assist in the review to enhance the capacity to examine complex technical evidence. Furthermore, the procuratorate should strengthen supervision over cases transferred by administrative agencies by establishing a system of regular inspections and reporting. For cases that should have been transferred but were not, the procuratorate should promptly issue prosecutorial recommendations to urge the administrative agency to transfer them; for cases transferred late or with insufficient evidence, the administrative agency should be required to rectify the situation within a specified timeframe. By strengthening supervision, the willingness of administrative agencies to transfer cases and the quality of the evidence can be improved. Theoretically, the early intervention and substantive review by procuratorial organs can effectively compensate for the shortcomings of administrative agencies in evidence collection and review, safeguard the legality and reliability of electronic evidence in environmental administrative enforcement, and ensure the uniform and correct implementation of the law.

4.3.3. Exploring the Integration of Restorative Justice and Electronic Evidence

The concept of restorative justice emphasizes the restoration of damaged ecosystems and the rehabilitation of social relationships, which aligns closely with the objectives of environmental crime governance. By incorporating the principles of restorative justice into the handling of electronic evidence in environmental criminal cases, electronic evidence serves as a key basis for assessing the severity of criminal conduct and the effectiveness of remediation. For example, monitoring data can be used to track the real-time operation of a company's pollution control facilities to determine whether it is implementing corrective measures in accordance with the remediation plan; blockchain-stored emissions data can be utilized to calculate the ecological restoration costs a company must bear. Specifically, in criminal proceedings, judicial authorities may require enterprises to submit environmental restoration plans and use electronic evidence (such as online monitoring data and video records of the restoration process) to oversee the implementation of these plans. Enterprises that actively fulfill their restoration obligations and achieve positive results may be granted leniency in sentencing; conversely, those that fail to fulfill their restoration obligations as required will face harsher penalties. In administrative proceedings, environmental protection authorities may assess an enterprise's corrective actions based on electronic evidence and impose stricter administrative penalties on enterprises that fail to make adequate improvements.

From a theoretical perspective, the integration of restorative justice with electronic evidence can achieve the integrated goal of "punishment-remediation-prevention" in environmental governance and enhance the effectiveness of combating environmental crimes. In practice, however, it is necessary to establish scientific assessment standards for ecological and environmental remediation and rules for the admissibility of electronic evidence to ensure accurate evaluation of remediation outcomes and the reasonable use of electronic evidence. At the same time, interdepartmental collaboration must be strengthened; environmental protection authorities, judicial bodies, and third-party

assessment agencies should establish information-sharing mechanisms to jointly promote the effective implementation of restorative justice in environmental crime cases.

5. Conclusion

This paper focuses on the development of electronic evidence rules in the coordination between administrative and criminal proceedings, revealing the core challenges in their legal positioning, procedural workflow, and technological adaptation: at the legal level, there are inconsistent standards for evidence admissibility, ambiguous definitions of evidence types, and a lack of rules for reverse coordination; at the technological level, there are insufficient safeguards for data authenticity, fragmented standards for forensic examination, and barriers to cross-departmental data sharing; and in practice, there is reluctance to transfer cases from administrative to criminal proceedings, a reliance on paper-based reviews, and regulatory loopholes in monitoring agencies. In response, this study proposes overcoming the obstacles to the transfer of electronic evidence between administrative and criminal proceedings by unifying legal admissibility rules, establishing a "two-stage review" model, strengthening the application of technologies such as blockchain, and improving mechanisms for administrative-criminal coordination. Future research could further focus on new forms of evidence generated by emerging technologies, the coordination of evidentiary sovereignty in cross-border environmental crimes, and the optimization of rules in empirical scenarios. This would promote the transformation and upgrading of a "technology-law" dual-driven environmental governance system in the digital age, providing institutional support for "precise pollution control and strict law enforcement."

References

1. C. Y. Wu, Y. Yuan, C. Zhang, et al., "An Empirical Study on Judicial Adjudication of Pollutant Characterization from the Perspective of Environmental Pollution Crimes: A Sample of 1,479 Judicial Rulings," *Environmental Protection*, vol. 49, no. 5, pp. 65–72, 2021.
2. Y. Li and J. Yan, "On the Evidentiary Value of Pollution Source Monitoring Data," *Journal of Hohai University (Philosophy and Social Sciences Edition)*, vol. 23, no. 6, pp. 102–108, 112, 2021.
3. S. K. Wang and Z. H. Miao, "A Study on the Evidentiary Nature and Admissibility of Environmental Monitoring Data," *Environmental Protection*, vol. 44, no. 22, pp. 53–55, 2016.
4. X. G. Zhao, "Evidence Issues and Solutions in the Coordination Between Ecological and Environmental Law Enforcement and Criminal Justice," *Evidence Science*, vol. 25, no. 5, pp. 547–557, 2017.
5. S. Wang and J. W. Li, "Approaches to Addressing Environmental Crime from the Perspective of the Integration of Criminal and Administrative Sanctions: Drawing on the EU Environmental Crime Directive," *Journal of Beijing Vocational College of Politics and Law*, no. 1, pp. 11–19, 2025.
6. Y. He, "A Study on the Application of Blockchain-Based Digital Forensics Technology in Public Security and Its Legal Regulation," *Research on the Rule of Law*, no. 3, pp. 57–71, 2024.
7. J. Liu, J. Yang, and K. Yang, "A Study on Internal and External Coordination and Integration in Public Interest Litigation by Environmental Prosecutors," *Journal of Liaoning Academy of Public Security and Judicial Administration*, no. 4, pp. 19–24, 2024.

Disclaimer/Publisher's Note: The statements, opinions and data contained in all publications are solely those of the individual author(s) and contributor(s) and not of Publisher and/or the editor(s). Publisher and/or the editor(s) disclaim responsibility for any injury to people or property resulting from any ideas, methods, instructions or products referred to in the content.