Law and Humanities
ISSN Print: 3079-5117
ISSN Online: 3079-5125
https://doi.org/10.63313/LH.9016

Research on the Application of Big Data Evidence in Criminal Procedure

You Wan
Anhui University of Finance and Economics, Bengbu 233030, China
Email: wizzy1220@163.com

How to cite this paper: Wan, Y. (2025). Research on the Application of Big Data Evidence in Criminal Procedure. Law and Humanities, 1(2), 65–73. ISSN Print: 3079-5117; ISSN Online: 3079-5125.
https://doi.org/10.63313/LH.9016
Published: 2025-06-26

Abstract

The rapid development of big data technology has profoundly transformed the mode of social operation, and has also had a revolutionary impact on the field of criminal procedure. Big data evidence, with its characteristics of magnanimity, pluralism, relevance and predictability, has shown great potential in improving investigation efficiency, assisting judicial decision-making and revealing the law of crime. However, as a new form of evidence, it faces serious challenges in terms of evidence qualification, authenticity examination, relevance determina-tion, guarantee of cross-examination right and prevention of algorithm bias. This article is based on the practice of criminal proceedings in China and draws on the beneficial experience abroad to systematically explore the conceptual characteristics, application value, practical difficulties and regulatory paths of big data evidence, and puts forward countermeasures and suggestions such as improving legislation, building multi-level review rules, strengthening proce-dural rights protection and improving algorithm governance mechanisms, so as to adhere to the litigation core values of procedural justice and human rights protection while maximizing the effectiveness of big data evidence.

Keywords

Big data evidence; Algorithm; Application rules; Types of evidence

1. Introduction

With the rapid development of information technology, human society has entered a data-driven era. Big data, as the core production factor and cognitive tool of this era, has profoundly reshaped the operation logic of various social systems, including the judicial field, with its unprecedented characteristics of Volume, Velocity, Variety and Value-4V. Criminal litigation, as an important field for the state to prosecute crimes and protect human rights, cannot be outside the flood of data. Big data evidence arises at the historic moment. It does not simply refer to a huge collection of electronic data, but refers to the specific information carrier and its analysis conclusion used to prove the facts of the case by collecting, storing, processing and analyzing massive, multi-source and heterogeneous data, mining the implicit relevance, regu-

larity or predictive information with specific algorithm models. Its form can be either the original data set as the basis for analysis, or the statistical report, behavior portrait, correlation map or prediction result generated after complex calculation. The use of big data evidence in criminal proceedings is no longer a theoretical concept, but a living judicial practice. For example, in the derivative criminal prosecution of a "first case of face recognition" in Hangzhou, the police precisely depict the behavior track and activity law of the suspect by using big data analysis technology through obtaining mass face capture data in public places, combining with the historical travel, payment and other debris information of the suspect, and providing key support for locking the suspect. Such practices highlight the great value of big data evidence in improving judicial efficiency and mining the chain of concealed evidence. However, under the halo of technology enabling, the legal and ethical shock caused by it as a new form of evidence cannot be ignored, which concerns whether criminal proceedings can continue to effectively fulfill their dual missions of fighting crime and safeguarding human rights in the digital era.

2. Concept of Big Data Evidence

Big data evidence, as an application of big data technology in the judicial field, undergoes three stages in its formation: data preparation, data processing and analysis, and knowledge presentation. Crucially, the big data evidence submitted in court as evidentiary material is substantively the product of the third stage—namely, the analytical report. Some scholars contend that the ontology of big data evidence concerns what evidentiary entity the concept "big data evidence" refers to; the author concurs that the ontology and structure of big data evidence should be distinguished. Differentiating "structure" from "ontology" is to differentiate the "source" from the "outcome": the "ontology" of big data evidence should unequivocally be the big data report generated during the knowledge presentation stage, while the case-relevant big data sets from the data preparation phase constitute its source and foundation, and the algorithmic models deployed during data processing and analysis represent its generation method—these two elements, together with the big data report, form an evidentiary structure with external linkages. This distinction is necessary for two reasons: First, both data preparation and data processing/analysis are merely prerequisite steps for generating the big data report. Although big data sets and algorithms contain case-relevant facts, these are dispersed across massive datasets and algorithms incomprehensible to laypersons—too fragmented and unextractable to exist as independent evidence. Only the semantically explicit big data report formed during knowledge presentation qualifies as the ontology of big data evidence and can functionally serve probative purposes in litigation. Second, the sheer volume and technical complexity of big data sets and algorithms render them impractical for demonstration during cross-examination. Submitting millions of data points as evidentiary ontology would severely impede trial efficiency, and full access to raw data

is unnecessary for verifying the admissibility or weight of big data evidence. Treating these elements as "ontology" would be extremely cost-ineffective and lack practical foundation—in judicial practice, big data evidence typically manifests as analytical reports issued by authorized entities. This does not, however, diminish the importance of big data sets and algorithms; conversely, the relevance of data sets to case facts and the scientific validity of algorithms determine the probative value of big data evidence. Authentication of big data evidence invariably begins with scrutinizing these two elements.

According to the definition method of the concept of category plus category difference, the category concept of big data evidence is an analysis report, which means that the characteristics of big data evidence different from other analysis reports are "the calculation and analysis of the collected, cleaned and processed big data sets related to the case by using big data algorithms". Therefore, this article defines big data evidence as "the analysis report obtained by using big data algorithms to calculate and analyze the collected, cleaned and processed big data sets related to the case to prove the facts of the case".

2. Unique Attributes and Criminal Justice Value of Big Data Evidence

To deeply understand the application of big data evidence in criminal proceedings, it is crucial to grasp its unique attributes that distinguish it from traditional forms of evidence. First, the massive and diverse nature of data sources. The foundation of big data evidence is a large-scale and diverse pool of raw data, which may include communication records, financial transactions, location trajectories, biometric features, network behavior, public surveillance videos, and other data. This broad spectrum enables it to construct a "data panorama" that far exceeds individual experience perception. Secondly, the algorithm dependence of the analysis method. From raw data to forming conclusions that can be used to prove the facts of a case, the core step is to use complex statistical models and machine learning algorithms for deep mining, pattern recognition, and correlation analysis. The design and selection of algorithms directly determine the form and tendency of the output results. Third, the relevance and predictability of information output. The core value of big data analysis lies in revealing the hidden correlation between data items, and possibly inferring future behavior or event probabilities based on historical data. This correlation often goes beyond direct causal proof, and its predictive power is a challenge to the traditional retrospective judicial proof model. Fourth, the inherent "black box" attribute and opacity. The complex algorithm model operation process is highly specialized and often regarded as a trade secret by commercial companies, making it difficult for non-professionals (including judges, prosecutors, lawyers, and even technicians) to fully understand and explain its decision-making logic.

However, it is precisely these unique attributes that endow big data evidence with

irreplaceable and significant value within criminal justice proceedings. During the criminal investigation phase, it functions as a high-performance engine, substantially enhancing information processing capacity and intelligence analysis accuracy. By integrating and analyzing multi-dimensional data—such as communications, financial transactions, transportation, and online activities—it enables investigators to rapidly narrow down suspect pools, reconstruct spatiotemporal routes of criminal activities, identify potential accomplice networks, detect anomalous fund flows (e.g., recognizing money laundering patterns), and even predict potential high-risk crimes (e.g., forecasting crime hotspots based on historical data).During the prosecutorial review stage, big data analysis reports provide prosecutors with objective and quantitative references. These assist in evaluating the completeness of the evidentiary chain, determining criminal intent (e.g., through keyword analysis of chat records), and quantifying the consequences of crimes (e.g., assessing fraud amounts using e-commerce data). This supports prosecutors in making more precise decisions regarding indictment and formulating sentencing recommendations. At the trial stage, the value of big data evidence lies in offering macro-level perspectives and contextual background information, aiding judges in their judicial fact-finding. For instance: Analyzing fluctuations in drug transaction data within specific regions and timeframes can indirectly corroborate a defendant's testimony regarding the scale of drug trafficking. Analyzing the similarity between a defendant's online behavioral patterns and the alleged cyberattack can strengthen the probative value of circumstantial evidence. Its powerful correlation-revealing capability helps transcend the superficial details of individual cases, presenting a criminal landscape closer to the underlying truth.

3. Core Dilemmas and Challenges in the Application of Big Data Evidence

Even as big data evidence demonstrates formidable capabilities, its application is deeply entangled in multifaceted legal and practical dilemmas, posing severe challenges to the long-established concepts and rules of criminal procedure.

3.1. Foundational Challenges to Evidentiary Rules

The existing evidentiary rules framework exhibits systemic incompatibility when confronting big data evidence. The admissibility determination dilemma stands foremost—while China’s Criminal Procedure Law categorizes electronic data as statutory evidence, the composite nature of big data evidence obscures its legal classification. For instance, during a network pyramid scheme trial, a local court encountered significant disagreement over whether the prosecution’s "User Behavior Correlation Graph Analysis Report" should be classified as electronic data or an expert opinion, resulting in disordered admissibility review standards. The erosion of reliability assessment stems from the engulfing effect of the techno-

logical black box: traditional verification methods prove ineffective against data contamination risks (e.g., an anti-fraud system generating erroneous judgments due to ingesting manipulated third-party payment data), algorithmic non-traceability (where multi-layered nonlinear computations of deep learning models defy visualization), and result non-reproducibility (where algorithmic iterations cause identical inputs to yield divergent outputs). Illustratively, a provincial public security bureau's drug flow prediction model was excluded by the court after defense challenges invoking the "garbage in, garbage out" principle due to undisclosed data cleaning rules.

3.2. Structural Conflicts in the Logic of Legal Proof

The logic of proof underlying big data evidence exhibits a fundamental tension with traditional paradigms of judicial proof. This tension manifests not only at the technical level but penetrates more profoundly into the epistemological and methodological core of criminal justice. Traditional judicial proof adheres to a causal chain construction model: it establishes necessary connections between "act and consequence" through retroactive fact reconstruction, relying on mutually corroborating evidentiary nodes such as physical evidence, documentary evidence, and testimonial evidence. Its logical foundation rests on the verifiability of empirical rules and scientific laws. In contrast, big data evidence operates via a correlation-based discovery mechanism: it reveals statistical associations between variables through pattern recognition within massive datasets, with its conclusions being inherently probabilistic inferences. When such population-level probabilities are directly applied to individual convictions, a perilous epistemic alienation of the proof logic occurs. Within specific judicial contexts, this alienation manifests as a threefold distortion:

First, the slippage from causal proof to correlation-based presumption undermines the foundation of the presumption of innocence. In a major serial theft case in one province, the prosecution submitted a "high-risk population behavior model" report based on 100,000 criminal records. This model extracted 20 behavioral characteristics through historical data analysis and indicated a 92% match between the defendant's behavioral profile and the model. The court directly treated this match rate as core evidence of the defendant's criminal propensity but overlooked two fatal flaws: First, the "historical criminal records" underpinning the model contained a substantial volume of unverified administrative penalty data; second, applying group statistical characteristics to an individual defendant constitutes a classic ecological fallacy. This logical leap essentially substitutes mathematical probability for the legal standard of "proof beyond reasonable doubt," trapping the defendant in a modern form of identity-based conviction—being found guilty by association of characteristics.

Second, embedded algorithmic bias leads to the automated reproduction of judicial discrimination. Exemplified by State v. Loomis in Wisconsin, USA, a recidivism risk

assessment tool systematically assigned higher risk scores to Black defendants. This originated from its training data—arrest records historically tainted by racial bias: when police over-patrolled Black communities, more arrest data from Black individuals was fed into the system, leading the algorithm to "learn" a spurious association of higher Black criminality. This bias finds real-world parallels in China: the "Police Brain" crime prediction system in an eastern city, trained primarily on surveillance data from urban commercial districts, achieved less than 30% accuracy in forecasting crime within urban-village rental areas along the urban-rural fringe. More insidious discrimination stems from the proxy variable trap—when algorithms infer economic status using zip codes or gauge job stability via food delivery ordering times, they effectively convert legally protected sensitive attributes into technical parameters. In an online lending fraud case, a defendant was deemed to possess "intent for illegal appropriation" based on "frequent browsing of luxury goods websites," demonstrating how algorithms reinforce societal structural inequalities.

Third, the misuse of predictive conclusions subverts the temporal sequence of judicial fact-finding. Traditional criminal litigation focuses on proving past facts, whereas the core value of big data evidence often lies in predicting future risks. When, in a juvenile delinquency case, the prosecution submits a "Violent Tendency Prediction Report" generated from a school bullying database as grounds for sentence enhancement, it essentially equates "potential future wrongdoing" with "established past criminal conduct." This judicial fiction—treating probabilistic futures as deterministic pasts—not only violates the principle of culpability but also breeds a "monster of preemptive adjudication." The danger intensifies when predictive models create feedback loops: police deploy more resources to specific communities based on crime prediction systems → arrests increase in those areas → more data reinforces the original bias → the model further targets the zone, ultimately forming an automated assembly line of judicial discrimination.

3.3. Erosion Crisis of Procedural Safeguards

The technological divide is dismantling the principle of prosecutorial-defensive equality in unprecedented ways, propelling criminal litigation toward a judicial dystopia of "digital might makes right." In the nationally high-profile "7·22" Cross-Border Online Gambling Case, the prosecution submitted a clustering analysis report based on millions of player behavioral data points as core evidence. Yet, the defense counsel, unable to access the raw data clusters or obtain algorithm feature engineering documentation, saw cross-examination reduced to a performative protest—this predicament exposes a tripartite structural oppression: knowledge monopoly barriers incapacitate the legal community—when convolutional neural networks optimize crime pattern recognition via gradient descent and random forest algorithms generate decision paths through information entropy node splitting, the

cognitive frameworks built through traditional legal training collapse entirely—trial transcripts from one local court reveal that 87% of defense lawyers admitted in court they "did not comprehend the report's algorithmic fundamentals"; information black box blockades exploit trade secret protections to entrench technological hegemony—in a Shenzhen case involving the crime of infringing on citizens' personal information, the technology vendor invoked Article 9 of the Anti-Unfair Competition Law to withhold the weighting parameters of the user profiling model—in an e-commerce fraud case, key feature vectors were labeled "core assets" and withheld, leaving the defense in a state of absolute vulnerability—"ignorant of both self and adversary"; resource asymmetry catastrophically tilts the litigation balance—prosecutors leverage provincial electronic evidence labs with tera-scale computing power, while defense expert assistants must self-fund even basic testing environments. This crisis materializes acutely when technical flaws directly erode substantive justice: in a Guizhou juvenile assault case involving an ethnic minority youth, the prosecution used a commercial Chinese NLP tool to analyze his social media chats, misclassifying a dialect phrase as aggressive language—the defense, lacking access to the model's dialect test set, could not prove the fatal flaw: the module's accuracy rate on dialects was below 45%; more gravely, when a pilot "Algorithmic Legal Aid" scheme was implemented, only 1 out of 34 duty lawyers possessed basic Python competency, laying bare the justice system's institutional inertia in confronting the digital transformation. This crisis represents the structural collapse of the "access to justice" framework in the digital age—as the right to defense enshrined in Article 14 of the Criminal Procedure Law collides with the technological black box of deep learning architectures, the very foundations of procedural justice crumble beneath the weight of algorithmic power.

4. Perfecting the Regulatory Framework for Big Data Evidence in China's Criminal Procedure

4.1. Systematizing the Legal Taxonomy and Admissibility Framework

To resolve the judicial adaptability crisis triggered by big data evidence, it is imperative to establish an independent subcategory of "Derived Big Data Evidence" within the revised Criminal Procedure Law, constructing a tiered review framework that balances inclusivity and binding force. The first tier—foundational legality review—must uphold constitutional boundaries, strictly adhering to the six lawful bases stipulated in Article 13 of the Personal Information Protection Law (PIPL) while implementing the Article 32 Data Security Law principles of "purpose specification and data minimization" for data collection. Procedural sanctions shall apply to evidence-gathering violating authorization requirements—for example, evidence obtained through warrantless extraction of mobile device data exceeding 30 days or using facial recognition databases of million-scale must be categorically excluded alongside its derived conclusions. The second tier—technical reliability thresh-

olds—requires quantifiable admission criteria, drawing on the EU Artificial Intelligence Act's regulatory logic for high-risk systems. Evidence proponents must submit algorithm performance validation reports with third-party testing certifications; deep learning models exceeding permissible opacity thresholds shall be presumed judicially unreliable. The third tier establishes three golden rules: (1) direct inference of individual conduct from group statistical characteristics is prohibited; (2) predictive conclusions must disclose confidence intervals and cannot solely support convictions; (3) algorithmic decision paths must be mapped to legal elements via explainability tools. These three tiers erect legal barriers against technological autocracy through integrated regulation—negating evidence admissibility, restricting probative value, and constraining inferential reasoning—while clarifying the scope of derivative exclusion: for instance, output from crime-prediction models trained on illegally obtained 100,000 payment records shall be excluded as "fruit of the poisonous tree," ensuring evidentiary rules remain rooted in the soil of rule-of-law civilization in the digital age.

4.2. Penetrative Scrutiny Mechanisms for Technological Black Boxes

Building a Dual-Track Verification System: Within judicial proceedings, implement tiered compliance with algorithmic explanation obligations—for transparent models (e.g., decision trees), require visual demonstration of reasoning paths; for deep learning models, mandate Local Interpretable Model-agnostic Explanations (LIME) reports. At the professional support level, emulate the Dutch Judicial Data Audit Authority model by establishing provincial Judicial Technology Validation Centers to conduct sandbox testing of critical evidence. For instance: voiceprint recognition evidence must be tested for misidentification rates under identical noise conditions; financial fraud analysis models require injected adversarial samples to verify stability. Concurrently establish a bias correction regime: obligate technology providers to conduct fairness testing per Personal Information Security Specification, disclosing model performance disparities across sensitive attributes (gender/region/etc.), such as ensuring $\leq 5\%$ deviation in recidivism prediction scores for ethnic minority defendants versus majority peers under identical offense circumstances.

5. Epilogue

In summary, the deep integration of big data evidence into criminal proceedings has become an irreversible tide of judicial intelligence. By uncovering correlations within massive datasets and leveraging algorithmic precision, it significantly enhances investigative capabilities and judicial decision-making—from the precise trajectory reconstruction in Hangzhou's facial recognition case to the intelligent detection of abnormal transaction patterns in financial crimes, all exemplify technology's transformative power in crime governance. Yet the double-edged nature of this tool grows increasingly evident: as algorithmic biases covertly replicate racial dis-

crimination, and "high-risk population models" substitute statistical correlation for individual culpability, big data evidence now fundamentally challenges the presumption of innocence, procedural fairness, and rights protection. Faced with the profound tension between efficiency and justice, innovation and regulation, neither techno-optimism nor conservative rejection offers a rational path forward. The solution lies in a trinitarian regulatory architecture: anchoring evidentiary boundaries through legal taxonomy—amend the Criminal Procedure Law to establish "Derived Big Data Evidence" as a distinct category, enforce strict exclusionary rules for illegally collected data; establishing algorithmic accountability through tiered explainability obligations—implement layered explanation mechanisms (e.g., LIME for deep learning), create judicial data audit institutions to conduct bias testing; rebalancing adversarial equality via procedural revolution—grant defense rights to algorithmic discovery and adversarial testing, integrate technical assistance into state-funded legal aid. Only through this framework can we harness big data's crime-fighting potential while upholding criminal procedure's sacred mission as a guardian of human rights. This ensures technological rationality serves the supreme value: "enabling the people to perceive fairness and justice in every judicial case." Thus shall we evolve from the reign of data power toward the promise of digital justice.

References

[1] Christopher Slobogin, "Government data mining and the fourth amendment," University of Chicago Law Review, Vol. 75, 2008.

[2] Kate Crawford, Jason Schultz, "Big Data and Due Process: Toward a Framework to Redress Predictive Privacy Harms," Boston College Law Review, Vol. 55, 2014.

[3] Kate Crawford, Rashida Richardson, Jason Schultz, "Dirty Data, Bad Predictions: How Civil Rights Violations Impact Police Data, Predictive Policing Systems, and Justice," New York University Law Review, Vol. 94, 2019.

[4] Matthew Tokson, "The Emerging Principles of Fourth Amendment Privacy," George Washington Law Review, Vol. 88, 2020.

[5] Orin S. Kerr, "An Equilibrium-Adjustment Theory of the Fourth Amendment," Harvard Law Review, Vol. 125, 2011.

[6] Orin S. Kerr, "The Case for the Third Party Doctrine," Michigan Law Review, Vol. 107, 2009.

[7] Sarah Braynea, "Big Data Surveillance: The Case of Policing," American Sociological Review, Vol. 82, 2017.

[8] Stephen E. Henderson, "A Few Criminal Justice Big Data Rules," Ohio State Journal of Criminal Law, Vol. 15, 2017.