PUNGGAWA LAW REVIEW
Punggawa Law Review
Volume 2, Number 1, 2027
E-ISSN: 3125-0580
Open Access: punggawajournal.com/plr

Criminal Liability for the Misuse of Artificial Intelligence in the Manipulation of Electronic Data within E-Ticketing Systems

Mahmudha Satrio Sakti[1], Krista Yitawati[2], Meirza Aulia Chairani[3]
[1] Master of Notary Study Program, Faculty of Law, Universitas Narotama Surabaya, Indonesia
[2,3] Faculty of Law, Universitas Narotama Surabaya, Indonesia
Correspondence: sktsuper@gmail.com

Article Info
Article history:
Received Oct 4th, 2026
Revised Nov 15th, 2026
Accepted Nov 23th, 2026

Keyword:
Artificial Intelligence; Criminal Liability; Personal Data Protection

ABSTRACT
The integration of artificial intelligence (AI) into Indonesia's Electronic Traffic Law Enforcement (ETLE) system introduces legal challenges concerning electronic data manipulation, criminal liability, and personal data protection. This study aims to analyze the applicability of Article 32 paragraphs (1) and (2) of the Electronic Information and Transactions Law to AI-assisted data manipulation and examine its relationship with personal data protection obligations. This study employs normative legal research using statutory and conceptual approaches, with primary and secondary legal materials analyzed through grammatical, systematic, and teleological interpretation. The findings demonstrate that AI is not recognized as an independent subject of criminal law; therefore, criminal liability must be attributed to individuals or corporate entities based on proven unlawful conduct, criminal intent, and operational control. Digital audit trails, system logs, and forensic examinations are essential for distinguishing intentional manipulation from technical failures and institutional negligence. Furthermore, noncompliance with personal data protection obligations does not automatically establish criminal liability but may indicate institutional accountability failures. This study proposes an integrated legal accountability framework combining criminal fault attribution, electronic evidence verification, and personal data protection compliance to strengthen legal certainty, proportional accountability, and procedural fairness in AI-supported traffic law enforcement.

© 2026 The Authors. Published by Punggawa Legacy Center. This is an open access article under the CC BY license (https://creativecommons.org/licenses/by/4.0/)

INTRODUCTION

The integration of artificial intelligence (AI) into electronic traffic law enforcement has transformed conventional traffic monitoring into a technology-driven process that relies on digital evidence and automated data analysis. In Indonesia, the Electronic Traffic Law Enforcement (ETLE) system utilizes electronic records to identify traffic violations, verify vehicle information, and support enforcement decisions (Ajisaka & Delano, 2026). Although technological automation can improve administrative efficiency, it also introduces legal risks involving inaccurate identification, algorithmic errors, and unauthorized manipulation of electronic evidence. Husada et al. (2026) emphasize that automated traffic enforcement must satisfy procedural fairness, transparency, and accountability to protect individuals from unjust legal consequences. Similarly, Rigo et al. (2025) highlight continuing regulatory and institutional challenges concerning electronic evidence and personal data protection within Indonesia's ETLE implementation.

The misuse of AI in manipulating electronic traffic data raises fundamental questions concerning criminal responsibility and the legal status of autonomous technological systems. Under the Indonesian legal framework, AI is generally understood as an electronic system or agent rather than an independent subject of criminal law (Haris & Tantimin, 2022). Consequently, criminal liability must be assessed in

relation to individuals or legal entities responsible for developing, operating, supervising, or controlling the technological system (Sebayang et al., 2024). Mecca et al. (2025) further identify regulatory challenges arising from the increasing application of AI within Indonesia's criminal justice system. These concerns demonstrate the importance of establishing a legally defensible mechanism for attributing unlawful conduct and criminal intent to identifiable actors rather than automatically assigning responsibility to technological systems.

Electronic data manipulation within ETLE systems must also be examined through the substantive requirements of Indonesian cybercrime legislation. Article 32 paragraphs (1) and (2) of the Electronic Information and Transactions Law (ITE Law) regulate specific unauthorized acts involving electronic information or documents, including alteration, deletion, concealment, and unlawful transfer. However, distinguishing deliberate manipulation from technical malfunction requires reliable evidence concerning system access, algorithmic configuration, transaction records, and digital audit trails. (Angyalossy & Anděl, 2025) underline the importance of evidentiary authenticity, transparency, and procedural fairness when AI-generated information is introduced into criminal proceedings. Furthermore, Arifudin MZ & Bima (2026) emphasize the need for verification standards and human oversight to preserve the legal reliability of AI-supported digital evidence in judicial processes.

The legal implications of AI-assisted manipulation extend beyond criminal liability to the protection of personal information processed through electronic traffic enforcement. Indonesia's Law Number 27 of 2022 concerning Personal Data Protection establishes obligations relating to lawful processing, data accuracy, security, and accountability, which are relevant to ETLE records containing identifiable personal information. Eddy & Sugianto (2026) identify wrongful ticketing, algorithmic inaccuracies, and insufficient institutional safeguards as significant concerns affecting personal data protection within Indonesia's ETLE system. Nevertheless, existing studies have predominantly examined algorithmic fairness, electronic evidence, AI regulation, or data protection as separate legal issues, leaving the relationship between criminal fault attribution and personal data governance insufficiently integrated. This study addresses that gap by examining how the elements of electronic data manipulation under the ITE Law interact with personal data protection obligations when AI technologies are misused within ETLE operations.

Accordingly, this study aims to analyze the applicability of Article 32 paragraphs (1) and (2) of the ITE Law to AI-assisted electronic data manipulation and to determine the legal basis for attributing criminal responsibility to relevant human or organizational actors. It further examines how the Personal Data Protection Law informs the assessment of institutional duties, unauthorized processing, and accountability in the management of electronic traffic records. Employing normative legal research through statutory and conceptual approaches, the analysis focuses on criminal intent, unlawful conduct, human control, evidentiary traceability, and data protection compliance. The study contributes to the development of an integrated legal framework that distinguishes intentional criminal manipulation from technical failure and institutional negligence without automatically equating data protection violations with criminal offenses. Its findings are expected to strengthen legal certainty, proportional criminal accountability, and the protection of individual rights in Indonesia's increasingly automated traffic enforcement system.

RESEARCH METHODS

This study employed a normative legal research design to examine criminal liability arising from the misuse of artificial intelligence (AI) in electronic data manipulation within Indonesia's Electronic Traffic Law Enforcement (ETLE) system. Following Marzuki (2021), normative legal research seeks to establish coherence between legal provisions, legal norms, and fundamental legal principles in addressing specific legal issues. This study adopted statutory and conceptual approaches to examine the applicable regulatory framework and develop legal arguments concerning criminal liability and fault attribution (Marzuki, 2007). The statutory approach focused on the Electronic Information and Transactions Law, Law Number 27 of 2022 concerning Personal Data Protection, and relevant regulations governing electronic systems and traffic law enforcement. Meanwhile, the conceptual approach examined legal doctrines concerning criminal responsibility, the legal status of AI as an electronic agent, and the attribution of fault to individuals or corporate entities.

The legal materials consisted of primary and secondary legal sources collected through documentary and literature review. Primary legal materials included relevant legislation and

regulations, while secondary legal materials comprised academic books, journal articles, legal doctrines, and scholarly publications addressing cybercrime, criminal liability, artificial intelligence governance, and personal data protection (Marzuki, 2007). These materials were systematically examined using grammatical, systematic, and teleological interpretation to determine the meaning, interrelationship, and legislative purposes of the applicable legal provisions. The analysis was conducted prescriptively to assess the applicability of Article 32 paragraphs (1) and (2) of the Electronic Information and Transactions Law and its relationship with personal data protection obligations. This analytical process was directed toward formulating a coherent legal framework that distinguishes intentional electronic data manipulation from technical failures and institutional negligence while ensuring proportional criminal liability and legal certainty.

RESULTS AND DISCUSSION

Criminal Qualification of AI-Assisted Electronic Data Manipulation under the Electronic Information and Transactions Law

The misuse of AI in Indonesia's Electronic Traffic Law Enforcement (ETLE) system raises challenges concerning the qualification of criminal acts, the reliability of electronic evidence, and the attribution of responsibility, since the interconnected infrastructure that processes vehicle images, registration numbers, violation records, and timestamps introduces risks of unauthorized data alteration, algorithmic manipulation, and inaccurate identification when electronic information is deliberately modified to misrepresent a violation or alter an offender's identity (Husada et al., 2026). The principal statutory basis is Article 32 paragraphs (1) and (2) of Law Number 11 of 2008 on Electronic Information and Transactions, as amended by Law Number 19 of 2016 and Law Number 1 of 2024: paragraph (1) covers intentional, unauthorized alterations, destruction, or concealment of electronic information belonging to another or the public, while paragraph (2) addresses unauthorized transfer or movement of such information into an unauthorized system, requiring examination of the actual conduct, the electronic object, the absence of lawful authority, and intent. In the ETLE context, prohibited conduct may include altering registration data, removing violation records, modifying photographic evidence, or transferring records to unauthorized systems—yet the technological sophistication of an intervention does not independently establish liability, which must remain grounded in statutory elements by identifying the human actor who employs the technology (Fajrin et al., 2026).

Crucially, intentional manipulation must be distinguished from technological malfunction: incorrect vehicle identification caused by poor image quality, software failure, or inaccurate classification algorithms does not necessarily constitute a criminal act under Article 32, but may instead indicate operational deficiencies requiring technical correction, administrative investigation, or assessment of other responsibilities, since liability depends on proving an identifiable actor intentionally engaged in prohibited conduct without lawful authority (Wijaya et al., 2025). Accordingly, AI-assisted manipulation must be assessed through a structured examination of both technological processes and legal requirements, with altered electronic information initiating investigation rather than automatically establishing wrongdoing, and investigators determining whether the alteration originated from deliberate human intervention, an authorized system process, an external cyberattack, or an unintended error—a determination that is essential because electronic records pass through multiple systems before use as evidence, and without adequate reconstruction criminal liability risks falling on individuals merely associated with the system rather than participating in the prohibited conduct.

Table 1 Legal Qualification of AI-Assisted Electronic Data Manipulation under Article 32 of the ITE Law

Legal element	Application within ETLE	Required evidentiary assessment
Intentional conduct	Deliberate alteration or unauthorized transfer of ETLE records	Instructions, communications, activity logs, and evidence supporting intent
Without right or unlawfully	Access or actions exceeding legally granted authority	Access permissions, operational authority, and authorization records
Electronic information or documents	Vehicle records, photographic evidence, timestamps, and violation documentation	Identification and authentication of the electronic records

Prohibited interference under Article 32(1)	Alteration, deletion, destruction, or concealment of electronic information	Original records, modification history, forensic examination
Unauthorized transfer under Article 32(2)	Transfer of protected ETLE information to an unauthorized electronic system	Transmission records, recipient-system identification, and access traces
Attribution to an actor	Human involvement in initiating or directing prohibited manipulation	Audit trails, operational responsibilities, and corroborating evidence
Exclusion of technical malfunction	Algorithmic errors occurring without deliberate interference	Technical diagnostics, system testing, and expert assessment

Table 1 demonstrates that the application of Article 32 requires a cumulative assessment of the relevant legal elements rather than reliance on the existence of altered data alone. Technical evidence is important because it may establish how electronic information was changed, but it does not necessarily reveal the legal intention of the responsible person. Similarly, unauthorized access may support an investigation into unlawful interference without independently establishing every element of the offense. The table therefore distinguishes technological indicators from the substantive requirements of criminal responsibility. This approach is consistent with the principle that criminal liability must be established through legally sufficient evidence rather than inferred from the automated nature of the system.

Attribution of Criminal Responsibility to Human Actors and Electronic System Operators

The second major finding concerns the legal status of AI and the attribution of responsibility, since within the examined framework AI is treated as an electronic system or agent rather than an independent subject capable of bearing criminal responsibility—a difficulty arising from its lack of legally recognized criminal personality and independently attributable culpability (Haris & Tantimin, 2022), a position also supported by Sebayang et al. (2024) on AI within Indonesia's criminal justice institutions, so responsibility must focus on the individuals or entities that design, deploy, operate, or control the system. Yet merely identifying a person associated with an AI system is insufficient; the inquiry must determine that person's authority, operational responsibilities, actual conduct, and relationship to the prohibited modification of electronic information, because a developer may possess algorithmic knowledge without access to operational records, an authorized operator may have system access but lack the technical capacity to modify the underlying algorithm, and an administrator may control permissions while remaining unaware of fraudulent instructions entered by another—differences that show why criminal fault attribution must rest on concrete participation and legally relevant culpability.

The analysis thus identifies three potentially responsible categories: technology developers, when evidence establishes intentional participation or another recognized basis of responsibility; operational personnel, when they deliberately alter electronic evidence or knowingly initiate prohibited transfers; and institutional system controllers, who bear responsibilities for governance, authorization, data integrity, and supervision, although institutional failure does not automatically prove the elements of an Article 32 offense (Priyanto et al., 2026). Attribution must also account for Law Number 1 of 2023 concerning the Criminal Code, which entered into force on 2 January 2026 and introduces corporate criminal responsibility relevant where misconduct involves organizational structures, though such responsibility must still be evaluated according to the applicable provisions, the relevant offense, the conditions for attribution, and the time of the conduct, so a company's mere involvement in developing or maintaining ETLE technology cannot independently justify sanctions. This reinforces the need to distinguish individual criminal wrongdoing from institutional negligence—focusing on conduct, authorization, and knowledge where an operator intentionally manipulates evidence, versus administrative or other consequences where the problem stems from inadequate supervision, weak access controls, or ineffective data validation—forms of responsibility that should not be treated as legally interchangeable (Tahir, 2025).

Table 2 Proposed Attribution of Legal Responsibility in AI-Supported ETLE Systems

Involved actor	Scope of control	Potential misconduct	Basis for legal assessment

AI developer	Algorithm design and model configuration	Intentional insertion of data-manipulation functions	Proven participation, knowledge, intent, and applicable offense
System administrator	Access permissions and system maintenance	Unauthorized modification or facilitation of manipulation	Access records, authorization, and conduct
ETLE operator	Verification and processing of traffic records	Deliberate alteration or falsification of electronic evidence	Operational logs, instructions, and proof of intent
Institutional controller	Governance, oversight, and data management	Failure to establish appropriate security and supervision	Statutory duties, organizational responsibility, and applicable liability rules
External unauthorized actor	Illegitimate access or interference	Unauthorized alteration or transfer of ETLE data	Digital forensic evidence and the relevant statutory offense

The framework presented in Table 2 provides a differentiated basis for examining responsibility across the ETLE technological chain. It does not presume that every listed actor is automatically criminally liable when manipulation occurs. Instead, it identifies the types of evidence and legal considerations necessary to determine responsibility according to the role of each actor. Such differentiation is particularly important where technological development, daily operation, and institutional supervision are performed by separate entities. A role-based approach may therefore reduce the risk of arbitrary attribution while preserving the possibility of criminal responsibility where the required elements are proven.

Digital Evidence, Criminal Intent, and the Importance of Audit Trails

A further finding concerns the importance of digital forensic evidence in establishing the relationship between AI-generated modifications and human criminal intent, since electronic information may be modified, duplicated, transferred, or deleted without immediately visible physical traces—characteristics that become especially challenging in an AI-supported ETLE environment involving automated classification, image recognition, database synchronization, and algorithmic decision support, so identifying the origin of a modification requires reconstructing the sequence of technical events rather than merely examining the final displayed information. Digital audit trails are central to this reconstruction, as system logs may record user authentication, access permissions, data modification, and transmission activities, helping determine whether an alteration occurred through an authorized administrative process or prohibited interference; yet an access log does not automatically establish criminal intent, because authentication may be compromised, automated actions misattributed, or records themselves incomplete or manipulated. Accordingly, digital evidence should be examined through mutually reinforcing procedures—preserving the original record, comparing modified information with earlier versions, reviewing system logs and algorithm configurations, and assessing technical infrastructure reliability, with expert testimony where necessary and scrutiny of authenticity, integrity, relevance, and procedural admissibility—since AI-related evidence raises significant challenges for authenticity, transparency, and fair-trial guarantees (Angyalossy & Anděl, 2025).

A crucial distinction separates technical causation from criminal intent: evidence that an AI system generated or modified information establishes a technical event but does not necessarily identify an individual possessing the required intent, so investigators must distinguish evidence explaining how a modification occurred from evidence showing why an identifiable person initiated or knowingly facilitated it—a distinction that becomes essential where software executes previously configured instructions without further human intervention, requiring digital traces to be connected with legally meaningful human conduct (Kian et al., 2026). The legal significance of audit trails also extends to institutional governance, since reliable recordkeeping clarifies whether an incident resulted from deliberate manipulation, unauthorized external access, internal procedural violation, or technical defect, whereas missing or unreliable logs obstruct reconstruction and may justify examining institutional compliance obligations without independently establishing an intentional offense under Article 32. This aligns with the distinction between technological reliability and procedural justice: a system may be

technically accurate yet legally problematic if outputs cannot be independently examined or contested, while algorithmic error does not necessarily invalidate every automated record—what matters is whether the evidence was collected, preserved, and evaluated through legally appropriate procedures, as verification and validation remain essential for protecting due process (Wijayanti et al., 2025), reinforcing that technological efficiency must not replace the evidentiary requirements of criminal proceedings.

Personal Data Protection and Institutional Accountability in AI-Based ETLE

The manipulation of ETLE data also carries significant implications under Law Number 27 of 2022 concerning Personal Data Protection, because electronic traffic enforcement involves information capable of directly or indirectly identifying individuals—particularly when vehicle registration records are linked to personal identity—creating legal responsibilities over collection, use, accuracy, storage, security, and disclosure that AI involvement does not eliminate, since processing remains attributable to recognized controllers or processors (Eddy & Sugianto, 2026). The law requires processing to be lawful, appropriately limited, accurate, secure, and accountable, with Article 16 governing processing principles, Article 35 imposing the controller's duty to protect and secure processed data, and Article 39 addressing unauthorized access, so these obligations must inform the entire operation of AI-supported enforcement rather than only a post-incident response. Such concerns become concrete when a registration number is deliberately replaced (creating an inaccurate association with an unrelated individual), a traffic record is unauthorizedly modified (compromising database integrity), or identifiable records are transferred to an unauthorized system (raising unlawful disclosure concerns)—yet each requires separate examination, because the elements of a criminal offense under the ITE Law are not identical to the requirements governing personal data processing. This yields an important distinction: a controller's failure to maintain accurate information may breach data protection obligations without proving intentional manipulation, and inadequate cybersecurity may expose records to interference without establishing an Article 32 offense, so consequences must turn on the specific provisions violated and supporting evidence (Fikri & Amelia, 2024).

A further consideration is the management of protection failures, since Article 46 imposes notification obligations when a personal data protection failure occurs, meaning an ETLE incident involving unauthorized alteration, loss, or disclosure of identifiable information may require assessing whether the legal conditions for notification are satisfied—though such failure must be evaluated independently of the criminal elements governing intentional electronic data manipulation. Institutional accountability likewise requires examining the relationship between technological design and organizational decision-making, because an institution may use AI to improve violation detection while retaining responsibilities for data validation, authorized access, security monitoring, and correction mechanisms—duties that are especially weighty where automated results support decisions affecting individuals' legal rights, given that algorithmic decision-making in law enforcement requires explanation and accountability to preserve procedural legitimacy (Yang, 2023). Accordingly, an accountable ETLE system should combine technological safeguards with administrative procedures allowing potentially inaccurate evidence to be reviewed and corrected.

Table 3 Relationship Between ETLE Data Manipulation and Personal Data Protection Obligations

Data protection principle	Potential risk in ETLE	Relevant legal assessment
Lawfulness of processing	Processing or disclosure without a valid legal basis	Determine whether processing complies with applicable authorization requirements
Data accuracy	Incorrect association between a vehicle, individual, and alleged violation	Examine validation, accuracy, and correction procedures
Purpose limitation	Use of traffic enforcement records for unrelated purposes	Assess consistency with the authorized purposes of processing
Data security	Unauthorized modification, deletion, or access	Evaluate technical and organizational safeguards

Controller accountability	Inadequate supervision or insufficient records of processing activities	Examine compliance with statutory controller obligations
Incident notification	Failure to provide required notice following a qualifying data protection failure	Assess the applicability of Article 46
Criminal responsibility	Deliberate manipulation or unauthorized transfer of electronic information	Separately evaluate the elements of relevant criminal offenses

Table 3 demonstrates that personal data protection obligations operate alongside, but are not identical to, the criminal provisions governing electronic information manipulation. The table identifies the principal areas where an ETLE incident may generate more than one legal question. For example, deliberately changing a traffic record may require examination under Article 32 of the ITE Law while also raising concerns concerning data accuracy and processing security. However, the existence of overlapping concerns does not justify treating administrative violations as conclusive evidence of criminal intent. The appropriate approach is to examine the legal requirements of each applicable provision independently while considering their factual relationship within the same incident.

Integrating Criminal Liability, Data Protection, and Algorithmic Governance

The relationship between the ITE Law and the Personal Data Protection Law calls for an integrated approach to legal accountability in AI-supported ETLE, since the former frames prohibited interference with electronic information while the latter governs the lawful and secure processing of identifiable data—regimes addressing different dimensions of misconduct that overlap when manipulation involves personal data, so effective analysis must identify the conduct, the applicable provisions, the actor's role, and the supporting evidence to avoid conflating criminal wrongdoing with technical errors or administrative deficiencies. This perspective matters because AI-supported enforcement spans multiple stages (surveillance capture, automated recognition, verification, and enforcement decision), each carrying distinct functions, responsibilities, and points of possible interference, so liability depends on where the alteration occurred and who held authority or control, conceptualizing accountability as a relationship among statutory duties, human conduct, technical evidence, and institutional arrangements. Preventive governance should thus complement criminal enforcement through strong access controls, reliable logging, independent verification, and integrity assessments—not as substitutes for criminal law but as safeguards supporting lawful administration, an alignment of technology with institutional readiness that Rigo et al. (2025) identify as essential amid Indonesia's ETLE legal and institutional challenges. Accountability also requires balancing enforcement interests with individual rights, since legitimacy depends on reliability and fairness and affected persons must have access to verification and correction procedures, a due-process and algorithmic-justice concern emphasized by Husada et al. (2026).

Doctrinally, the proposed framework distinguishes three categories: intentional and unauthorized interference with electronic information (assessed under the relevant criminal offense), failures in personal data governance (assessed under the Personal Data Protection Law), and technical or operational failures (requiring administrative correction or system improvement without necessarily establishing intentional wrongdoing)—a separation essential to preserving the principle that punishment must rest on proven legal requirements rather than generalized assumptions about technological risk. Integrating these categories contributes conceptually to debates on AI-related criminal responsibility, which have variously addressed AI as an instrument of crime, algorithmic decision-making, evidentiary reliability, and data protection, by linking the elements of the relevant criminal provisions to the responsibilities of controlling and processing personal information within Indonesian ETLE, yielding a framework that emphasizes proportionality, verifiable attribution, and the preservation of procedural safeguards.

CONCLUSION

This study concludes that criminal liability for the misuse of artificial intelligence in electronic data manipulation within Indonesia's Electronic Traffic Law Enforcement (ETLE) system must be attributed to legally recognized individuals or corporate entities rather than AI itself. The application of Article 32 paragraphs (1) and (2) of the Electronic Information and Transactions Law requires proof of

prohibited conduct, unlawfulness, criminal intent, and the involvement of identifiable actors. Digital audit trails, system activity logs, algorithmic configurations, and forensic examinations are essential for establishing the relationship between electronic manipulation and human conduct. Nevertheless, technical malfunctions, algorithmic inaccuracies, and institutional negligence cannot automatically be classified as intentional criminal offenses. Therefore, criminal responsibility must be determined proportionally according to each actor's authority, involvement, control, and proven culpability.

Furthermore, electronic data manipulation within the ETLE system is closely related to personal data protection obligations under Law Number 27 of 2022, particularly concerning lawfulness, accuracy, security, purpose limitation, and controller accountability. Although violations of these obligations do not automatically establish criminal liability under the Electronic Information and Transactions Law, they provide relevant grounds for assessing institutional negligence and other applicable legal responsibilities. This study proposes an integrated legal accountability framework that connects criminal fault attribution, electronic evidence verification, and personal data protection compliance. Accordingly, government authorities and electronic system operators should strengthen regulatory harmonization, human oversight, digital audit mechanisms, and institutional security standards. These measures are essential for ensuring legal certainty, proportional criminal accountability, procedural fairness, and the protection of individual rights in Indonesia's increasingly automated traffic enforcement system.

REFERENCES

Ajisaka, D., & Delano, T. (2026). *Pertanggungjawaban Pidana dalam Kecelakaan Lalu Lintas yang Melibatkan Kendaraan Otonom: Tantangan Atribusi Kesalahan*. *3*(3). https://doi.org/10.71153/jimmi.v3i3.683

Angyalossy, P., & Anděl, D. (2025). *The Impact of AI on Evidence in Criminal Proceedings*. https://scispace.com/papers/the-impact-of-ai-on-evidence-in-criminal-proceedings-cgxvxg68fsse

Arifudin MZ, M., & Bima, M. C. (2026). Legalitas Bukti Digital Berbasis Kecerdasan Buatan dalam Proses Peradilan. *Jurnal Hukum, Politik Dan Ilmu Sosial*. https://scispace.com/papers/legalitas-bukti-digital-berbasis-kecerdasan-buatan-dalam-e9jppxchdyf6

Eddy, A. S., & Sugianto, F. (2026). Implementation of Personal Data Protection Against Wrongful Ticketing in the Electronic Law Enforcement System. *International Journal of Social Service and Research*. https://scispace.com/papers/implementation-of-personal-data-protection-against-wrongful-cuhz5nni1wjn

Fajrin, N., Suryani, A. I., & Rato, D. (2026). Legal Certainty of Criminal Responsibility for Artificial Intelligence Scam through Electronic Communications in Indonesia. *Rechtenstudent Journal*. https://scispace.com/papers/legal-certainty-of-criminal-responsibility-for-artificial-nonf97su3al1

Fikri, A., & Amelia, T. (2024). Indonesia’s Legal Policy on Protecting Personal Data from Artificial Intelligence Abuse. *SHS Web of Conferences*. https://scispace.com/papers/indonesias-legal-policy-on-protecting-personal-data-from-6nhems9ykxvz

Haris, M. T. A. R., & Tantimin, T. (2022). Analisis Pertanggungjawaban Hukum Pidana terhadap Pemanfaatan Artificial Intelligence di Indonesia. *Jurnal Komunikasi Hukum*, *8*(1). https://doi.org/10.23887/jkh.v8i1.44408

Husada, A., Parmono, B., & Hidayati, R. (2026). Ensuring Fairness in Automated Traffic Enforcement: Examining Algorithmic Justice and Due Process in Malang’s ETLE System. *Bulletin of Community Engagement*, *6*(2). https://scispace.com/papers/ensuring-fairness-in-automated-traffic-enforcement-examining-c4r7ojrkt9gb

Kian, A. M. L., Karo Karo, R. P. P., & Gaol, S. L. (2026). Reconstructing Cyber Mens Rea Through Electronic Evidence and Algorithmic Accountability. *Jurnal Ius Constituendum*. https://scispace.com/papers/reconstructing-cyber-mens-rea-through-electronic-evidence-falxmkgkbmm7

Marzuki, P. M. (2007). *Penelitian Hukum*. Kencana Prenada Media Group.

Mecca, A. S. P., Hidaya, W. A., & Tuasikal, H. (2025). Pemanfaatan Teknologi Kecerdasan Buatan (Artificial Intelligence) dalam Sistem Peradilan Pidana di Indonesia. *Jurnal Sosial Dan Teknologi*, *5*(6). https://doi.org/10.59188/jurnalsostech.v5i6.32207

Priyanto, A., Sanjaya, F., & Eryke, H. (2026). Reconstruction of Criminal Liability Doctrine in the Artificial Intellegence Ecosystem in Indonesia: Analysis of Norms' Vapor, Reinterpretation of Mens Rea and Hybrid Liability Model Based on Subtantive Justice. *Sosioedukasi: Jurnal Ilmiah Ilmu Pendidikan Dan Sosial*. https://scispace.com/papers/reconstruction-of-criminal-liability-doctrine-in-the-316fii1k637g

Rigo, S., Rudagi, R., & Diani, S. W. (2025). Analisis Yuridis dan Kelembagaan terhadap Implementasi Tilang Elektronik: Studi Literatur. *Pendas: Jurnal Ilmiah Pendidikan Dasar*. https://scispace.com/papers/analisis-yuridis-dan-kelembagaan-terhadap-implementasi-nmtqunwttkmo

Sebayang, E. K., Mulyadi, M., & Ekaputra, M. (2024). Potensi Pemanfaatan Teknologi Artificial Intelligence sebagai Produk Lembaga Peradilan Pidana di Indonesia. *Locus Journal of Academic Literature Review*, *3*(4). https://doi.org/10.56128/ljoalr.v3i4.311

Tahir, Ach. (2025). Challenges of Criminal Liability Related to Artificial Intelligence (AI) in Indonesia: Lessons from European Law. *Jurisprudentie: Jurusan Ilmu Hukum Fakultas Syariah Dan Hukum*. https://scispace.com/papers/challenges-of-criminal-liability-related-to-artificial-ky7y1e5k7if2

Wijaya, F. N., Saputro, W. G., & Henda, R. (2025). Due Process of Law in Verification and Validation of Electronic Evidence on the Use of Fake Motor Vehicle Registration Numbers in the Enforcement of Etilang. *Journal of World Science*. https://scispace.com/papers/due-process-of-law-in-verification-and-validation-of-gyafp8n0t9ku

Wijayanti, E., Prasetiawati, E., & Sugiatro. (2025). Interpretasi ayat-ayat huzn (depresi) perspektif psikologi Abu Zayd al-Balkhi (w. 934 M). *Semiotika-Q*, *5*(2), 667–688. https://doi.org/10.19109/jsq.v5i2.27801

Yang, L. (2023). *Application and Regulation of Algorithm Technology in Automated Decision Making for Law Enforcement*. https://scispace.com/papers/application-and-regulation-of-algorithm-technology-in-2tvcpz48g0