

**JLPH:**
**Journal of Law, Politic
and Humanities**<https://dinastires.org/JLPH> ✉ dinasti.info@gmail.com ☎ +62 811 7404 455E-ISSN: 2962-2816
P-ISSN: 2747-1985DOI: <https://doi.org/10.38035/jlph.v6i6>
<https://creativecommons.org/licenses/by/4.0/>

Received: 20 September 2026 | Revised: 06 Oktober 2026 | Accepted: 14 Oktober 2026

The Urgency of Formulating Criminal Law Policy Regarding the Misuse of Artificial Intelligence to Ensure Legal Certainty

Faishal Ali Assegaf¹¹Universitas Bengkulu, Bengkulu, Indonesia, Faishalali.assegaf@gmail.comCorresponding Author: Faishalali.assegaf@gmail.com¹

Abstract: The development of Artificial Intelligence (AI) has brought significant changes to various aspects of life, while also creating increasingly complex forms of misuse, such as digital information manipulation, automated cyberattacks, and personal data exploitation. These conditions demonstrate the limitations of conventional criminal law in anticipating and addressing AI-based crimes. In Indonesia, there is currently no specific and comprehensive criminal law regulation governing the misuse of AI, which may lead to regulatory gaps, differences in legal interpretation, and legal uncertainty. This study aims to analyze the urgency of establishing criminal law policies concerning the misuse of AI and to examine the ideal direction of criminal law policy to achieve legal certainty. The study finds that establishing criminal law policies concerning AI misuse is an urgent necessity. Such policies should be adaptive, preventive, responsive, and forward-looking. An ideal regulatory framework should address the definition and scope of AI, limitations on its use, criminal liability, prevention, supervision, system security standards, and the enhancement of law enforcement capacity. Through clear and comprehensive policies, criminal law is expected to provide legal certainty while protecting society from the negative impacts of AI misuse.

Keywords: Artificial Intelligence, Criminal Law Policy, AI Misuse, Legal Certainty, Cybercrime

Abstrak: Perkembangan Artificial Intelligence (AI) telah memberikan perubahan signifikan dalam berbagai aspek kehidupan, tetapi juga menimbulkan potensi penyalahgunaan yang semakin kompleks, seperti manipulasi informasi digital, serangan siber otomatis, dan eksploitasi data pribadi. Kondisi tersebut menunjukkan adanya keterbatasan hukum pidana konvensional dalam mengantisipasi dan menangani kejahatan berbasis AI. Di Indonesia, belum terdapat pengaturan hukum pidana yang secara khusus dan komprehensif mengatur penyalahgunaan AI, sehingga berpotensi menimbulkan kekosongan norma, perbedaan penafsiran, dan ketidakpastian hukum. Kajian ini bertujuan untuk menganalisis urgensi pembentukan kebijakan hukum pidana terhadap penyalahgunaan AI serta mengkaji arah kebijakan hukum pidana yang ideal guna mewujudkan kepastian hukum. Hasil kajian menunjukkan bahwa pembentukan kebijakan hukum pidana terhadap penyalahgunaan AI merupakan kebutuhan yang mendesak. Kebijakan tersebut perlu bersifat adaptif, preventif,

responsif, dan berorientasi pada masa depan. Pengaturan yang ideal perlu mencakup definisi dan ruang lingkup AI, batasan penggunaan, pertanggungjawaban pidana, pencegahan, pengawasan, standar keamanan sistem, serta peningkatan kapasitas aparat penegak hukum. Dengan kebijakan yang jelas dan komprehensif, hukum pidana diharapkan mampu memberikan kepastian hukum sekaligus melindungi masyarakat dari dampak negatif penyalahgunaan AI.

Kata Kunci: *Artificial Intelligence, Kebijakan Hukum Pidana, Penyalahgunaan AI, Kepastian Hukum, Kejahatan Siber*

INTRODUCTION

The development of Artificial Intelligence (AI) as part of the Industry 4.0 revolution has brought about rapid changes in modern life. This technology serves not merely as a tool but has evolved into a system capable of making data-driven decisions autonomously. In practice, AI is utilized across various strategic sectors, including finance, security, healthcare, and digital communication. However, this advancement has not always been matched by adequate regulatory frameworks, particularly within the realm of criminal law (Ian Goodfellow, 2016).

In recent years, the misuse of AI has shown an increasingly complex and rising trend. Technologies such as deepfakes, automated hacking, and AI-driven fraud have caused serious economic and social impacts. AI-based crimes are not only difficult to detect but also challenging to prove, as they involve systems that operate automatically and across national borders. This situation demonstrates that conventional criminal justice systems face limitations in addressing these new forms of crime (Marc Goodman, 2015).

The primary issue lies not only in law enforcement but also in the absence of criminal law policies specifically regulating AI. Current Indonesian positive law as reflected in various regulations concerning information technology remains general in nature and lacks specific provisions regarding AI. Consequently, a legal vacuum exists, potentially leading to legal uncertainty and creating opportunities for the misuse of technology without clear sanctions (Josua Sitompul, 2012).

From the perspective of the rule of law, legal certainty is a fundamental principle that the state must guarantee. When the law fails to keep pace with technological advancements, its function as a tool for regulating and protecting society is compromised. Therefore, a criminal law policy is required that can address the challenges posed by the evolution of AI, encompassing both preventive and repressive measures. Such a policy serves not only to penalize offenders but also to regulate and guide the use of technology to prevent its misuse (Bambang Waluyo, 2017).

The urgency of formulating criminal law policies regarding AI is also closely linked to the need to protect the broader public interest. The misuse of AI can impact various aspects of life, ranging from privacy violations and information manipulation to the disruption of social stability. In this context, the state has an obligation to intervene through firm and comprehensive legal policies to ensure that technological advancements remain within the bounds of applicable law (Nyoman Serikat Putra Jaya, 2020).

Furthermore, within the framework of criminal policy, the formulation of criminal law policies regarding AI must be conducted in a planned and forward-looking manner. This is crucial given the highly dynamic and unpredictable nature of technological advancement. Without a clear policy, criminal law will inevitably remain reactive and lag behind technological developments. Therefore, strategic measures are required to formulate legal

policies that not only address current issues but are also capable of anticipating future challenges (Rika Ratna Permata, 2022).

Based on the foregoing, it is evident that establishing a criminal law policy regarding the misuse of AI is a matter of urgent necessity. Without a clear and comprehensive policy, legal certainty cannot be achieved, and the potential for technological misuse will continue to rise. Therefore, an in-depth study is required to formulate a criminal law policy capable of addressing the challenges posed by AI advancements while simultaneously ensuring legal certainty in Indonesia.

METHODS

This study employs a normative legal research method (juridical-normative), involving the examination and analysis of legal norms concerning the misuse of Artificial Intelligence (AI) within the framework of criminal law policy in Indonesia. The study utilizes both the statute approach and the conceptual approach to identify and analyze applicable legal provisions and criminal law policy concepts relevant to the evolution of AI technology. The legal materials employed include primary sources specifically legislation regarding information technology, data protection, and criminal law; secondary sources such as books, scholarly journals, research findings, and expert legal opinions; and tertiary sources including legal dictionaries and other supporting materials. Data collection was conducted through library research, followed by a qualitative-descriptive analysis that elaborates on, interprets, and interrelates various legal provisions and concepts. This process aims to address the urgency of formulating a criminal law policy regarding AI misuse and to outline a policy direction capable of ensuring legal certainty in Indonesia.

RESULTS AND DISCUSSION

The Urgency of Formulating Criminal Law Policy Regarding the Misuse of Artificial Intelligence

The development of Artificial Intelligence (AI) as part of the global digital transformation has fundamentally altered societal lifestyles. AI is no longer merely an assistive tool; it has evolved into a system capable of autonomous operation through data processing and complex algorithms. In this context, while AI holds immense potential for application across various fields, it simultaneously creates opportunities for misuse that could lead to criminal activity (Sudikno Mertokusumo, 2016).

The urgency of formulating criminal law policies regarding AI has become increasingly apparent as technology-driven crimes grow more complex. Crimes leveraging AI are no longer limited to conventional forms, they have evolved into offenses that are systematic, automated, and difficult to detect such as the manipulation of digital information, automated cyberattacks, and the large-scale exploitation of personal data. Such crimes not only harm individuals but also threaten social stability and national security (Abdul Wahid dan Mohammad Labib, 2010).

Under these circumstances, the current criminal justice system faces limitations in keeping pace with technological advancements. Criminal law tends to be static, whereas technology evolves dynamically and rapidly. This imbalance often causes the law to lag behind in regulating new phenomena emerging in society. Therefore, a criminal law policy is required that is not merely reactive but also capable of anticipating future technological developments (Satjipto Rahardjo, 2009).

Furthermore, the absence of criminal law policies specifically addressing AI creates the potential for legal uncertainty. In law enforcement practice, officials often struggle to classify AI-related actions under existing legal provisions, as there are currently no legal norms explicitly regulating the use and misuse of AI. Consequently, law enforcement efforts are

suboptimal and may lead to divergent interpretations in the application of the law (Diantha I Made Pasek, 2017).

From the perspective of legal protection, formulating criminal law policies regarding AI is a strategic step toward safeguarding the public interest. The misuse of AI can impact various aspects of life, ranging from privacy violations and the dissemination of misleading information to potential algorithm-based discrimination. Consequently, the state has an obligation to intervene through regulations capable of providing maximum legal protection for the public. In this context, criminal law serves as a vital instrument for maintaining order and justice (Erdianto Effendi, 2021).

Furthermore, within the framework of criminal policy, the formulation of AI regulations must be comprehensive and forward-looking. Such policy should not merely address prohibitions and sanctions but also encompass measures for prevention, oversight, and the control of AI usage. Thus, criminal law serves not only as an instrument of enforcement but also as a means to guide technological development so that it remains within the bounds of applicable law (Sigid Suseno, 2021).

Thus, it can be concluded that the urgency of establishing a criminal law policy regarding the misuse of AI is a necessity that cannot be postponed. Without a clear and adaptive policy, the criminal justice system will struggle to cope with increasingly complex technological developments. Therefore, concrete steps are needed to formulate a criminal law policy that can address the challenges of AI development while simultaneously ensuring legal certainty in Indonesia.

The Ideal Direction of Criminal Law Policy Regarding the Misuse of Artificial Intelligence

The rapid advancement of Artificial Intelligence (AI) necessitates the formulation of criminal law policies that are not only responsive but also visionary and adaptive to technological dynamics. In this context, the ideal direction for criminal law policy must be capable of addressing the various challenges posed by the misuse of AI while simultaneously providing legal certainty for the public. Such policies must be comprehensively designed, taking into account juridical, sociological, and philosophical aspects (Romli Atmasasmita, 2017).

A key direction in criminal law policy is the formulation of specific regulations that clearly and comprehensively govern the use of AI. These regulations must encompass the definition of AI, the scope of its application, and the boundaries regarding what is permitted and what is prohibited. Clear regulations will minimize the potential for multiple interpretations during legal application, thereby establishing legal certainty in the enforcement of criminal law regarding the misuse of AI (Lawrence M. Friedman, 1975).

Furthermore, an ideal criminal law policy must clearly regulate criminal liability regarding the use of AI. In this regard, a flexible approach is required to determine the liable legal subject whether an individual, a corporation, or another party involved in the development and use of AI. This approach is essential given the autonomous nature of AI, which necessitates a broader concept of liability than that found in conventional criminal law (Chairul Huda, 2016).

The future direction of criminal law policy involves strengthening the preventive aspect of AI regulation. Policy should not focus solely on imposing sanctions on offenders but must also be capable of preventing technology misuse from the outset. This can be achieved through the regulation of AI system security standards, mandatory algorithmic transparency, and effective oversight mechanisms for the technology's use. Consequently, criminal law becomes not only repressive but also preventive and educational in nature (Agus Raharjo, 2021).

Furthermore, an ideal criminal law policy must be supported by enhancing the capacity of law enforcement officials to understand and address technology-based crimes. Without adequate understanding, effectively enforcing the law against AI misuse would be difficult. Therefore, training and competency development for law enforcement officials are essential to enable them to keep pace with increasingly complex technological advancements (Susi Dwi Harijanti, 2021).

In a global context, the direction of criminal law policy regarding AI must also take into account developments in international law. Given that AI-based crimes are often transnational in nature, international cooperation is required to address them. Indonesia needs to adopt relevant international principles without disregarding national legal values. This is crucial to ensure that the criminal law policy formulated is not only effective at the national level but also capable of addressing global challenges (Hikmahanto Juwana, 2020).

Consequently, the ideal criminal law policy regarding the misuse of AI must be comprehensive, adaptive, and forward-looking. Such a policy should not only address enforcement but also encompass prevention, oversight, and the capacity building of law enforcement officials. Through appropriate policy measures, it is expected that Indonesia's criminal law will be capable of providing legal certainty while simultaneously protecting the public from the negative impacts of AI technological advancements.

CONCLUSIONS AND RECOMMENDATIONS

Conclusion

1. The development of Artificial Intelligence (AI) has significantly impacted various aspects of life but has also given rise to increasingly complex and diverse potential for misuse. Against this backdrop, Indonesia's current criminal justice system lacks specific and comprehensive regulations regarding AI, resulting in a legal vacuum and uncertainty in law enforcement particularly when addressing technology-based crimes.
2. Formulating criminal law policy regarding the misuse of AI is an urgent necessity, given the evolving nature of digital crimes that often elude the reach of conventional law. Therefore, the ideal criminal law policy must be adaptive, preventive, and responsive, while clearly defining legal liability to ensure legal certainty and public protection.

Recommendations

1. The government needs to urgently formulate and establish specific regulations governing the use of Artificial Intelligence from a criminal law perspective whether through the enactment of new legislation or the refinement of existing regulations to ensure legal certainty and prevent the future misuse of the technology.
2. It is necessary to enhance the capacity and competence of law enforcement officials in understanding and handling technology-based crimes, as well as to strengthen cooperation among the government, academia, and technology practitioners in formulating legal policies that are comprehensive, adaptive, and implementable in line with the evolution of the digital era.

REFERENCES

- Abdul Wahid dan Mohammad Labib. *Kejahatan Mayantara (Cyber Crime)*. Bandung: Refika Aditama, 2010.
- Agus Raharjo. "Pengaturan Teknologi Informasi dalam Perspektif Hukum Pidana." *Jurnal Hukum*, Vol. 23 No. 1, 2021.
- Bambang Waluyo. *Penegakan Hukum di Indonesia*. Jakarta: Sinar Grafika, 2017.
- Chairul Huda. *Dari Tiada Pidana Tanpa Kesalahan Menuju Kepada Tiada Pertanggungjawaban Pidana Tanpa Kesalahan*. Jakarta: Kencana, 2016.

- Diantha I Made Pasek. *Metodologi Penelitian Hukum Normatif*. Jakarta: Prenada Media, 2017.
- Erdianto Effendi. "Penegakan Hukum terhadap Kejahatan Siber di Indonesia." *Jurnal Ilmu Hukum*, Vol. 15 No. 2, 2021.
- Hikmahanto Juwana. "Hukum Internasional dalam Perkembangan Teknologi Global." *Jurnal Hukum Internasional*, Vol. 14 No. 3, 2020.
- Ian Goodfellow, Yoshua Bengio, dan Aaron Courville. *Deep Learning*. Cambridge: MIT Press, 2016.
- Josua Sitompul. *Cyberspace, Cybercrimes, Cyberlaw: Tinjauan Aspek Hukum Pidana*. Jakarta: Tatanusa, 2012.
- Lawrence M. Friedman. *The Legal System: A Social Science Perspective*. New York: Russell Sage Foundation, 1975.
- Marc Goodman. *Future Crimes*. New York: Doubleday, 2015.
- Nyoman Serikat Putra Jaya. "Kebijakan Hukum Pidana dalam Menanggulangi Kejahatan Siber." *Jurnal Hukum*, Vol. 22 No. 3, 2020.
- Rika Ratna Permata. "Perlindungan Hukum terhadap Penyalahgunaan Data dalam Teknologi Digital." *Jurnal Rechts Vinding*, Vol. 11 No. 2, 2022.
- Romli Atmasasmita. *Reformasi Hukum Pidana*. Bandung: Mandar Maju, 2017.
- Satjipto Rahardjo. *Hukum Progresif*. Jakarta: Kompas, 2009.
- Sigid Suseno. "Kebijakan Hukum Pidana dalam Era Digital." *Jurnal Hukum dan Peradilan*, Vol. 10 No. 1, 2021.
- Sudikno Mertokusumo. *Mengenal Hukum: Suatu Pengantar*. Yogyakarta: Liberty, 2016.
- Susi Dwi Harijanti. "Penguatan Kapasitas Penegak Hukum dalam Era Digital." *Jurnal Konstitusi*, Vol. 18 No. 2, 2021.