Jurnal Daulat Hukum
Volume 8 No.4, December 2025
ISSN: 2614-560X
SINTA 3 Decree No. 0547/ES/DT.05.00/2024
Dated May 15, 2024

Misuse of Artificial Intelligence in Cybercrime: Criminal Liability and Electoral Integrity

Hadi Jumhadi[1)] & Dini Dewi Heniarti[2)]
[1)]Faculty of Law, Universitas Islam Bandung (UNISBA), Indonesia Indonesia, E-mail: nizamputra2009@gmail.com
[2)]Faculty of Law, Universitas Islam Bandung (UNISBA), Indonesia, E-mail: diniheniarti@unisba.ac.id

Abstract. *This study examines the misuse of artificial intelligence (AI) from the perspective of cybercrime and its implications for electoral integrity. The rapid development of AI has transformed cybercrime from conventional, human-centered acts into autonomous, large-scale, and structurally complex operations capable of manipulating public perception and democratic processes. This research aims to analyze the characteristics of AI-enabled cybercrime in elections, assess the applicability of the classical concept of mens rea in crimes involving autonomous systems, and formulate adaptive models of criminal liability in response to these challenges. The study employs a qualitative legal research method with a normative and conceptual approach. Data are collected through library research using primary legal materials in the form of statutory regulations and secondary legal materials consisting of scholarly articles, legal doctrines, and relevant academic publications. The analysis is conducted through descriptive-analytical techniques, legal interpretation, and conceptual analysis. The findings demonstrate that AI-driven cybercrime creates ontological and epistemological challenges for criminal law, particularly in attributing intent and responsibility. As AI cannot be recognized as a legal subject, criminal liability must be reconstructed and directed toward human and institutional actors through layered and contextual liability models. The novelty of this research lies in its integration of mens rea theory with the structural characteristics of AI-enabled cybercrime, offering a proactive and anticipatory criminal law framework to safeguard electoral integrity in the digital era.*

Keywords: *Artificial Intelligence; Cybercrime; Criminal; Electoral; Mens rea.*

1. Introduction

The rapid development of information technology has fundamentally transformed the nature of crime, shifting it from physical spaces to digital environments. This transformation is evident in the escalation of cybercrime, which has evolved beyond conventional hacking into

systematic manipulation of information and large-scale attacks on digital infrastructure (Bego et al., 2025). In this context, technology functions not merely as a tool, but as a central medium that amplifies the impact of modern criminal conduct.

The complexity of cybercrime intensifies with the increasing use of artificial intelligence (AI). AI enables automated attacks, data-driven targeting, and the creation of manipulative content that closely resembles authentic information. Within the socio-political sphere, particularly during elections, AI facilitates disinformation, opinion manipulation, and the erosion of democratic legitimacy. The core legal challenge lies not only in the technical nature of such crimes, but in the ability of criminal law to address actions generated by autonomous systems beyond direct human control.

Previous studies have explored various forms of cybercrime. Research on cyberstalking highlights how digital anonymity expands interpersonal crime and complicates law enforcement efforts (Fadilah et al., 2021). Other studies emphasize cyberterrorism as a significant threat to national security, despite the absence of explicit regulatory terminology, including within Indonesia's ITE Law (Nopitasari & Fitriono, 2024). Globally, scholars have increasingly focused on AI-driven cyber threats, particularly deepfakes, automated propaganda, and structured disinformation campaigns (Velasco, 2022).

Despite these developments, criminal law has not fully anticipated the phenomenological shift caused by AI functioning as a quasi-actor in cybercrime. AI not only accelerates criminal activities but also introduces new layers of anonymity and causal complexity. In electoral contexts, this phenomenon poses systemic risks to democratic integrity, as AI-enabled interference can occur on a massive scale while obscuring accountability.

From an academic perspective, most criminal law studies continue to treat AI merely as an instrument rather than a determinant of criminal liability structures. Legal scholarship consistently maintains that AI cannot yet be recognized as a legal subject capable of bearing criminal responsibility (Baker & Robinson, 2020). Consequently, analyses of mens rea in crimes involving autonomous systems remain underdeveloped, particularly regarding cybercrimes that directly affect electoral processes.

Therefore, clear identification of the legal problems arising from AI-enabled cybercrime is essential to prevent normative ambiguity, enforcement gaps, and inconsistent attribution of criminal responsibility.

The novelty of this research lies in its examination of AI-enabled cybercrime in elections through the lens of mens rea theory. Rather than focusing solely on attribution of responsibility, this study interrogates how criminal fault can be constructed when unlawful acts are generated by autonomous systems. By integrating classical criminal law doctrine with the characteristics of AI technology, this research offers a new framework for understanding criminal liability in the digital age.

This study is urgent as it seeks to comprehensively analyze forms of AI-based cybercrime that threaten electoral integrity. It also aims to evaluate the relevance and limitations of mens rea theory in addressing crimes involving autonomous systems, and to formulate adaptive models of criminal liability in response to technological advancements.

This research aims to analyze comprehensively forms of AI-based cybercrime that threaten electoral integrity and to formulate adaptive criminal liability models in response to autonomous systems. Theoretically, this research contributes to the development of criminal law and legal philosophy in responding to non-human entities. Practically, it provides policy-relevant insights for regulators, election organizers, and law enforcement agencies in mitigating AI-driven cyber threats. Without such analysis, criminal law risks lagging behind technological realities, potentially enabling new forms of impunity that undermine public trust in democratic processes.

2. Research Methods

This research employs a qualitative research method with a normative legal research orientation. The qualitative approach is selected to enable an in-depth examination of AI-enabled cybercrime and the structure of criminal liability, which cannot be adequately captured through quantitative measurement alone (Nasution, 2023).

The research applies a normative approach and a conceptual approach. The normative approach is used to analyze statutory regulations related to cybercrime, artificial intelligence, and electoral integrity. Meanwhile, the conceptual approach is applied to examine the doctrine of *mens rea* and criminal liability in the context of autonomous systems (Wada et al., 2024).

The research specification is descriptive-analytical, aiming to describe legal phenomena related to the misuse of artificial intelligence in cybercrime and to analyze them systematically based on prevailing legal norms and theories. This specification allows the study to identify discrepancies between technological development and existing criminal law frameworks (Sutikno & Hadisaputra, 2020).

Legal materials are collected through library research. Primary legal materials consist of relevant statutory regulations, while secondary legal materials include textbooks, scholarly journal articles, and legal doctrines addressing cybercrime, artificial intelligence, and criminal liability. Tertiary legal materials are used to support and clarify legal terminology and concepts.

Data analysis is conducted using a qualitative descriptive-analytical technique, involving legal interpretation and conceptual analysis. The analysis focuses on the applicability of *mens rea* theory to AI-enabled cybercrime and the formulation of adaptive criminal liability mechanisms in response to technological advancements.

3. Results and Discussion

3.1. Characteristics of AI-Enabled Cybercrime and Electoral Threats

The results of this research indicate that artificial intelligence has fundamentally transformed the structure of cybercrime in the electoral context. Unlike conventional cybercrime, which relies on continuous human intervention, AI enables criminal activities to be conducted automatically, repetitively, and on a massive scale without direct human involvement at each operational stage. This finding demonstrates that AI no longer functions merely as a tool, but has become an active component that shapes the operational logic of cybercrime itself.

The study finds that the use of AI in electoral settings primarily targets the manipulation of the public information environment. AI systems are employed to generate, distribute, and amplify political content rapidly and selectively, blurring the distinction between authentic information and manipulative narratives. As a result, AI-driven cybercrime does not merely disrupt technical systems, but systematically influences public opinion and voter preferences.

Another key finding is the increasing difficulty of attributing criminal responsibility in AI-enabled cybercrime. AI operates within technological layers that obscure the causal link between actions and human actors. This condition creates significant challenges for identifying perpetrators and establishing legal accountability, particularly when AI systems are deployed across multiple platforms and jurisdictions.

The research also reveals that AI systems possess adaptive capabilities that allow them to operate in real time and adjust their outputs based on public responses. Through data-driven personalization, AI can modify political messages to target specific voter groups with high precision. This finding indicates that electoral threats posed by AI are not only technical in nature, but also cognitive and psychological, as they subtly influence voter behavior over time.

Based on these findings, the study identifies five core characteristics of AI-enabled cybercrime in elections: high-speed and large-scale information dissemination, actor anonymity, system autonomy in decision-making, the ability to manipulate public perception, and direct impact on electoral integrity and legitimacy. These characteristics demonstrate that AI-based cybercrime represents a qualitative departure from earlier forms of digital crime.

3.2 Ontological and Epistemological Consequences in Determining Criminal Fault

The results further indicate that AI-enabled cybercrime raises fundamental ontological challenges for criminal law. AI cannot be classified as a legal subject, yet it produces actions that generate significant legal consequences. This finding highlights a structural tension between the classical assumption of criminal law that offenders are human actors and the technological reality in which non-human systems generate legally relevant conduct.

In addition, the research identifies serious epistemological difficulties in proving criminal fault. AI systems often operate through complex, non-linear processes that are not fully transparent. As a result, it becomes increasingly difficult to trace intention, knowledge, or negligence back to specific human actors. This condition undermines traditional evidentiary approaches that rely on subjective intent as the primary basis for establishing criminal responsibility.

The findings suggest that, in the context of AI-enabled cybercrime, criminal fault tends to be structural rather than purely individual. Liability emerges from the interaction between system design, human decision-making, and the context in which AI technologies are deployed. Consequently, AI-driven cybercrime requires a reconceptualization of the relationship between action, fault, and criminal accountability.

3.3. Artificial Intelligence, Cybercrime, and Electoral Integrity

The findings of this study are consistent with research indicating that advances in artificial intelligence have expanded cybercrime from technical offenses into systematic manipulation of information and public perception (Bego et al., 2025). In electoral contexts, the deployment of AI for automated political content generation, intelligent bots, and deepfake production illustrates how technology not only accelerates criminal activity but also reshapes its objectives and societal impact. AI enables cybercrime to operate directly within the cognitive domain of voters, which lies at the core of democratic decision-making.

The adaptive and real-time nature of AI-driven operations reinforces the argument that visual manipulation and structured disinformation cannot be adequately addressed through traditional legal instruments (Velasco, 2022). Moreover, the difficulty of attributing responsibility identified in this study aligns with prior research on anonymity in digital crime, where offenders exploit technological infrastructures to evade legal identification (Fadilah et al., 2021).

3.4. Mens Rea and the Transformation of Criminal Fault

The finding that criminal fault in AI-enabled cybercrime is predominantly structural supports the view that artificial intelligence lacks moral agency and intentionality, making direct attribution of mens rea to AI conceptually impossible (Baker & Robinson, 2020). As a result, classical interpretations of mens rea become inadequate when unlawful outcomes are generated by autonomous systems.

This transformation from individual fault to structural fault is also consistent with contemporary developments in legal philosophy, which emphasize the social and technological contexts shaping human action (Rikiansyah et al., 2024). In this framework, mens rea is no longer confined to subjective intention but is understood as emerging from systemic configurations that enable harmful conduct.

3.5. Ontological and Epistemological Challenges in Criminal Accountability

The unresolved ontological status of AI within criminal law strengthens the argument that AI functions as a functional actor rather than a legal actor. This perspective aligns with cross-jurisdictional findings showing the absence of global consensus on recognizing AI as a subject of criminal liability (Duan, 2022). Consequently, criminal responsibility must continue to be directed toward human or institutional actors who design, deploy, or benefit from AI systems.

This view is consistent with criminal law scholarship that evaluates artificial intelligence as a non-human actor capable of producing legally relevant effects without possessing the ontological status of a criminal subject (Kan, 2024).

Epistemological challenges in proving fault are further exacerbated by the black-box nature of many AI models, which complicates efforts to establish causal links between human actions and unlawful outcomes (Abbas et al., 2024). These challenges suggest that evidentiary frameworks in criminal law must evolve to incorporate technological and systemic analysis alongside traditional investigative methods.

3.6. Normative Analysis and Models of Criminal Liability

Normative analysis of the Electronic Information and Transactions Law and the Election Law demonstrates that, although AI is not recognized as a legal subject, AI-enabled actions can still be attributed to human actors through grammatical, systematic, and teleological interpretation. This approach reflects the reactive nature of positive law in responding to technological developments (Nopitasari & Fitriono, 2024; Velasco, 2022).

This approach is particularly relevant to developer liability, where criminal responsibility may arise from flawed system design or the absence of adequate safeguards that enable unlawful AI-generated outcomes (Al-Ahmad & Al-Khazraji, 2025).

Within this normative gap, the liability models identified in this study direct human liability, developer liability, corporate vicarious liability, constructive mens rea, and shared liability represent legal strategies to maintain accountability in complex technological environments (Baker & Robinson, 2020; Abbas et al., 2024). These models indicate that criminal liability in AI-enabled cybercrime must be layered, contextual, and responsive to the distributed nature of technological agency.

3.7. Implications for Electoral Integrity and Legal Reform

The findings of this research reinforce the view that artificial intelligence poses a multidimensional threat to electoral integrity, extending beyond violations of positive law to the erosion of fundamental democratic values. When AI is used for manipulative purposes,

electoral processes lose public rationality and transparency, undermining trust in democratic institutions.

In the context of Indonesia's shift toward a restorative criminal justice paradigm, this study demonstrates that restorative approaches must be complemented by preventive and deterrent mechanisms when addressing AI-enabled cybercrime (Rikiansyah et al., 2024). Legal and electoral reform is therefore necessary to ensure that technological development does not generate new zones of impunity that threaten democratic legitimacy.

4. Conclusion

This research concludes that the misuse of artificial intelligence in cybercrime poses a fundamental threat to electoral integrity by transforming cyber offenses from human-centered actions into autonomous, large-scale, and structurally complex operations. AI-enabled cybercrime undermines democratic processes through systematic manipulation of public perception, while simultaneously challenging classical criminal law concepts, particularly *mens rea*, which are grounded in human intentionality. Given that AI cannot be recognized as a legal subject, criminal liability must be reconstructed and attributed to human and institutional actors through adaptive and layered liability models. Therefore, criminal law must evolve beyond reactive regulation toward a proactive and anticipatory framework capable of addressing the unique risks posed by AI-driven cybercrime in democratic elections.

5. References

Abbas, T. N. A., Kadhim, A. A., Hameed, R., & Qasim, N. H. (2024). Artificial Intelligence and Criminal Liability: Exploring the Legal Implica-tions of AI-Enabled Crimes; Inteligencia artificial y responsabilidad penal: exploración de las implicaciones legales de los delitos impulsados por la IA. *Encuentros (Maracaibo)*, *22*, 140–159.

Al-Ahmad, M. H., & Al-Khazraji, I. S. (2025). Criminal Liability for Artificial Intelligence Crimes. In *Intelligence-Driven Circular Economy: Regeneration Towards Sustainability and Social Responsibility --- Volume 2* (pp. 575–587). Springer Nature Switzerland.

Baker, D. J., & Robinson, P. H. (Eds.). (2020). *Artificial Intelligence and the Law: Cybercrime and Criminal Liability*. Routledge.

Bego, K. C., Aziz, F. R., Rahmad, R. A., & Budianto, H. (2025). Tindak Pidana Cybercrime: Tantangan Hukum Pidana Dalam Menanggulangi Kejahatan di Dunia Maya. *Jurnal Kolaboratif Sains*, *8*(1), 506–511.

Duan, Z. (2022). Artificial Intelligence and the Law: Cybercrime and Criminal Liability. By Dennis J. Baker and Paul H. Robinson (Routledge, 2021, 280 pp.). *International Review of Law*.

Fadilah, A., Aranggraeni, R., & Putri, S. R. (2021). Eksistensi Keamanan Siber Terhadap Tindakan Cyberstalking Dalam Sistem Pertanggungjawaban Pidana Cybercrime. *Syntax Literate: Jurnal Ilmiah Indonesia*, *6*(4), 1555.

Kan, C. H. (2024). Criminal Liability of Artificial Intelligence from the Perspective of Criminal Law: An Evaluation in the Context of the General Theory of Crime and Fundamental Principles. *International Journal of Eurasia Social Sciences*, *14*(55).

Nopitasari, G., & Fitriono, R. A. (2024). Pertanggungjawaban Pidana Pelaku Kejahatan Cyber Terrorism Dalam Undang-Undang Nasional. *Konsensus: Jurnal Ilmu Pertahanan, Hukum Dan Ilmu Komunikasi*, *1*(4), 180–199. https://doi.org/10.62383/konsensus.v1i4.266

Rikiansyah, R., Septiawan, A., & Shanty, S. (2024). Kajian Filsafat Hukum Terhadap Perubahan Paradigma Hukum Pidana di Indonesia: Dari Pembalasan ke Pemulihan. *Indonesian Journal of Law and Justice*, *1*(4), 8. https://doi.org/10.47134/ijlj.v1i4.2719

Velasco, C. (2022). Cybercrime and Artificial Intelligence: An Overview of the Work of International Organizations on Criminal Justice and the International Applicable Instruments. *ERA Forum*, *23*(1), 109–126.