Science of Law Journal (2026)
Clausius Scientific Press, Canada

DOI: 10.23977/law.2026.050204
ISSN 2616-2296 Vol. 5 Num. 2

The Challenges in Admitting Generative AI Evidence

Lin Fei[1,a,*]

[1]*Guilin University of Electronic Technology, Guilin, Guangxi, China*
[a]*1549409884@qq.com*
[*]*Corresponding author*

Keywords: Generative Artificial Intelligence Evidence, Criminal Procedure, Types of Evidence

Abstract: As the third generation of machine evidence, generative AI evidence represents a new form of evidence that has emerged from the application of intelligent technologies in the judicial field. It is closely connected to concepts such as big data evidence and algorithmic evidence, and is widely used in scenarios including AI-related criminal cases and crime prediction. Currently, this type of evidence faces numerous challenges regarding its admissibility. Legally, the definition of its evidentiary attributes remains ambiguous, with ongoing disputes over its classification—including the expert opinion theory, electronic data theory, documentary evidence theory, and independent evidence theory—making it difficult to fit within existing statutory categories of evidence.

1. Introduction

Generative Artificial Intelligence (GAI) refers to the production of new content by machines driven by GAI, based on input information. This content is rooted in mechanization. Since GAI is endowed with capabilities such as deep learning, reasoning, and human-machine interaction, it can generate content at both the “belief” and “expression” levels [1]. classifies generative AI evidence into three categories: broad, intermediate, and narrow [2]. In the broad sense, generative AI evidence refers to materials capable of proving criminal facts, obtained by investigative agencies, other authorities, or authorized bodies through the scientific screening, comparison, and searching of existing data. In the intermediate sense, it refers to materials capable of proving criminal facts that are derived through in-depth mining and analysis of vast amounts of disorganized data by investigative agencies, other authorities, or authorized bodies using algorithmic models. In the narrow sense, it refers to relevant or predictive information derived through mining, assessment, and analysis of large datasets by investigative agencies, other authorities, or authorized bodies using algorithmic models. Generative AI evidence in the narrow sense refers to relevant or predictive information derived through mining, assessment, and analysis of vast amounts of data by investigative agencies, other authorities, or authorized bodies using algorithmic models.

Although scholars differ in their definitions and interpretations of generative AI evidence, they share a common understanding of its characteristics, including machine-generated nature, algorithmic autonomy, and data dependency. However, determining what type of evidence this machine-generated data constitutes and how it should be reviewed and regulated during its application has become a practical challenge for adjudicators [3].

2. Distinguishing Generative Artificial Intelligence Evidence from Traditional Evidence

Currently, academic circles are divided on the classification of GAI evidence, with various theories, including the "electronic data theory," the "expert opinion theory," and the "witness testimony theory." In judicial practice, this has led to confusion, as similar types of evidence are classified differently, resulting in inconsistent rulings [4]. A thorough analysis of the fundamental differences between GAI evidence and traditional statutory evidence, coupled with a comprehensive demonstration of the necessity and feasibility of recognizing it as an independent category of evidence, is not only a practical necessity for resolving the current challenges in judicial application but also an inevitable choice for improving China's evidence system.

2.1. Generative AI Evidence and Electronic Data

As one of the statutory categories of evidence, electronic data refers to "information formed or stored on electronic media through email, electronic data interchange, online chat records, blogs, microblogs, text messages, electronic signatures, domain names, etc." Its core attributes are originality, dependence on a physical medium, and immediacy [5]. From a technical perspective, the generation of electronic data naturally preserves digital traces during the occurrence of case facts. Adhering to the principle of "contact leaves a trace" in material exchange, such data directly reflects case facts in digital form. Its formation does not rely on subsequent analysis or processing; it can be used as evidence simply by extracting and preserving it through technical means. From a legal perspective, electronic data adheres to the "principle of dual connection," meaning it must be linked both to the facts of the case itself and to the parties involved, relevant items, and other elements. The core of its review and assessment lies in verifying the data's authenticity and integrity, employing the judicial method of "identity verification"—for example, confirming that the data has not been tampered with by comparing its hash values.

At the time of generation, electronic data serves as a real-time record of the facts of a case; its creation is temporally consistent with the occurrence of those facts. For example, in cases of online fraud, the fraudulent text messages sent by scammers are generated and preserved the instant they are sent, constituting original evidence "generated at the time of the incident." In contrast, GAI evidence is conclusive material generated after the incident by judicial authorities or parties involved [6]. It is created by collecting massive amounts of electronic data to prove specific facts of a case, and then mining, cleaning, correlating, and analyzing that data through algorithmic models. This constitutes "post-incident" derived evidence. For example, in cases involving the crime of organizing and leading pyramid schemes, after investigative authorities collect massive amounts of electronic data—such as registration data, transaction records, and hierarchical relationships from the involved platforms—they use GAI systems to construct algorithmic models. Through analysis, they derive conclusions regarding the number of individuals involved, the amount of money involved, and the hierarchical structure. These conclusions are not the raw data itself, but rather the result of in-depth processing and logical deduction of the raw data [7].

In terms of form, electronic data manifests as raw digital information stored on electronic media, with its core value residing in the data itself. It can be directly read and displayed through technical means; for example, chat records extracted from a mobile phone can be presented directly in text form, and video data extracted from surveillance equipment can be played back directly. In contrast, GAI evidence typically takes the form of analytical reports, visual charts, data models, and other transformed formats. Its core value lies not in the raw data, but in the conclusions output by the algorithm. For example, in financial fraud cases, after a GAI system analyzes massive amounts of transaction data, the resulting "Fund Flow Analysis Report" presents the flow of funds and the relationships between involved accounts in chart form. This report is a logical reconstruction of the

original transaction data, rather than a simple presentation of the raw data.

In terms of evidence types, electronic data can serve as both direct and circumstantial evidence to prove the facts of a case. For instance, in a theft case, surveillance footage directly recording the suspect's theft process constitutes direct evidence; in an assault case, the victim's call records proving contact with the suspect before and after the incident constitute circumstantial evidence. The evidentiary mechanism of GAI evidence involves using algorithms to establish correlations between data, thereby transforming "data correlations" into "logical causality." GAI evidence itself does not directly point to the facts of the case; it must be combined with other evidence to form a complete chain of proof. For instance, in online gambling cases, the conclusion drawn by the GAI system that "the transaction frequency of the involved account is abnormal" must be combined with other evidence—such as the account holder's statements, bank statements, and data from the gambling platform—to prove the criminal fact that the account holder participated in gambling.

Furthermore, the focus of electronic data examination lies in authenticity and integrity, with the core objective being to ensure that the data has not been tampered with or forged. Examination methods include verifying hash values, reviewing extraction procedures, and validating storage media. In contrast, the examination of GAI evidence focuses not only on the authenticity and integrity of the raw data but also on technical issues such as the reliability of the algorithms and the legality of the data processing procedures.

2.2. Generative AI Evidence and Expert Opinions

An expert opinion is "a conclusive opinion issued by a person with specialized knowledge who, upon assignment or engagement by judicial authorities, analyzes and judges specialized issues requiring resolution in a case using their specialized knowledge and skills." Its core attributes are human expertise, statutory procedures, and procedural transparency. From a technical perspective, the generation of expert opinions relies on the expert's specialized knowledge and practical experience. The expert reaches conclusions through observation, examination, and analysis of the submitted materials, applying professional logic [8]. For example, a forensic pathologist's assessment of a victim's injuries relies on forensic medical knowledge and clinical experience, while handwriting analysis relies on graphological knowledge and forensic expertise. From a legal perspective, the generation of expert opinions must follow statutory procedures. The expert must possess statutory qualifications, the examination process must comply with industry standards, and the expert report must specify the basis, methods, and process of the examination to ensure the verifiability and cross-examinability of the conclusions.

The core of an expert opinion lies in the subjective cognitive activities of human experts. As entities possessing specialized knowledge, experts play a leading role in the assessment process, and their professional competence, practical experience, and professional ethics directly influence the accuracy of the conclusions. In contrast, the primary generator of GAI evidence is an intelligent machine; humans play only a supporting role in stages such as data input, algorithm selection, and model training, while the final analytical conclusions are "machine opinions" autonomously derived by algorithms. This process does not require the subjective judgment of human experts and relies entirely on the computational logic of the algorithm.

Expert opinions address "specialized issues"—that is, problems that adjudicators cannot resolve based on common sense or experience alone, but which require specialized knowledge in a specific field. While GAI evidence relies on complex algorithmic technologies, its conclusions are essentially the result of logical induction and statistical analysis of massive amounts of data; they merely reflect an advantage in computational power rather than a breakthrough in specialized knowledge. As scholar Zhou (2023) has pointed out, "The reason why large datasets cannot be

directly read by human beings is not that their content is profound and obscure, requiring specialized knowledge to understand, but simply because of their sheer volume [9]. If one were to attempt to read them using the human resources available in judicial practice, the task could not be completed within a reasonable timeframe; therefore, computer processing power must be used to accelerate the process." Regarding GAI evidence, adjudicators can typically understand it based on common sense, without relying on specialized knowledge.

The generation of expert opinions must follow strict statutory procedures. Regulations such as the General Rules on Judicial Appraisal Procedures and the Rules on Appraisal by Public Security Organs clearly stipulate the qualifications of appraisal institutions and experts, the commissioning and acceptance of appraisals, the appraisal process, and the issuance of appraisal reports, ensuring the openness, fairness, and verifiability of the appraisal process. For example, experts must specify the basis, methods, and process of the examination in their reports, undergo cross-examination by both the prosecution and the defense, and, when necessary, appear in court to testify and explain how the conclusions were reached. In contrast, the generation of GAI evidence suffers from a "black box" problem: information regarding the design principles, operational logic, and data processing standards of the algorithms is often not disclosed to the public, making it difficult for judicial authorities and parties to understand how the conclusions were formed. Furthermore, China's current judicial appraisal regulations do not include GAI analysis within the scope of statutory appraisals [10]. Consequently, GAI evidence lacks the statutory qualification requirements and procedural safeguards necessary for expert opinions, resulting in its admissibility and verifiability being far lower than those of traditional expert opinions.

3. Conclusions

The legal status of generative AI evidence is a central issue in both its theoretical research and judicial application, and it serves as the theoretical premise and legal basis for resolving the practical challenges in its recognition. This paper argues that relevant research should focus on the core characteristics of generative AI evidence and its distinction from traditional evidence. Regarding core characteristics, generative AI evidence is fundamentally defined by machine-generated content, algorithmic autonomy, and data dependency, which fundamentally distinguish it from the originality of electronic data and the human expertise inherent in expert opinions.

Acknowledgements

The authors gratefully acknowledge the financial support from the Innovation Project of GUET Graduate Education (Project No. 2026YCXS167).

References

[1] Xiong, X. B. (2025). Dilemmas and regulatory approaches in the admissibility of generative AI evidence. Legal Science (Journal of Northwest University of Political Science and Law), 43(1), 72.
[2] Feng, Y. (2024). A study on the pathways for the admissibility of criminal big data evidence. Journal of Dalian University of Technology (Social Sciences Edition), 45(5), 93.
[3] Xie, D. K. (2025). Typological analysis and rule construction of artificial intelligence evidence. Learning and Exploration, (3), 62.
[4] Xie, Y. P. (2024). The dual mission of China's criminal justice reform in the era of artificial intelligence. Political and Legal Studies, (5), 84.
[5] Yu, P. W. (2024). The legal nature and rules of application of artificial intelligence evidence in criminal proceedings. Chinese Journal of Criminal Law, (5), 39.
[6] Pan, J. G. (2024). Risks and regulation of criminal evidence application in the digital age: An analysis from the

perspective of algorithmic evidence. Research on the Rule of Law, (6), 27.
[7] Cheng, L. (2022). On the formalization and substantivization of cross-examination of big data evidence. Politics and Law, (5), 97.
[8] Shi, P. P. (2024). On big data investigations: Focusing on the right to informational self-determination. Research on the Rule of Law, (6), 17.
[9] Zhou, M. H. (2023). On the legal status of big data evidence. Legal Science (Journal of Northwest University of Political Science and Law), (4), 108.
[10] Hu, M. (2025). On the triadic structure of criminal evidence in the digital age. Chinese and Foreign Law, (1), 56.