West Science Law and Human Rights
Vol. 4, No. 01, January 2026, pp. 31~38

Public Protection from The Risk of Criminality Based on Artificial Intelligence from a Legal Perspective Modern Crime

Maria Angelorum Boekan
Atma Jaya University Yogyakarta

Article Info

Article history:

Received January, 2026
Revised January, 2026
Accepted January, 2026

Keywords:

Artificial Intelligence
AI-Enabled Crime
Cyber Law
Modern Criminal Law
Public Protection

ABSTRACT

The development of artificial intelligence (AI) has brought about significant changes in the social, economic, and legal order. Despite the various benefits offered, the use of AI also opens up the possibility of new forms of crime that are increasingly complex, automated, transcend national borders, and difficult to identify. AI-based crimes include automated fraud, identity forgery through deepfake technology, adaptive cyberattacks, misuse of personal data, and transnational cybercrime. These phenomena pose serious threats to public security, national resilience, and public trust in digital governance. Therefore, this study examines crime patterns that utilize AI and analyzes modern criminal law responses to these risks, both in the Indonesian context and internationally. This study uses a normative juridical method with a statutory and conceptual approach to examine criminal law norms, the regulation of cybercrime, and international instruments related to the use of artificial intelligence (AI). The results of the study indicate that modern criminal law still essentially places humans and corporations as the primary subjects of criminal responsibility, while AI is viewed as a means or tool that can be exploited in committing crimes. Therefore, to ensure effective public protection from AI-based crimes, adaptive legal reforms, prevention-oriented law enforcement, strengthening corporate criminal liability, and increased international cooperation are needed.

Corresponding Author:

Name: Maria Angelorum Boekan
Institution Address: Atma Jaya University Yogyakarta
e-mail: anggyangelorum@gmail.com

1. INTRODUCTION

Over the past twenty years, advances in Artificial Intelligence (AI) have become a key factor driving the acceleration of digital transformation globally. This technology has fundamentally changed the way people work, communicate, and make choices. The application of AI across various sectors, including business, government, healthcare, education, and security, has been shown to improve work efficiency, productivity, and the capacity to process and analyze large amounts of data that were previously difficult to perform manually [1]. Within the framework of the modern state, AI is also beginning to be utilized in the provision of public services and the formulation of strategic policies, making it a crucial component in the development of digital governance [2].

However, this technological advancement also poses serious challenges in the form of crimes that utilize artificial intelligence (AI) with characteristics that differ from conventional crimes. These crimes are committed through the misuse of AI capabilities, for example, algorithm manipulation, the creation of fake content based on deepfakes, the automatic spread of disinformation, adaptive cyberattacks, and fraud using autonomous bots [3]. The nature of AI-based crimes tends to be complex, structured, and difficult to track, so that their impact is not only detrimental to individuals, but also has the potential to disrupt social stability, national security, and reduce public trust in the legal system and state institutions [4].

One of the main challenges that arises is the inability of traditional criminal law to address crimes involving AI technology. Conventional criminal law generally assumes that perpetrators of crimes are humans who act with their own consciousness and will (actus reus and mens rea) [Lawrence Lessig, 2006]. However, in the practice of AI-based crimes, unlawful acts can be carried out by semi-autonomous systems that operate based on algorithms and data. This creates difficulties in determining who can be considered a legal subject and who is criminally responsible. The problem is further complicated when losses arise from algorithmic bias, design errors, or data processing failures that cannot be directly attributed to a person's malicious intent [5].

Beyond criminal liability, law enforcement officials also face significant challenges in establishing evidence. Digital forensics, crime tracing, and proving intent become more complex when AI systems operate as opaque "black boxes." This opacity not only hampers investigations but also potentially undermines the principles of legal certainty and fairness in criminal justice. Furthermore, the often transnational nature of AI-based crimes necessitates international cooperation and legal harmonization, which have yet to be fully realized.

This situation underscores the importance of modern criminal law reforms to adapt quickly to technological developments. A criminal law approach cannot be merely repressive and reactive; it must be designed to be preventative and responsive through the creation of flexible and adaptive regulations for AI technology. These reforms must be based on the principles of justice, proportionality, and respect for human rights, while ensuring the protection of personal data, the security of public systems, and legal certainty for the public.

This research aims to examine the importance and direction of modern criminal law development in addressing the risks of crimes involving Artificial Intelligence (AI). The novelty of this research lies in the effort to design a conceptual framework for criminal law that is flexible and responsive to AI, viewing technology not only as a means of committing crimes but also as an object that needs to be regulated through a new normative approach. Thus, the research findings are expected to contribute, both theoretically and practically, to the development of criminal law policies that can protect public security while still supporting technological progress [6].

2. LITERATURE REVIEW

This literature review aims to explore and map the development of thinking and research findings related to protecting the public from the risks of crime arising from the use of artificial intelligence (AI) within the framework of modern criminal law. The literature discussed includes the concept of AI and its impact on criminal practices, changes and adaptations of modern criminal law in response to technological advances, and the importance of legal protection for the public amidst the use of AI.

2.1 *First Literature*

The first literature highlights the development of artificial intelligence (AI) and its relationship to the emergence of new types of crime. According to [7], AI is a system designed to mimic human intellectual abilities through automated learning, reasoning, and decision-making. While these capabilities offer many benefits, such as increased efficiency and security, AI also has the potential to be misused for criminal purposes.

Several studies have shown that AI technology has been misused for various crimes, including digital fraud, data manipulation, deepfake content creation, and cybercrimes that are increasingly difficult for law enforcement to uncover [8]. The literature emphasizes that AI-based crimes are complex, cross-border, and often cannot be adequately addressed by conventional criminal law.

In other words, this study confirms that advances in AI technology have a direct impact on contemporary crime patterns, so flexible and progressive legal adjustments are needed to safeguard the interests of society.

2.2 *Second Literature*

The second literature emphasizes an understanding of modern criminal law in the face of technological developments. [9] asserts that modern criminal law emphasizes not only sanctions but also crime prevention, community protection, and social risk management. This approach is particularly relevant in the context of artificial intelligence, as potential criminal acts often arise in a preventative and risk-based manner.

Some experts emphasize that modern criminal law should adopt the principle of risk-based regulation, meaning that the law should not only act after a crime has occurred but should also be able to predict and prevent potential dangers arising from the use of advanced technology [10]. This approach aligns with the concept of public protection, where public safety is the primary focus of criminal law enforcement.

The literature emphasizes that modern criminal law must broaden the scope of responsibility, not only for individuals but also to include corporations and AI technology developers, so that legal protection for society can be implemented effectively.

2.3 *Third Literature*

The third literature emphasizes the importance of public protection and regulating the use of AI from a legal and policy perspective. [11] emphasized that the use of AI in society must be accompanied by a legal framework that guarantees accountability, transparency, and the protection of human rights. Without proper regulation, AI risks becoming a tool that increases crime and injustice.

Several studies highlight the importance of the state's role in formulating effective legal policies to control the risks posed by AI, whether through criminal law, administrative law, or non-penal mechanisms [9]. Protecting the public means not only prosecuting perpetrators but also involving systematic preventive efforts to prevent the misuse of technology from the design stage to its implementation.

This literature emphasizes that to protect society from the risks of crime related to artificial intelligence (AI), a modern criminal law approach is needed that is comprehensive, flexible, and focuses on prevention and ongoing protection for the public [12].

3. METHODS

This study employs a normative legal research method with two approaches: a statute approach and a conceptual approach. These approaches are applied to deeply analyze criminal law norms, modern criminal law principles, and ideas regarding public protection against the risks of crime arising from artificial intelligence.

The subject of this research is the modern criminal law system that regulates the prevention and handling of technology-based crimes. The research object encompasses various forms of legal protection for the public against the risks of crime arising from the use and misuse of artificial intelligence within the framework of modern criminal law.

This research uses library research. Sources include university libraries and legal literature searches through scientific journal databases, both national and international, laws and regulations, and related official publications.

The research instrument used a document study method that encompasses three types of legal materials. Primary legal materials consist of laws and regulations related to criminal law and information technology. Secondary legal materials include books and scientific journal articles, while tertiary legal materials include legal dictionaries and encyclopedias.

The legal material sampling method used purposive sampling, which involves the deliberate and targeted selection of legal materials based on their relevance to the research topic. Data were collected through a literature study method, which involved identifying, recording, and categorizing legal sources relevant to the research problem.

Data analysis was conducted qualitatively using a descriptive-analytical approach, namely by examining data through legal interpretation and the preparation of legal arguments, so that conclusions can be drawn regarding the form of public protection against the risk of crime related to artificial intelligence from a modern criminal law perspective.

4. RESULTS AND DISCUSSION

This section presents the main research findings and their discussion systematically, in line with the research objectives. The presentation focuses on relevant data and information related to protecting the public from the risks of artificial intelligence (AI)-based crime. The research results are analyzed and evaluated, then interpreted by linking them to developments in modern criminal law concepts and recent research findings, ensuring alignment between the title, problem formulation, discussion, and bibliography.

4.1 Patterns and Characteristics of Artificial Intelligence-Based Crime

Research reveals that crimes involving artificial intelligence are fundamentally different from conventional crimes. AI-based crimes are automated, adaptable, cross national borders, and occur on a large scale at breakneck speed. In this context, AI serves not only as a tool but has become a key driver of crime by increasing the effectiveness, reach, and complexity of crime [13].

In Indonesia, crimes utilizing AI technology most frequently occur in the form of automated digital fraud, misuse of personal data, sophisticated cyberattacks, and identity fraud through deepfake technology. Perpetrators use various methods such as chatbots, voice cloning, and AI-based phishing, which can mimic human communication patterns with remarkable accuracy. As a result, victims often have difficulty distinguishing between genuine and fake interactions. This situation not only increases the success rate of criminal acts but also poses significant challenges in proving the perpetrator's intent or culpability (mens rea) in criminal proceedings.

Globally, research shows that crimes utilizing artificial intelligence are becoming increasingly complex and organized. AI is not only being used for individual criminal purposes, but also for political manipulation, transnational financial crimes, attacks on critical infrastructure, and the development of autonomous weapons. [14] For example, the use of deepfake technology in the 2024 United States Election demonstrates how the misuse of AI can disrupt democratic processes, undermine public trust, and threaten national stability. These findings align with international studies highlighting AI as a new risk in modern crime.

Overall, this research demonstrates that artificial intelligence has evolved from a mere support tool to a fully autonomous system capable of generating direct legal and social impacts through machine learning. This development requires fundamental adjustments to criminal law doctrine, which has historically focused solely on human actions.

4.2 Challenges of Modern Criminal Law in Facing AI-Based Crimes

Research shows that modern criminal law still faces structural obstacles in addressing crimes involving artificial intelligence. The main difficulty arises because the concept of criminal responsibility so far only recognizes humans as legal subjects. Meanwhile, AI systems are capable of operating independently and making decisions without direct human intervention. [15] However, because AI lacks moral consciousness or ethical intent, current criminal law cannot yet hold it directly accountable.

From a modern criminal law perspective, the principle of geen straf zonder schuld (no crime without fault) remains upheld, emphasizing that criminal responsibility rests with the individual or legal entity controlling AI technology. Research shows that this responsibility can be imposed on developers, users, and companies. Developers can be held liable if proven negligent in designing a secure system or intentionally creating high-risk technology without adequate security mechanisms. Users are criminally liable when using AI to commit crimes. Meanwhile, companies can be held criminally liable if they fail to implement the principle of due diligence in the development, use, or supervision of the AI systems they control [16].

In addition to issues related to legal subjects, research also identified challenges in determining the locus delicti (place of occurrence) and tempus delicti (time of occurrence) in transnational AI-based crimes. AI-based cybercrimes can be committed from one country, utilize digital infrastructure in another, and cause harm in multiple regions simultaneously. This situation makes criminal law enforcement at the national level less effective without a strong and coordinated international cooperation mechanism.

In other words, this research emphasizes the importance of reforming criminal law through a lex adaptiva approach. Criminal norms need to be interpreted more broadly to encompass actions that occur in the digital world and utilize artificial intelligence. Furthermore, the formulation of new types of criminal offenses that clearly regulate the misuse of AI is necessary.

4.3 Community Protection Strategy through a Criminal Law Approach

Based on research findings, efforts to protect the public from the threat of crime involving artificial intelligence cannot rely solely on criminal law enforcement. Modern criminal law needs to be developed with a preventative approach, adapt to technological advances, and involve collaboration across various sectors. One of the most urgent steps is the development of specific regulations related to artificial intelligence. Currently, the lack of laws specifically governing AI means law enforcement officials are still relying on general criminal provisions, which are not designed to address the complexities of algorithmic systems and autonomous technology.

The next strategy is to implement proactive law enforcement by utilizing artificial intelligence to identify crime patterns early. Through a predictive policing approach, law enforcement can map potential criminal risks before they cause harm, thereby making public protection more effective.

However, the implementation of this strategy must respect human rights and adhere to the principle of proportionality to prevent abuse of authority.

Furthermore, this study emphasizes the importance of strengthening corporate criminal liability. Because the development and operation of AI technology are generally carried out by business entities, the application of the concept of corporate criminal liability is an important tool to encourage ethical and responsible AI governance practices. Furthermore, independent AI audit and oversight mechanisms are needed to ensure the use of algorithms is transparent, safe, and accountable.

At the international level, this research emphasizes the importance of cooperation between countries. Harmonizing legal regulations, strengthening extradition mechanisms, and increasing the exchange of digital intelligence information must be seriously pursued to close legal loopholes frequently exploited by cybercriminals. Without cross-border coordination, national criminal laws will always lag behind the rapid development of artificial intelligence technology.

Thus, efforts to protect the public from the threat of AI-based crimes require a comprehensive update of criminal law, which is not only reactive to crimes that have already occurred, but also proactive and forward-looking to anticipate future technological advances.

Table 1.

No.	Types of AI-Based Crimes	Modus Operandi	Legal Implications
1.	Fraudulent crimes committed digitally using automated systems.	*Chatbot*, adaptive phishing, voice cloning	The difficulty of proving intent or deliberate action and determining the identity of the perpetrator
2.	Unauthorized or misuse of personal data	Collection and processing of data through algorithms carried out in an unauthorized manner	Violation of privacy rights and the impact of financial losses experienced by victims.
3.	Adaptive cyber attacks	Artificial intelligence systems adapt attack methods to exploit digital security gaps.	Dangers that can disrupt important systems and threaten national security.
4.	Digital identity manipulation or forgery using deepfake technology, where a person's face, voice, or behavior is realistically imitated to deceive or mislead others.	Falsification of voices and images of public figures for certain purposes.	Damage or decline in public trust in public institutions and democratic processes.
5.	Crimes that cross legal boundaries	Use of international scale servers and networks.	Constraints related to locus delicti and tempus delictirefers to the difficulty in determining the place (locus) and time (tempus) of a crime. Locus delicti becomes an obstacle when it is difficult to determine the exact location where the crime occurred, which affects the court's jurisdiction. Meanwhile, tempus delicti creates

			problems when the exact time of the crime is unclear, making it difficult to apply appropriate law or determine the statute of limitations.

5. CONCLUSION

This study concludes that the use of artificial intelligence (AI) in various crimes has made the nature of crimes more complex, automated, adaptive, and transnational, thus posing significant challenges to the criminal justice system. AI-based crimes, such as automated digital fraud, deepfake content creation, adaptive cyberattacks, and misuse of personal data, not only harm individuals but also threaten social, economic, and democratic stability. Conventional criminal law still has limitations because it focuses on human actors and subjective proof of guilt, while AI systems operate autonomously and are not fully transparent. Nevertheless, criminal liability can still be implemented by placing responsibility on the individuals or corporations that design, operate, and control AI, emphasizing the principles of prudence, oversight, and accountability, so that public protection can still be achieved from a modern criminal law perspective.

SUGGESTIONS

Based on the research findings, it is recommended that future criminal law development emphasize an adaptive and preventative approach to addressing crimes involving artificial intelligence. The government and legislators need to draft specific regulations regarding AI that clearly define the limits and forms of criminal liability, particularly for companies and those controlling the technology. Furthermore, increasing the capacity of law enforcement officials through the use of digital technology, implementing audit mechanisms and algorithm transparency, and strengthening international cooperation are crucial steps to address transnational cybercrime. This approach is expected to create a balance between technological advancement, human rights protection, and public security.

ACKNOWLEDGEMENTS

The author would like to express his gratitude to all parties who participated in the completion of this research. Special appreciation is extended to his academic supervisors and colleagues for their guidance, input, and constructive discussions throughout the research process. He also acknowledges the support and facilities provided by the institutions that made this research possible. If any funding or sponsorship is available, he acknowledges and expresses his deepest appreciation for the assistance provided.

REFERENCES

[1] S. J. Russell and P. Norvig, "Artificial Intelligence: A Modern Approach, Global Edition 4e," 2021.

[2] S. Klaus, "The fourth industrial revolution." Moscow: Ekonomika, 2016.

[3] J. M. Balkin, "Free speech in the algorithmic society: Big data, private governance, and new school speech regulation," *UCDL rev.*, vol. 51, p. 1149, 2017.

[4] B. Chesney and D. Citron, "Deep fakes: A looming challenge for privacy, democracy, and national security," *Calif. L. Rev.*, vol. 107, p. 1753, 2019.

[5] S. H. Barda Nawawi Arief, *Masalah penegakan hukum dan kebijakan hukum pidana dalam penanggulangan kejahatan*. Prenada Media, 2018.

[6] Council of Europe, "Council of Europe. Convention on Cybercrime (Budapest Convention, ETS No. 185)."

[7] FCC, "Federal Communications Commission (FCC). FCC forfeiture order. Washington, DC: FCC.," 2024.

[8] S. W. Brenner, *Cybercrime: criminal threats from cyberspace*. Bloomsbury Publishing USA, 2010.

[9] A. G. Ferguson, "The rise of big data policing: Surveillance, race, and the future of law enforcement," in *The rise of big data policing*, New York University Press, 2017.

[10] S. Rahardjo, "Legal Science, Bandung." Alumni, 2012.

[11] ENISA, “European Union Agency for Cybersecurity (ENISA). Artificial intelligence cybersecurity challenges: Threat landscape for artificial intelligence. ENISA.”

[12] G. Hallevy, *Liability for crimes involving artificial intelligence systems*, vol. 257. Springer, 2015.

[13] H. T. Muladi, “Prinsip Pengaturan dalam Kriminalisasi dalam Buku Demokratisasi,” *Hak Asasi Mns. dan Reformasi Huk. di Indones. Habibie Center, Jakarta*, 2002.

[14] B. OECD, “Recommendation of the council on artificial intelligence,” *Organ. Econ. Coop. Dev.*, 2019.

[15] F. Pasquale, *The black box society: The secret algorithms that control money and information*. Harvard University Press, 2015.

[16] United Nations Office on Drugs and Crime, “Emerging threats: The intersection of criminal and technological innovation in the use of automation and artificial intelligence in the cybercrime landscape of Southeast Asia. Cybercrime Technical Policy Brief,” *UNODC*, 2025.

BIOGRAPHIES OF AUTHORS

	Maria Angelorum BoekanShe earned her Bachelor of Laws (S1) from Widya Mandira Catholic University, Kupang, with a study period of 3.5 years. Currently, she is pursuing a Master of Laws (S2) at Atma Jaya University, Yogyakarta. Her field of expertise is Criminal Law, with research interests in cybercrime and litigation law, particularly in addressing the challenges of legal protection in the digital era. Maria can be contacted via email: anggyangelorum@gmail.com .