Academic Journal of Law and Society
ISSN: 3080-9908 (Print), ISSN: 3080-9916 (Online) | Vol. 1, No. 2, 2026

Research on the Admissibility and Examination Rules of Algorithmic Evidence in Criminal Cases

Jie Xia

School of Law, Anhui University of Finance & Economics, Bengbu Anhui 233041, China

Abstract: In the digital age, algorithmic evidence generated by the intervention of algorithmic technology in criminal justice is structurally impacting the traditional evidence rules system. Algorithmic evidence includes two basic forms: "matching" and "inductive." Inductive evidence, with its dual characteristics of generative dynamic fact-finding and machine-decision-based data processing, differs from static electronic data and expert opinions based on natural persons, and should be granted independent evidentiary status. At the admissibility level, algorithmic evidence meets the substantive requirements of Article 50 of the Criminal Procedure Law, which states that "materials that can be used to prove the facts of a case are evidence." Its admissibility must be determined through a triple test of relevance, reliability, and legality. At the review rules level, a two-tiered system should be constructed, distinguishing between admissibility review and probative value assessment: the former focuses on relevance, reliability, and legality as core dimensions; the latter can introduce mechanisms such as likelihood evaluation, corroboration rules, and expert assistance. Simultaneously, the obligation to disclose algorithmic technology should be improved, and the expert assistant system optimized to ensure the substantive nature of cross-examination in court, thereby achieving an organic unity between technological empowerment and procedural justice.

Keywords: Algorithmic evidence, Criminal proceedings, Admissibility of evidence, Evidence review.

1. Introduction

Currently, economic crimes involving large numbers of people, such as telecommunications fraud and illegal fundraising, continue to occur frequently. The massive amounts of data related to funds, communications, and social media involved in these cases are difficult to verify manually. Public security and procuratorial organs widely use algorithms to conduct data collision and modeling analysis, resulting in materials such as comparison screenshots and analysis reports, which are collectively referred to as algorithmic evidence in academic circles. However, judicial practice is rife with problems in classifying this evidence: facial recognition and financial tracking materials are often considered electronic data, while reports analyzing pyramid scheme amounts and hierarchical levels are often treated as expert opinions, with many judgments directly avoiding their evidentiary attributes[1]. This confusion in characterization leads to a lack of uniformity in evidence collection and cross-examination standards. Defenses are unable to effectively defend against flaws in the underlying algorithms and original data, and the potential for algorithmic bias and data tampering can easily lead to errors in fact-finding, creating a risk of wrongful convictions. This situation of regulatory gaps and misapplication not only weakens the probative value of algorithmic evidence but also may create hidden dangers for erroneous judgments. This article aims to systematically demonstrate the criminal evidentiary qualification of algorithmic evidence and, based on this, construct a review rule system adapted to its technical characteristics.

2. Definition and Type Classification of Algorithmic Evidence

2.1. Conceptual disputes and normative definitions

In academia, three distinct discourses exist regarding evidence forms centered on algorithmic technology: "big data evidence," "artificial intelligence evidence," and "algorithmic evidence."[6] This conceptual divergence directly impacts the selection of regulatory targets and the design direction of rule systems. The concept of big data evidence confuses the massive amounts of data themselves with the results of data analysis, subsuming both under the same concept—big data evidence is understood as both the massive amounts of electronic data themselves and big data analysis reports. This dual reference leads to blurred conceptual boundaries, hindering precise regulation. The concept of artificial intelligence evidence, on the other hand, overemphasizes the "intelligent" aspect of machine learning, failing to encompass the large number of evidence forms in practice based on non-machine learning algorithms (such as probabilistic statistical models, regression analysis, and other traditional algorithms)[3]. In contrast, algorithmic evidence better reveals the core characteristic of this type of evidence—"algorithms are key to the probative role of big data-related evidence."[6] Using algorithmic evidence to encompass related concepts is compatible with existing evidence review systems and directly connects with theoretical research findings related to algorithms. From the perspective of evidence law, algorithmic evidence refers to evidentiary materials formed in criminal justice activities through the processing and analysis of massive amounts of data using algorithms, which can be used to prove the facts of a case. Algorithmic evidence consists of three inseparable core elements: first, the original massive amount of electronic data; second, the algorithm program with fixed operational logic; and third, the analytical conclusions output after the algorithm runs, which are also the final evidentiary carriers submitted to the court for the purpose of determining the case.

2.2. Typification of proof forms

Based on the differences in how algorithms play a proving role, algorithmic evidence can be divided into two basic

forms .

Matching-based algorithmic evidence relies on comparisons with massive databases to provide proof. Its mechanism involves comparing existing traces or leads with a specific database. The algorithm retrieves and analyzes the database based on given information, ultimately pointing to specific data that shares similarities or relevance with that information. The core of this type of evidence lies in uncovering the relationships between data; facial recognition comparisons, DNA database comparisons, and vehicle trajectory information comparisons are typical examples. In this type of evidence, the algorithm serves only as a retrieval and filtering tool, without uncovering deep patterns or generating new facts. The algorithm's reasoning chain is clear, and the original data can be retrieved for reverse verification, resulting in relatively low technical risk.

Inductive algorithmic evidence is evidence that leverages big data analysis based on algorithmic models to provide proof. Its mechanism involves the investigating authorities extracting fragmented and disorganized original data related to a case, then using specialized algorithmic models to integrate, statistically analyze, and correlate the data, extracting the hidden logic and patterns within the data, and ultimately generating a summary analysis report . Examples include reports analyzing pyramid scheme levels and cash flows, visualizations of telecom fraud funding chains, and statistical conclusions on losses suffered by victims of fundraising fraud. Unlike matching algorithmic evidence, this algorithm does not simply extract existing information from a database; instead, it generates new evidentiary information not directly presented in the original data through the mining and induction of data patterns. It is this qualitative transformation from " data " to " conclusion " that allows inductive algorithmic evidence to transcend the traditional boundaries of electronic data in terms of evidentiary logic, making its review more complex and challenging.

3. Evidentiary Value of Algorithmic Evidence

3.1. The Structural Dilemma of the System of Legally Statutory Types of Evidence

Article 50 of the Criminal Procedure Law lists eight categories of legally admissible evidence. Regarding the nature of this legislative model, scholars hold differing interpretations: some consider it " closed, " while others see it as " semi-open . " From a literal interpretation perspective , the statement in the first paragraph, "Materials that can be used to prove the facts of a case are all evidence ," seems to reserve regulatory space for the inclusion of new types of evidence. However, from a systematic interpretation perspective, the core function of China's evidence classification system is to establish differentiated rules for the collection, examination, and use of different types of evidence. If a new form of evidence cannot be categorized into any existing type, its examination and judgment will face a lack of regulatory basis. Therefore, this legislative model essentially exhibits a " semi-closed " characteristic—existing types are relatively fixed, and the inclusion of new evidence lacks a clear regulatory channel.

This structural dilemma is particularly pronounced when dealing with algorithmic evidence. The judiciary's response generally falls into three categories: First, classifying algorithmic evidence as electronic data . This approach is somewhat reasonable for matching-type algorithmic evidence, but inductive algorithmic evidence, due to its secondary processing and autonomous conclusion generation, transcends the functional boundaries of electronic data as a static information carrier. Second, treating algorithmic evidence as expert opinions . This approach is the closest in form, but inductive algorithmic evidence presents " machine decision-making " rather than " expert judgment . " Expert opinions are essentially personal judgments made by experts using specialized knowledge on specialized issues, while inductive algorithmic evidence involves the algorithm system independently completing the entire process from data input to conclusion output. There is a fundamental difference between the autonomous operation of the algorithm and the expert-led analysis[5]. Third, avoiding explicit identification of evidence types . Using algorithmic analysis reports as non-standardized materials such as " analysis process " or " explanation of circumstances , " while avoiding qualitative difficulties in individual cases, deprives the examination and judgment of evidence of standardized support and substantially weakens the defense's right to cross-examine due to a lack of clear targets.

3.2. Substantive Determination of Admissibility of Evidence

The dilemma of the statutory evidence categories system lies essentially in binding evidentiary qualifications to statutory forms. However, Article 50, Paragraph 1 of the Criminal Procedure Law explicitly stipulates: " Materials that can be used to prove the facts of a case are all evidence. " This legislative expression effectively establishes a judgment logic for evidentiary qualifications based on substantive function rather than external form. Following this logic, whether algorithmic evidence can obtain evidentiary qualifications depends on whether it meets the substantive requirements of evidence—objectivity, relevance, and legality—rather than whether it can be classified into a certain predetermined statutory type.

From the perspective of the current statutory evidence system, matching algorithmic evidence can be considered an evolution of electronic data. In terms of storage medium, digital presentation, extraction and preservation methods, and underlying evidentiary logic, matching evidence differs from ordinary electronic data only superficially in data size and whether it relies on algorithmic retrieval; there is no essential difference. Tested against the three criteria of evidence (relevance, admissibility, and relevance), matching algorithmic evidence fully qualifies as criminal evidence. In terms of objectivity, the algorithm code and comparison parameters are pre-standardized, the computational process is mechanically fixed, and it is not subject to subjective interference from investigators. In terms of relevance, the comparison clues originate from the facts to be proven in the case; the identity, funds, and trajectory information stored in the database are objectively related to the acts involved, and the comparison conclusions can directly identify suspects and corroborate relevant facts of the crime. In terms of legality, the investigative authorities legally seize the storage medium, seal the data, prepare extraction records, and complete integrity verification; the subject, procedure, and form of evidence collection are all legal, and the evidence has no procedural flaws.

Regarding the legal characterization of inductive algorithmic evidence, the academic community mainly holds

three mainstream views: the electronic data view, the expert opinion view, and the independent evidence view. By analyzing the inherent flaws of the first two viewpoints, the independent evidentiary status of inductive algorithms can be proven. First, inductive evidence cannot be classified as electronic data. Electronic data is a static original record without a deductive or inductive process; inductive evidence involves secondary, in-depth processing of fragmented original data, uncovering inherent patterns to generate entirely new derived conclusions. It belongs to dynamic reasoning results, and its probative value far exceeds that of the original data. The generation logic and probative function of the two are fundamentally different, and classifying them as electronic data would cause a misalignment of the review rules. Second, inductive evidence is not equivalent to expert opinions. Traditional expert opinions are centered on qualified natural persons, who can appear in court to fully present the reasoning process and be cross-examined; inductive algorithmic evidence is the result of an algorithm applying logical rules of experience, relying on automatic machine calculation, and belongs to purely machine-based decision-making[1]. Simply adopting the rules for expert testimony and qualification review would create a regulatory gap.

This demonstrates that inductive algorithmic evidence should be classified as an independent new type of criminal evidence, simultaneously satisfying the three characteristics of evidence and possessing complete evidentiary qualifications. In terms of objectivity, when the algorithm model and statistical parameters are pre-fixed, the operation is free from subjective interference, and the original data is complete and unaltered, the conclusions drawn are repeatable and verifiable . Of course, the algorithm design itself may implicitly contain the designer's value presuppositions, and the selection of training data may carry inherent biases, but these factors do not negate the objectivity of algorithmic evidence at the operational level. In terms of relevance, inductive algorithmic evidence is an analysis report formed by fitting massive amounts of weakly correlated data to an algorithm, which may have a unique high similarity to the facts to be proven[2]. In this relevance model, a single data point may not have a direct connection with the facts of the case, but the overall regularity of the data can point to the facts to be proven. In terms of legality, algorithmic evidence encompasses two dimensions: the legality of the data source and the legality of the algorithm's operation. The former requires that the collection process for the basic data used as input to the algorithm comply with legal regulations and must not be obtained in a way that infringes on citizens' basic rights; the latter requires that the design and operation of the algorithm do not violate the basic requirements of procedural justice, including but not limited to not containing discriminatory designs, not improperly processing personal information, and not evading judicial review in a black-box manner.

4. The System of Rules for Examining Algorithmic Evidence

The review of algorithmic evidence should follow a two-tiered structure: " admissibility of evidence review – probative value assessment . " The admissibility of evidence review addresses whether algorithmic evidence qualifies for use in court , while the probative value assessment addresses the strength of proof of the facts to be proven by the algorithmic evidence[7].

4.1. Three Dimensions of Evidence Admissibility Examination

Relevance review. The relevance review of algorithmic evidence requires that the scope of the collected basic data has a reasonable logical connection to the case, and that the content of the analysis report has a substantial impact on the existence or non-existence of the essential facts. For inductive algorithmic evidence, the core of relevance review lies in assessing whether there is a " unique high degree of similarity " between the data patterns revealed by the algorithm and the facts to be proven . Only when the similarity between the algorithm's prediction results and the facts to be proven reaches a " striking " level can the inherent risk of bias in similarity-based evidence be overcome[2].

Reliability review. The reliability of algorithmic evidence is a prerequisite for its probative value and also the key challenge in its review. Reliability review should include three levels: the collection of basic data should be comprehensive and accurate, free from data contamination or bias, and the data sources should be independent and verifiable; the algorithm design should be scientifically sound, thoroughly tested and verified, with an error rate within an acceptable range, demonstrating robustness; and the algorithm's output results should be repeatable, cross-validated, and free from technical defects such as overfitting that could distort the conclusions. It is important to note that reliability review does not require complete algorithm transparency[4] . In cases involving trade secrets or state secrets, the alternative standard of " algorithm trustworthiness " can be adopted .

Legality review. The legality review of algorithmic evidence should be carried out from three levels: the collection of basic data should follow legal procedures, and should not infringe upon the legitimate rights and interests of citizens or violate relevant laws and regulations on personal information protection; the design and application of the algorithm should comply with legal norms and ethical requirements, and there should be no improper circumstances such as algorithmic discrimination, and personal information should be processed in a manner that conforms to the " principle of proportionality " ; the transformation process from raw data to algorithmic conclusions should comply with procedural regulations, and the fixation, storage, and transfer of evidence should comply with legal requirements.

4.2. Differentiated Approaches to Evidence Assessment

Evaluation of the probative value of matching algorithm evidence. Since the probative mechanism of matching algorithm evidence is relatively intuitive , examiners can directly determine whether there is a similarity or convergence between trace information and selected data . The focus of its probative value evaluation lies in verifying the authenticity of the relationship between the two. A likelihood ratio evaluation method can be introduced: based on Bayes' theorem, the probative strength of the evidence is quantitatively evaluated by calculating the ratio of " the probability of obtaining the evidence under the condition that the fact to be proven is true " to " the probability of obtaining the evidence under the condition that the fact to be proven is false . " The higher the likelihood ratio, the stronger the

probative value of the evidence for the fact to be proven. When the likelihood ratio reaches a certain threshold, the evidence can be considered to provide " strong support ."[7] Furthermore, for matching algorithm evidence of the same type (such as facial recognition comparison and DNA comparison), the corroboration rule should apply ; conviction should not be based solely on the algorithm comparison result, but must be corroborated by other evidence.

Evaluating the probative value of inductive algorithmic evidence. Evaluating the probative value of inductive algorithmic evidence faces greater challenges. This can be approached through the following paths: First, a review of the " pre-understanding " of behavioral data patterns , assessing whether the selected behavioral characteristics upon which the algorithm is based are complete and accurately depict the essential characteristics of a specific criminal act. Second, a review of the data source ; backend data directly extracted from criminal platforms differs significantly in completeness and accuracy from financial data obtained from banks and other third-party institutions. The former, being directly derived from criminal activity, has a stronger correlation, while the latter may lose some probative value due to data cleaning, information anonymization, and other processes. Third, algorithm verification , verifying the reliability of the algorithm through data sampling, or detecting algorithmic bias through data back-analysis.

4.3. Improvement of procedural safeguard mechanisms

The black box nature of algorithms is a core obstacle to effective review. Therefore, the prosecution's obligation to disclose algorithmic technology should be established. Disclosure should cover the algorithm's operational logic, specific parameters, training data sources, and verification test results. The disclosure period should begin from the review and prosecution stage to ensure the defense has sufficient preparation time. The standard for disclosure should adhere to the requirement of " simplicity, " explaining the algorithm's basic operating principles in a way that helps the parties understand, rather than simply providing source code[6]. For parts involving trade secrets, limited disclosure is permitted under a confidentiality agreement, with the court organizing experts from both sides to review the evidence in a closed setting. The due process principle requires that the prosecution not exclude the defense's effective participation in the review of evidence based on technical complexity.

Given the highly specialized nature of algorithmic evidence, the institutional function of expert assistants should be fully utilized. On the one hand, the restrictions on the number of expert assistants should be appropriately relaxed to meet the actual needs of examining complex algorithmic evidence. On the other hand, the rights of expert assistants to access algorithm-related information and testing environments should be guaranteed. If the defense lacks sufficient financial resources, a mechanism could be explored whereby the court appoints expert assistants ex officio, similar to the model where expert witnesses are paid by the state, with funding provided by legal aid funds or special fiscal funds[5]. Simultaneously, the boundaries of the expert assistants' responsibilities should be clearly defined; their function is to assist the court in understanding technical issues and providing professional opinions, rather than replacing the judge's fact-finding function.

5. Conclusion

With the widespread adoption of digital investigative methods, algorithmic evidence has become crucial in crimes involving large numbers of people. However, traditional evidence rules are ill-suited to this situation, leading to problems such as inconsistent characterization, superficial cross-examination, and a lack of unified standards for probative value, thus undermining judicial fairness. Clarifying the legal attributes is fundamental to the standardized application of these rules. A tiered and categorized regulatory approach should be implemented for algorithmic evidence, along with comprehensive legislation, algorithm registration, and a long-term mechanism for excluding illegally obtained algorithmic evidence. This approach aims to balance the efficiency of combating cybercrime, constrain the power of algorithms, avoid biased judgments, balance the punishment of crime with procedural justice, and implement the requirements for substantive reform of court trials.

References

[1] Bao Jianhua. Research on the legal status of big data evidence [J]. Journal of Liaoning Police Academy, 2026, 28 (1): 51-57.

[2] Ye Xiangyu. Predictive evidence in criminal proceedings: attributes, risks and applicable rules [J]. Journal of Beijing University of Science and Technology (Social Sciences Edition), 2026, 42 (1): 85-96.

[3] Wang Jun. Dilemmas and normative approaches to the examination of evidence by artificial intelligence in criminal proceedings [J]. Journal of Zhejiang Police Academy, 2025, (4):69-87.

[4] Pan Jingui. Risks and regulation of criminal evidence use in the digital age - an analytical perspective of algorithmic evidence [J]. Legal Studies, 2024, (6):26-42.

[5] Yu Pengwen. The legal nature and application rules of artificial intelligence evidence in criminal proceedings [J]. Chinese Journal of Criminal Law, 2024, (5):36-54.

[6] Zhang Di. Algorithmic evidence in criminal proceedings: concept, mechanism and application [J]. Journal of Henan University (Social Sciences Edition), 2023, 63 (3): 36-42+153.

[7] Ma Mingliang, Wang Shibao. On the rules of probative value of big data evidence [J]. Evidence Science, 2021, 29 (6): 645-656.