Jurnal Ilmu Hukum Prima
Vol. 8 No. 1 April 2025
E-ISSN : 2614-2244
ISSN : 2088-5288

The Urgency of Establishing Legal Instruments Against Potential Artificial Intelligence (AI) Crimes

Anggada Perkasa[1], Andini Pratiwi Siregar[2], Venia Utami Keliat[3]
PUI-PT Criminal Law and Green Economy, Universitas Prima Indonesia.
Corresponding Author:
anggadaperkasa@unprimdn.ac.id

ABSTRACT
The development of artificial intelligence (AI) has brought significant progress in various sectors, but on the other hand, it also presents the potential for crimes that have not been fully accommodated in the existing legal system. Crimes involving AI, such as deepfakes, data manipulation, autonomous cyber attacks, and misuse of algorithms, raise serious issues in terms of legal accountability, perpetrator identification, and victim protection. The criminal law system in Indonesia, which generally still relies on the principles of legality and the subjectivity of human error, does not yet have adequate legal instruments to address AI-based crimes that are autonomous and adaptive. This study aims to examine the legal vacuum that occurs, evaluate regulations in several other countries as a comparison, and offer the urgency and direction for the formation of new legal instruments in Indonesia. The method used is juridical-normative with a comparative and conceptual approach. The results of the study indicate the need to establish a special legal framework regarding AI, both in the form of new laws and reformulation of criminal norms that can accommodate the unique nature of artificial intelligence. Without adaptive legal reform, Indonesia will face serious legal loopholes that can be exploited by digital criminals.

Keywords: Artificial Intelligence, AI Crime, Legal Void, Criminal Law, Technology Regulation.

INTRODUCTION
The development of artificial intelligence (AI) technology has brought about a major transformation in various aspects of human life, from the industrial sector, health, finance, to the legal system itself. AI's ability to process big data, conduct independent learning (machine learning), and make decisions autonomously makes it a revolutionary technology. However, behind this progress, new challenges arise in the form of potential crimes committed with or by AI systems, which create new complexities in law enforcement.

AI-based crimes have different characteristics compared to conventional crimes and classic cybercrimes. AI can be used to create deepfakes, spread disinformation, perform automated hacking, and run malicious algorithms without direct human intervention. In some cases, it is difficult to determine who should be held accountable: the system creator, the user, the data owner, or even the AI system itself. This situation raises serious legal issues, especially in the context of Indonesian criminal law, which is still oriented towards individual liability based on fault (schuld) and the principle of legality.

E-ISSN : 2614-2244
ISSN : 2088-5288

Until now, Indonesia has not had specific regulations that comprehensively regulate AI-based crimes. The Electronic Information and Transactions Law (UU ITE) and other legal instruments are still general and have not been able to cover the complexity and dynamics of crimes mediated by artificial intelligence. On the other hand, several countries such as the European Union and the United States have begun to develop legal frameworks to regulate the use and potential deviations of AI technology.

Based on these conditions, this paper aims to highlight the urgency of establishing a special legal instrument in Indonesia to anticipate and overcome crimes involving artificial intelligence. By analyzing the existing legal gaps and comparing them with regulatory approaches in several other countries, it is hoped that this study can provide a conceptual contribution to the formulation of national legal policies that are more adaptive to technological developments.

METHOD

This study uses a normative legal approach, namely legal research that focuses on the study of positive legal norms, both those written in laws and regulations and those that develop in legal practice and doctrine. This approach is relevant because the main objective of the study is to identify legal gaps and propose the formation of new legal instruments that are able to answer legal challenges due to the emergence of artificial intelligence (AI)-based crimes.

RESULTS AND DISCUSSION

Legal Gap in Handling AI-Based Crimes in Indonesia

The emergence of artificial intelligence (AI) as a technology capable of performing autonomous actions has caused disruption not only in the economic and social fields but also in the legal system, especially criminal law. Crimes involving AI have unique characteristics: they are automatic, complex, adaptive, and in many cases, do not involve direct human intervention when the unlawful act occurs. This raises a fundamental question: how can the Indonesian criminal law system, which is rooted in the principle of legality and oriented towards human actors, answer this challenge?

To date, there has been no specific regulation in Indonesia that explicitly regulates unlawful acts committed by or with the assistance of AI. Law Number 11 of 2008 concerning Electronic Information and Transactions (UU ITE) does contain provisions related to cybercrime, but its nature is still too general and has not accommodated the diversity of modus operandi that have emerged due to the development of AI. Likewise, the Criminal Code (KUHP) still focuses on human perpetrators as legal subjects and assumes the existence of mens rea (evil intent), which cannot be directly applied to non-human entities such as AI systems.

As a concrete example, in the case of deepfake videos that are automatically created and distributed by AI to defame someone, law enforcement faces obstacles in determining the subject of the perpetrator, the motive, and the structure of responsibility. AI does not have the will or legal awareness like humans, so the dolus (intentional) approach in criminal law becomes irrelevant. This creates a serious legal gap where violations can occur, but cannot be legally qualified in the existing criminal system.

E-ISSN : 2614-2244
ISSN : 2088-5288

In addition, the process of proof in criminal cases involving AI also faces technical and normative challenges. Many AI systems operate through black box algorithms, namely algorithms whose working processes are not fully transparent or cannot be explained by their users themselves. This makes it difficult for law enforcement officers to prove the causal relationship between AI actions and the resulting legal impacts. As a result, victims of crimes caused by AI may not get justice because the legal system is unable to reach and resolve cases effectively.

Furthermore, in the context of national criminal law, there is no clear legal definition of what is meant by "criminal acts by AI" or how AI can be considered a tool of criminal acts or a new legal subject. In fact, along with the increasingly widespread application of AI in public services, banking, autonomous vehicles, and defense and security systems, the potential for misuse of AI by individuals, groups, or autonomously is increasing.

Therefore, this legal vacuum is not only a technical or sectoral problem, but has touched on fundamental aspects of legal protection and criminal justice. Without clear norms and legal instruments, the state risks failing to carry out its function of protecting its citizens from new forms of crime that cannot be anticipated by traditional law.

Complexity of Legal Liability

One of the main challenges is determining the legal subject in criminal acts involving AI. There are several possible perpetrators:

1. AI Developer
2. System owner or user
3. Third parties who abuse AI
4. or even AI itself.

However, the Indonesian legal system has not yet recognized artificial intelligence (AI) as a legal subject, either in the capacity of a public or private legal subject. AI is still positioned passively, namely as a human aid (instrument), not as an entity that has its legal rights and obligations. This is an obstacle in responding to the development of AI, which is increasingly autonomous, complex, and even in some cases able to make decisions without direct human intervention.

In contrast to Indonesia’s conventional legal approach, several discourses at the international level have begun to open discussions on the possibility of recognizing “electronic personhood,” a concept that suggests that autonomous AI entities be given limited legal status like legal entities. The goal is not to equate AI with humans, but rather to create a more realistic framework of legal responsibility for AI systems that can make their own decisions and give rise to real legal consequences. This concept has been proposed in several reports and policy discussions, including in the European Parliament Committee on Legal Affairs (2017) document proposing a special legal status for advanced AI.

However, formal recognition of AI as a legal subject still draws much criticism, both from a legal, ethical, and philosophical perspective. On the one hand, giving legal status to AI can pave the way for more targeted legal accountability. On the other hand, this risks blurring the concept of human responsibility and can become a loophole to avoid accountability, especially by parties who develop or operate AI.

E-ISSN : 2614-2244
ISSN : 2088-5288

In this context, the strict liability or vicarious liability approach is a more rational alternative and can be immediately implemented in the Indonesian legal system. Strict liability allows developers, owners, or operators of AI to be held liable for losses caused by AI even if they are not directly at fault. This approach is commonly applied in cases where the inherent risk of technology is very high, such as in environmental law or traffic accidents.

Meanwhile, vicarious liability allows someone to be responsible for the actions of another party (in this case, AI) if the legal relationship and control between the parties are proven. For example, if a company's AI is used to manipulatively target consumers through a discriminatory algorithm, then the company as the owner or controller of the AI can be held legally responsible for the impacts caused. This approach does not depend on the existence of malicious intent, but rather on the fact of the legal relationship and dominant position over the AI.

The implementation of these two approaches can be a pragmatic solution in overcoming the legal vacuum without having to wait for formal recognition of AI as a legal subject. However, this approach still requires the support of explicit legal norms in the form of new regulations, because the Criminal Code and the ITE Law currently do not have provisions that regulate such a liability model in the context of AI.

Thus, the urgency of establishing new legal instruments becomes even stronger — not only to protect society from AI crimes, but also to provide legal certainty for business actors, technology innovators, and law enforcers in facing the ever-evolving digital crime landscape.

Comparative Study: Other Countries' Responses

In facing the legal challenges posed by artificial intelligence, several countries and regions have taken strategic steps by drafting more progressive and adaptive regulations. Comparative studies of the responses of these countries are important to provide a broader perspective and as a reference in formulating legal policies in Indonesia. These responses are generally focused on two main aspects: regulation of the use of AI and regulation of legal responsibility for the impacts or crimes caused by AI.

a. European Union: European Union Artificial Intelligence Act (EU AI Act)

The European Union is a pioneer in developing a comprehensive legal framework on AI. Through the EU AI Act, which was first proposed in 2021 and is now in the final stage of legislation, the EU applies a risk-based approach. In this approach, AI systems are classified into four categories:

1. Unacceptable risk is prohibited (example: social rating system as in China).
2. High risk – permitted but closely monitored (examples: AI for job recruitment or facial recognition by law enforcement).
3. Limited risk (limited risk) – subject to certain transparency obligations.
4. Minimal risk – free to use.

In the context of crime, this regulation is very important because it establishes the responsibilities of developers and users of AI that cause negative impacts, including legal or social harm. The EU AI Act also requires documentation, audits, and reliability

E-ISSN : 2614-2244
ISSN : 2088-5288

testing of AI systems, including guarantees of non-discrimination and protection of human rights.

b. United States: Regulatory Fragmentation and Civil Liability Approaches

Unlike the European Union, the United States does not yet have a specific federal legal framework that comprehensively regulates the use of AI, including in the context of crime. AI regulation in the US tends to be sectoral and fragmented, depending on the state and the area of use, such as AI in finance, health, or autonomous vehicles.

However, the US legal system is known to be progressive in its approach to civil litigation against technological harm. US courts have begun to apply product liability and negligence principles to AI developers or distributors if they are found to have been negligent in designing a safe and reliable system. This allows victims of AI crimes, such as chatbot-based fraud or discriminatory bias in job selection algorithms, to seek compensation through civil lawsuits.

Additionally, several institutions such as the National Institute of Standards and Technology (NIST) have issued technical guidelines on accountability and fairness in AI systems, although they are not yet legally binding.

c. People's Republic of China: State Supervision and Control Approach

China has taken a different approach from the European Union and the United States, with strict supervision and centralized regulation. The Chinese government has implemented various regulations regarding recommendation algorithms, facial recognition, and restrictions on the use of deepfakes and synthetic content. In 2022, China issued the "Regulations on the Administration of Deep Synthesis Internet Information Services", which requires AI service providers to flag synthetic content (deepfakes) and ensure that it does not mislead the public.

China also requires tech companies to report the algorithms they use to the state, and gives authorities full authority to block AI systems deemed to endanger social stability. While these policies have been effective in preventing the misuse of AI, China's approach has also drawn criticism from the international community for potentially undermining the principles of privacy and civil liberties.

Implications for Indonesia

From the comparative study, it can be concluded that there is no single approach that is completely ideal, but there are important principles that can be adopted by Indonesia:

1. The importance of classifying the risks of AI use (as in the European Union) to prioritize regulation in high-risk sectors.
2. There is a need for flexible legal liability mechanisms, including strict liability and corporate liability, as applied in the US legal system.
3. Strengthening supervision of AI algorithms and systems that have a broad impact on society, as done by China.

Indonesia needs to formulate regulations that not only protect society from the negative impacts of AI but also do not hinder innovation. Therefore, the formation of national regulations on AI

E-ISSN : 2614-2244
ISSN : 2088-5288

needs to be preceded by a multidisciplinary study that includes aspects of law, technology, human rights, and national security.

Urgency of Establishing New Legal Instruments

Given the legal vacuum, complexity of accountability, and international practices, the creation of new legal instruments is an urgent need. These instruments can be in the form of:

1. Special Law on AI, or
2. Amendments to the ITE Law and the Criminal Code include articles relevant to the illegal use of AI.

The instrument should include:

1. Legal definitions of AI and AI-based crimes
2. Classification of risks and types of violations;
3. Criminal and civil liability mechanisms;
4. Protection of victims' rights and rights to personal data;
5. Ethical obligations and transparency of AI developers and users.

CONCLUSION

The rapid development of artificial intelligence (AI) has brought various benefits in the fields of technology, economy, and public services. However, on the other hand, the emergence of increasingly autonomous AI also poses significant legal challenges, especially related to the potential for crimes involving or committed by AI systems. AI-based crimes have unique characteristics - automatic, adaptive, and often without direct human control, making them difficult to reach by the legal system, which currently still focuses on human actors as legal subjects.

To date, there is no specific legal instrument in Indonesia that comprehensively regulates the use, responsibilities, and legal impacts of AI systems. This legal vacuum risks creating legal uncertainty, complicating law enforcement, and opening loopholes for misuse of technology that can harm society, threaten human rights, and damage the existing legal order. Existing legal systems, such as the Criminal Code and the ITE Law, have proven inadequate to respond to new forms of crime arising from the use of AI.

Comparative studies of other countries such as the European Union, the United States, and China show that each country has begun to take progressive steps in building a regulatory framework for AI, both in terms of risk classification, legal responsibility, and oversight mechanisms. This is an important lesson for Indonesia so that it does not lag in forming a legal system that is adaptive and responsive to the challenges of modern technology.

Thus, the urgency of establishing a new legal instrument is very important and urgent. The instrument must be able to address the problem of the absence of norms, establish a fair legal accountability framework, guarantee the protection of community rights, and encourage the use of AI ethically and responsibly. Without proper regulation, AI will not only be a tool for innovation, but can also be a real threat to legal justice and national security.

E-ISSN : 2614-2244
ISSN : 2088-5288

BIBLIOGRAPHY

Indonesian Internet Service Providers Association. (2023). APJII Internet Survey Report 2023. https://apjii.or.id

European Commission. (2021). Proposal for a Regulation laying down harmonized rules on artificial intelligence (Artificial Intelligence Act). Brussels.https://eur-lex.europa.eu

European Parliament Committee on Legal Affairs. (2017). Report with recommendations to the Commission on Civil Law Rules on Robotics (2015/2103(INL)).

Febrian, AY (2022). Legal challenges to the use of Artificial Intelligence in the Indonesian criminal law system. Journal of Law & Development, 52(1), 112–132. https://doi.org/10.21143/jhp.vol52.no1.2853

Fitriyani, R. (2020). Regulation and Legal Protection against Cybercrime from the Perspective of National and International Law. Journal of Law and Economic Development, 8(1), 45–56.

Kusumawardhani, A. (2023). Potential of Artificial Intelligence as a Criminal Act: Indonesian Positive Law Perspective. Scientific Journal of Legal Policy, 17(2), 193–210.

National Institute of Standards and Technology (NIST). (2023). AI Risk Management Framework (AI RMF 1.0). US Department of Commerce.https://www.nist.gov/itl/ai-risk-management-framework

OECD. (2019). OECD Principles on Artificial Intelligence. https://www.oecd.org/going-digital/ai/principles/

Sihombing, D. (2021). Legal responsibility for the use of AI systems in public services. Journal of Law and Technology, 4(2), 78–95.

Tjong, AF (2022). Personhood in the Perspective of Artificial Intelligence: Need or Fear? Journal of Digital Constitution, 6(1), 1–20.

Law Number 11 of 2008 concerning Electronic Information and Transactions (ITE Law), as amended by Law No. 19 of 2016.