GIJLSS
Greenation International Journal of Law and Social Sciences
+62 81210467572 https://research.e-greenation.org/GIJLSS greenation.info@gmail.com
GREENATION RESEARCH

DOI: https://doi.org/10.38035/gijlss.v3i3

Utilization of Artificial Intelligence in Cybercrime Investigation Process and Protection of Suspects' Human Rights

Chitto Cumbhadrika[1], KMS Herman[2]
[1]Universitas Borobudur, Jakarta, Indonesia, cumbhadrika@yahoo.com
[2]Universitas Borobudur, Jakarta, Indonesia, kms_herman@borobudur.ac.id

Corresponding Author: cumbhadrika@yahoo.com[1]

Abstract: The use of artificial intelligence (AI) in cybercrime investigations presents an opportunity to increase the effectiveness of law enforcement through digital forensic analysis, crime pattern detection, and electronic evidence processing. However, the application of AI also raises legal challenges, particularly regarding the validity of evidence, the principle of chain of custody, and potential violations of suspects' human rights, such as the right to privacy and the right to legal counsel, as guaranteed in Law Number 1 of 2024 concerning Electronic Information and Transactions, Law Number 27 of 2022 concerning Personal Data Protection, Law Number 8 of 1981 concerning the Criminal Procedure Code, and Law Number 1 of 2023 concerning the Criminal Code. A normative legal analysis shows that current regulations do not specifically regulate the mechanisms for using AI in investigations, thus creating legal uncertainty and the risk of algorithmic bias that could harm suspects. Therefore, legal reforms are needed in the form of developing technical guidelines, AI system audit standards, and specific regulations that balance the effectiveness of law enforcement with the protection of human rights. Harmonizing technology, due process principles, and human rights protection will ensure that the use of AI not only improves investigative capacity but also strengthens legal certainty and the legitimacy of criminal justice processes in the digital era.

Keywords: Artificial Intelligence, Investigation, Crime, Information Technology Crime

INTRODUCTION

The development of artificial intelligence (AI) technology has changed the paradigm of cybercrime investigation in Indonesia (Budiman, 2022). AI enables the analysis of large amounts of digital data, the detection of attack patterns, and the identification of perpetrators through various electronic traces (Rustiyana, 2025). This change requires investigators to master technological competencies while understanding its legal implications. AI technology is not merely a tool but also has the potential to create new legal consequences if its analysis results are used as the basis for unsupervised investigative actions (Mecca, 2025). This phenomenon emphasizes the importance of balancing investigative effectiveness with human rights protection.

AI in cybercrime investigations can help authorities unravel the relationships between complex digital data (Dzaky, 2025). Machine learning, facial recognition, and predictive analytics systems enable the identification of behavioral patterns that are difficult to detect manually (Ramadhan, 2024). These advantages present opportunities to increase the effectiveness of law enforcement. However, the speed and analytical capacity of AI pose a risk of algorithmic error and bias. Article 5 of the ITE Law, in conjunction with Law No. Law No. 1 of 2024 recognizes electronic information as valid evidence, but this evidence must be accountable (Mursyid, 2025).

The validity of AI-generated electronic evidence is a central issue in the legal process. Article 184 paragraph (1) of the Criminal Procedure Code stipulates that valid evidence consists of witness testimony, expert testimony, letters, clues, and the defendant's testimony (Helmawansyah, 2021). AI produces digital evidence that is sometimes difficult to verify manually, creating legal uncertainty. This ambiguity has the potential to violate the principle of due process of law (Rosyadi, 2025). This principle must be upheld to prevent AI results from causing injustice to suspects.

AI systems have the potential for bias because they are trained using historical data that may contain inequalities (Kushariyadi, 2024). Algorithmic bias can lead to differential treatment of certain suspects, violating the principle of equality before the law (Article 27 paragraph (1) of the 1945 Constitution of the Republic of Indonesia) (Ariyadi, 2025). These risks require controls, audits, and accountability standards for the use of AI. Without oversight, AI analysis results could justify investigative actions that unfairly harm individuals (Maimun, 2025). The principle of justice requires transparency and accuracy in the use of intelligent technology.

The human rights of suspects are a crucial consideration in technology-based investigations (Iman, 2025). Article 28G paragraph (1) of the 1945 Constitution of the Republic of Indonesia guarantees the right to personal protection, honor, and security. Article 54 of the Criminal Procedure Code states that suspects have the right to legal counsel from the beginning of the investigation (Yuserlina, 2021). AI used without regard for these rights can lead to violations of privacy and the right to legal defense (Nirwan, 2025). Law enforcement must ensure that technology does not diminish or violate the basic rights of suspects.

Personal data privacy is a critical issue in digital investigations (Agustin, 2024). Law No. 27 of 2022 concerning Personal Data Protection, Article 20 paragraph (1), emphasizes that data processing must be lawful and appropriate for its intended purpose. AI that accesses personal information without a legal basis can violate a suspect's right to privacy. Data integrity and information security are absolute requirements, as stipulated in Article 35 of the Privacy and Data Protection Law, which requires data controllers to protect data from leaks or misuse (Usman, 2024). Suspects have the right to protection against unauthorized analysis.

Cybercrimes are regulated in the ITE Law in conjunction with Law No. 1 of 2024, including illegal access (Article 30), unauthorized interception (Article 31), data manipulation (Article 32), and the distribution of prohibited content (Article 27) (Maesaroh, 2024). Cybercrimes are cross-jurisdictional and complex, requiring sophisticated analytical methods (Aini, 2024). Digital evidence is scattered across various platforms, posing challenges in collection and verification. These crimes often utilize disguise techniques, VPNs, or encryption, complicating the identification of perpetrators (Butarbutar, 2023). AI technology is a potential solution for tracing criminal patterns and networks.

Violations of suspects' human rights can occur if AI is used without control. AI that assesses suspects based on digital data can lead to the assumption of guilt before manual verification, which violates the principle of presumption of innocence (Hardhika, 2023). It

requires transparency and auditing of AI systems. Human rights protection must be a reference point in every stage of technology-based investigations (Pratama, 2024).

Law No. 1 of 2023 concerning the Criminal Code regulates technology-based crimes, including the destruction of electronic systems (Articles 331–334). This provision emphasizes the adaptation of criminal law to digital developments. However, the Criminal Code (KUHP) does not yet regulate procedures for the use of AI in the provision of evidence, creating uncertainty in investigative practices. Existing regulations provide a criminal basis but fail to address the technical and ethical aspects of AI. This emphasizes the need for additional guidelines for the safe and legal integration of AI.

The ITE Law, in conjunction with Law No. 1 of 2024, provides investigators with the opportunity to seek assistance from information technology experts (Article 43 paragraph (6)). This provision provides a basis for the use of intelligent technology as an assistive device, but does not establish standards for system accuracy or accountability. This regulatory gap requires attention to prevent arbitrary use of AI. Technical standards and system audits are crucial to ensure the accountability of digital evidence. Law enforcement must still adhere to the principles of due process and human rights protection.

Minister of Communication and Information Technology Circular Letter No. 9 of 2023 concerning the Ethics of Artificial Intelligence emphasizes transparency, accountability, and algorithmic fairness. These guidelines serve as an ethical reference for the use of AI, although they are not yet legally binding. These principles are relevant for law enforcement officials to ensure that the use of AI does not harm suspects. These ethical standards also support the harmonization of technological advancements and the protection of individual rights. Implementing these guidelines is the first step in regulating the safe and legitimate use of AI.

The overall legal framework demonstrates that Indonesia already has a legal basis for the use of digital evidence and AI in general. The ITE Law, in conjunction with Law No. 1 of 2024, the Privacy and Personal Data Protection Law, the Criminal Procedure Code, and the Criminal Code, provides the normative foundation, while the Circular Letter of the Minister of Communication and Information Technology provides ethical guidelines. The main challenges lie in the technical mechanisms, system audits, and accountability for the use of AI. Protecting the human rights of suspects must remain a primary focus to ensure that the investigation process does not lead to injustice. The integration of law, technology, and human rights principles will ensure that cybercrime investigations are effective and legitimate.

METHOD

This research is a normative juridical method employing a statutory and conceptual approach. The statutory approach employed to examine positive legal norms governing the use of artificial intelligence (AI) in the criminal justice system, particularly at the stage of cybercrime investigation. The analysis is conducted on the provisions of Law Number 11 of 2008 concerning Electronic Information and Transactions, as amended by Law Number 1 of 2024, Law Number 8 of 1981 concerning Criminal Procedure Law, and other relevant derivative regulations. The conceptual approach is used to understand and formulate new legal ideas related to the integration of AI technology into fair investigative practices, with reference to legal doctrine, general principles of good governance, and the principle of human rights protection. Through the combination of these two approaches, this study seeks to find a balance between technological innovation and legal certainty and offers a regulatory framework that can accommodate technological developments without neglecting the values of justice and ethical responsibility in law enforcement.

RESULT AND DISCUSSION

Utilization of Artificial Intelligence in Cybercrime Investigations

The use of artificial intelligence (AI) by law enforcement has introduced new methods in cybercrime investigations. AI is used to trace the digital footprints of perpetrators through the analysis of large data scattered across various electronic platforms. The technique enables the identification of attack patterns that were previously difficult to uncover manually. Facial recognition is used to detect and verify the identity of suspects based on digital video recordings or photos. Crime prediction using algorithms is also beginning to be applied to analyze potential criminal risks based on historical patterns.

The Cyber Crime Directorate of the National Police's Criminal Investigation Agency (Bareskrim Polri) is one example of AI implementation in Indonesia. Their AI system includes digital data forensic analysis and the detection of the distribution of prohibited content. This analysis accelerates the process of identifying electronic evidence and connecting perpetrator networks spread across platforms. The use of this technology also helps investigators determine the next steps in the investigation more precisely. This case study demonstrates the effectiveness of AI in supporting the investigative process, but it still requires professional oversight.

The validity of AI-generated electronic evidence is a primary focus in law enforcement. Article 5 of the ITE Law, in conjunction with Law No. 1 of 2024, stipulates that electronic information and/or electronic documents can be used as valid legal evidence. Article 184, paragraph (1) of the Criminal Procedure Code also recognizes expert testimony and written evidence as legal evidence. The output of AI-generated algorithms must be explainable, verifiable, and accountable to meet the criteria for valid evidence. Unclear algorithmic calculations or decisions can give rise to legal debate in court.

The validity of digital evidence often faces technical and legal challenges. Complex algorithms are sometimes difficult for judges or those assessing the evidence to understand. It poses the risk that AI results will be rejected or their validity questioned. The availability of complete documentation and an explanation of the AI methodology is crucial for verifying evidence. The lack of explanation can disadvantage suspects and create legal uncertainty.

Digital chain of custody is a crucial principle for maintaining the authenticity of electronic evidence. Digital evidence processed by AI must be systematically recorded to ensure its integrity. Every step in data processing must be documented, including the handling, storage, and transfer of electronic information. This principle aligns with the provisions of the ITE Law, particularly Article 5 paragraphs (1) and (2), which recognize the validity of electronic information as legal evidence, and Articles 32 and 48, which emphasize the prohibition on altering or damaging the integrity of electronic data. Investigators have a responsibility to ensure that digital evidence is not modified or lost during the investigation process.

Investigators' responsibilities include recording every AI data processing activity. This documentation serves as a basis for accountability if questions arise regarding the process or results of the analysis. A transparent and auditable AI system helps maintain the credibility of evidence. Every change or input to data must be clearly recorded to avoid any doubt in court. This practice supports the principle of due process and protects the rights of suspects.

The risk of algorithmic bias is a key legal challenge in the use of AI. Algorithms trained with historical data can replicate previous inequalities or errors. It can result in unfair decisions against specific suspects. Algorithmic bias can impact crime predictions and perpetrator identification. Understanding AI data sources and methodologies is crucial to mitigating the risk of injustice.

Identification errors also pose a significant risk. Facial recognition, for example, can misidentify individuals due to image quality or similarity in facial features. This error can

lead to inaccurate investigations. Manual validation is still necessary to ensure AI results are correct and accurate.

Protecting suspects' privacy rights also faces challenges with the use of AI. AI can process sensitive information that should not be accessed without permission. Article 20, paragraph (2) of Law No. 27 of 2022 emphasizes that data processing must be lawful and for a clear purpose. Failure to comply with this provision could harm suspects and lead to human rights violations. Ethical and legal aspects are key to ensuring that the use of AI does not violate suspects' rights.

AI usage presents both complex opportunities and risks for cybercrime investigations. This technology can improve the effectiveness of law enforcement, but it must still maintain accuracy, accountability, and the protection of suspects' rights. Investigators must balance the use of AI with applicable legal principles, including the Criminal Procedure Code (KUHAP), the ITE Law in conjunction with Law No. 1 of 2024, the PDP Law, and the Criminal Code. Chain of custody documentation, evidence validity, and algorithm audits are crucial components. This legal challenge demands high awareness and competence from law enforcement officers so that the investigation process remains legal and fair.

Legal Analysis and Recommendations for Strengthening Regulations

The current regulatory framework does not specifically regulate the operational mechanisms of artificial intelligence (AI) in cybercrime investigations. The ITE Law, in conjunction with Law No. 1 of 2024, provides a legal basis for the use of electronic information as evidence, but does not include detailed procedures for AI analysis. The PDP Law regulates personal data protection, including the processing of sensitive information, but does not mention automated algorithms in investigative practice. The Criminal Procedure Code (KUHAP) and the Criminal Code (KUHP) provide a criminal and procedural legal basis, but they are still general and have not adapted to the challenges of modern technology. This gap in norms creates legal uncertainty and the potential risk of violations of suspects' human rights.

An evaluation of the integration between the ITE Law, the PDP Law, the Criminal Procedure Code, and the Criminal Code reveals gaps in the implementation of AI. Each regulation has a different focus, resulting in fragmented legal norms. Electronic evidence generated by AI requires technical validation, while the PDP Law emphasizes consent and the purpose of data processing. The Criminal Procedure Code regulates investigative procedures and the rights of suspects, but does not provide practical guidelines for the use of AI. This fragmentation makes it difficult for law enforcement officials to balance the effectiveness of investigations with the protection of suspects' rights.

The use of AI without transparency has the potential to violate the principle of due process of law. Suspects must have legal certainty regarding the investigative methods and the basis for decisions made by automated systems. The ambiguity of AI algorithms or predictive decisions can lead to the assumption of guilt before the court has assessed the facts. Transparency in AI operations is a prerequisite for ensuring the protection of suspects' human rights.

The accountability of investigators and the responsibility of AI system developers are important legal issues. Investigators are responsible for using technology to gather evidence. AI system developers also play a crucial role in ensuring algorithms function accurately and fairly. Failure to comply with technical standards can result in legal consequences. Separation of responsibilities between law enforcement and technology providers is crucial for reducing the risk of errors and human rights violations.

A comparative analysis with the European Union demonstrates strict AI regulation through the EU AI Act. This regulation establishes standards for AI use, audits, and risk

assessments for systems used by the public and law enforcement. The United States, through its AI Bill of Rights, emphasizes individual rights, algorithm transparency, and the accountability of technology providers. Japan, through its AI Ethics Guidelines, emphasizes ethics, safety, and individual privacy rights in the use of AI. The comparative study delivers important lessons for Indonesia regarding the importance of clear and comprehensive regulations.

The implementation of international practices highlights the need for technical and ethical audits of AI systems. These audit standards include algorithm validation, documentation of automated decisions, and error correction mechanisms. Regular audits can prevent algorithmic bias and misidentification of suspects. This process aligns with the principle of due process and the right to justice for every individual. An independent oversight body can strengthen these mechanisms to ensure law enforcement remains accountable and transparent.

The development of specific regulations or implementing regulations for the ITE Law in conjunction with Law No. 1 of 2024 is a strategic step. These regulations should contain operational standards for the use of AI in investigations, including evidence validation procedures and provisions for algorithm audits. Additional regulations should address documentation, the digital chain of custody, and the responsibilities of investigators and technology developers. Clear legal certainty will protect suspects from potential human rights violations. These operational standards will also facilitate law enforcement in implementing the technology legally and effectively.

Ethical and technical audits are essential to ensure AI operates in accordance with the law and human rights principles. Technical audits examine the accuracy, data security, and robustness of algorithms, while ethical audits assess the impact on the rights of suspects and the public. This combined audit helps identify bias, prediction errors, and privacy violations. Audit results can serve as a basis for improving legal systems and documentation. Audit practices also enhance the legitimacy of AI use in the eyes of the public and the courts.

The establishment of an independent oversight body is a crucial strategy for human rights protection. This body is tasked with monitoring the use of AI by law enforcement officials, assessing compliance with regulations, and receiving complaints from the public or suspects. The independent oversight function prevents the misuse of automated systems and strengthens accountability. This body can collaborate with data authorities, academics, and human rights organizations for regular evaluations. This mechanism ensures that technological innovation does not compromise citizens' fundamental rights.

The overall analysis demonstrates the need for harmonization between technology, law, and human rights. Existing regulations provide a normative foundation, but they are insufficient to regulate the detailed operation of AI. Technical and ethical audits, operational standards, and independent oversight are crucial instruments for balancing the effectiveness of investigations with the protection of suspects. Integrating these three aspects will ensure that the use of AI supports lawful, fair, and transparent law enforcement. This approach ensures that suspects' human rights remain protected despite the increasing complexity of technology.

CONCLUSION

The use of artificial intelligence (AI) in cybercrime investigations offers significant opportunities to increase the effectiveness of law enforcement by accelerating data analysis, detecting crime patterns, and tracing complex digital footprints. This technology enables law enforcement officials to work more efficiently in identifying perpetrators and accurately processing electronic evidence. However, the application of AI also carries significant legal consequences, particularly regarding the validity of evidence, the responsibility of

investigators, and the protection of suspects' human rights. The absence of regulations explicitly governing the use of AI in investigations creates legal uncertainty and risks violating the principles of due process of law, the presumption of innocence, and the right to privacy as guaranteed by the 1945 Constitution of the Republic of Indonesia, the Criminal Procedure Code, the Electronic Information and Transactions Law in conjunction with Law No. 1 of 2024, and the Personal Data Protection Law. This situation underscores the urgency of legal reforms that adapt to technological developments to ensure substantive justice in the digital era.

The government needs to immediately develop technical guidelines and audit standards for AI systems used in cybercrime investigations to ensure the reliability, transparency, and accountability of their results. New regulations must harmonize effective law enforcement with the principles of human rights protection, including independent oversight mechanisms for the use of automated systems by law enforcement officials. In addition to regulatory aspects, enhancing investigators' capacity in digital ethics, responsible use of technology, and understanding the risks of algorithmic bias are crucial steps to prevent the misuse of AI. Implementation of technology should not only be oriented towards efficiency but also ensure justice and legal certainty for all parties. Integrating technology, law, and humanity is key to ensuring investigations in the era of artificial intelligence remain within the legal framework, are fair, transparent, and respectful of human dignity.

REFERENCES

Agustin, S. (2024). Dampak Kemajuan Teknologi Informasi Era Digital Terhadap Keamanan Data Pribadi Tantangan Dan Penanggulangan Terhadap Kejahatan Cyber. *Jurnal Penelitian Multidisiplin Bangsa, 1*(6), 500-504.

Aini, N., & Lubis, F. (2024). Tantangan Pembuktian Dalam Kasus Kejahatan Siber. *Judge: Jurnal Hukum*, 5(02), 55-63.

Ariyadi, F. (2025). Algorithmic Bias Dalam Restorative Justice: Ancaman Bagi Marginal. *National Multidisciplinary Sciences, 4*(3), 148-158.

Budiman, M. A. (2022). Penggunaan Agen Berbasis Intelijen Untuk Menangani Kejahatan Siber. *Journal of Innovation Research and Knowledge, 1*(8), 455-462.

Butarbutar, R. (2023). Kejahatan siber terhadap individu: Jenis, analisis, dan perkembangannya. *Technology and Economics Law Journal, 2*(2), 3.

Dzaky, M. A. T., & Edrisy, I. F. (2025). *Strategi Pencegahan Kejahatan Siber di Indonesia: Sinergi antara UU ITE dan Kebijakan Keamanan Digital. PESHUM: Jurnal Pendidikan, Sosial dan Humaniora,* 4(2), 3614–3625.

Hardhika, R. (2023). Transformasi Digital Wajah Peradilan: Peran Artificial Intelligence Dalam Penguatan Integritas. *Judex Laguens, 1*(2), 341-380.

Helmawansyah, M. (2021). Penggunaan Barang Bukti Elektronik yang Dijadikan Alat Bukti dalam Perkara Pidana. *Journal of Law (Jurnal Ilmu Hukum), 7*(2), 527-541.

Iman, M., & Firdaus, A. (2025). Akselerasi Teknologi: Konsep Pengawasan Penyidikan Menggunakan Sistem Eletronik. *National Multidisciplinary Sciences,* 4(3), 52-57.

Kushariyadi, K. AKushariyadi, K., Apriyanto, H., Herdiana, Y., Asy'ari, F. H., Judijanto, L., Pasrun, Y. P., & Mardikawati, B. (2024). *Artificial intelligence: Dinamika perkembangan AI beserta penerapannya.* Jambi: PT. Sonpedia Publishing Indonesia.

Maesaroh, R. S. (2024). Tantangan Keamanan Siber dan Implikasinya terhadap Hukum Kenegaraan: Tinjauan atas Peran Negara dalam Menjamin Ketahanan Digital. *Staatsrecht: Jurnal Hukum Kenegaraan dan Politik Islam, 4*(2), 255-274.

Maimun, A. &. (2025). Penggunaan Ai Dalam Proses Pemeriksaan Tersangka Dalam Penyidikan Di Kepolisian. *National Multidisciplinary Sciences, 4*(3), 33-40.

Mecca, A. S. P., Hidaya, W. A., & Tuasikal, H. (2025). *Pemanfaatan Teknologi Kecerdasan Buatan (Artificial Intelligence) dalam Sistem Peradilan Pidana di Indonesia. Jurnal Sosial Teknologi,* 5(6).

Mursyid, M. P. (2025). Rekonstruksi Peran Digital Forensik Dalam Penyidikan Tindak Pidana Siber: Analisis Kritis Terhadap Konstruksi Hukum Pidana di Indonesia. *Jurnal Tana Mana, 6*(2), 289-296.

Nirwan, D., & Sampurna, A. (2025). *Menyelaraskan Teknologi dengan Perlindungan Hak Privasi. Juris Prudentia: Jurnal Hukum Ekselen,* 7(2).

Pratama, M. A. (2024). Kompromi Etis dalam AI Generatif Memetakan Konflik Nilai Keadilan, Transparansi, dan Utilitas. *Judge: Jurnal Hukum, 5*(02), 220-229.

Ramadhan, G. R. (2024). Penerapan Machine Learning Dalam Pengenalan Wajah Untuk Sistem Keamanan. *Jurnal Dunia Data, 1*(4).

Rosyadi, S. Y. (2025). Pembaruan Hukum di Era Digital: Aspek Hukum terhadap Validitas Hasil Analisis Artificial Intelligence Sebagai Alat Bukti Dalam Penegakan Hukum Pidana Pertambangan. *Judge: Jurnal Hukum, 6*(03), 563-577.

Rustiyana, R. J. (2025). *Pemanfaataan AI dalam Keamanan Siber.* Jambi: PT. Sonpedia Publishing Indonesia.

Usman, N. &. (2024). Perlindungan Hukum Data Pribadi dan Pertanggungjawaban Otoritas Terhadap Keamanan Siber Menurut Tinjauan UU PDP. *DOKTRINA: JOURNAL OF LAW, 7*(2), 178-201.

Yuserlina, A. (2021). Pelaksanaan Pemberian Bantuan Hukum Pada Tingkat Penyidikan Berdasarkan Kitab Undang-Undang Hukum Acara Pidana (KUHAP) Di Wilayah Hukum Polres Bukittinggi. *Ensiklopedia Social Review, 3*(2), 237-246.