Research Article

AI Abuse and Its Implications for Global Environmental Law

Muzaki Adi Nugroho* and Ratih Mega Puspa Sari

Doctoral of Law Program, Universitas Islam Sultan Agung (UNISSULA), Semarang, Indonesia

ORCID

Muzaki Adi Nugroho: https://orcid.org/0009-0000-6323-2130

Abstract.

The development of artificial intelligence (AI) technology has brought extraordinary benefits to various sectors of human life. However, behind its potential, AI also carries serious risks to digital security and the environment. Misuse of AI, including manipulation of emission data, the spread of environmental disinformation, and the use of autonomous AI to hide illegal industrial activities, creates new challenges for criminal law and environmental law. This study uses a normative and conceptual legal approach to examine forms of the misuse of AI and their implications for the global environmental law system. The results show that Indonesia does not yet have adequate regulations. Therefore, it is necessary to establish a new legal framework that is interdisciplinary, responsive to technological developments, and pays attention to the precautionary principle in international environmental law.

Keywords: AI, digital crime, technology abuse

Corresponding Author: Muzaki Adi Nugroho; email: muzakiadinugroho@gmail.com

Published: 3 November 2025

Publishing services provided by Knowledge E

Selection and Peer-review under the responsibility of the 8th Legal International Conference and Studies Conference Committee.

1. Introduction

The rapid development of artificial intelligence (AI) technology in the last decade has had a tremendous impact on human life. However, along with the increasing use, various abuses of AI have emerged that not only threaten data security, information integrity, and public trust, but also have direct and indirect impacts on global environmental law. Abuse of AI can take the form of manipulation of environmental monitoring data, the spread of disinformation related to climate change, and the protection of illegal activities by large corporations. Recent cases have shown the use of AI by several companies to falsify carbon emission data to pass international regulations, as reported by the World Economic Forum (2024) and the UNEP report in 2023. This makes it clear that AI not only poses challenges in the realm of digital criminal law, but also poses a real threat to ecological justice and the international legal order.

The advancement of AI provides great benefits in the industrial, health, education, and legal sectors. However, AI is also used for criminal activities, including the creation of deepfakes, fraudulent chatbots, and environmental data manipulation (Pratama, AR, 2023). In the legal context, this raises new issues because AI systems are often autonomous and not directly controlled by humans (Floridi, L., et al., 2023).

Specifically in the environmental context, AI has been used by corporations to disguise carbon emissions activities, falsify satellite data, and obscure environmental violations (UNEP, 2023). This poses a significant risk to the integrity of global environmental law, given that climate change mitigation efforts depend on legitimate and accountable data (Adams, J., 2024). Indonesia currently does not have regulations that specifically regulate AI. The Criminal Code and the ITE Law do not include autonomous AI systems as legal subjects or objects (Smith, E., 2024).

The digital revolution that has occurred has given birth to various technological innovations that have fundamentally changed the way humans live, work, and interact. One of the most striking innovations in the development of this technology is artificial intelligence (AI). AI is a computer system or machine that is capable of carrying out tasks that usually require human intelligence, such as decision making, pattern recognition, natural language processing, and learning from data independently (Russell, Stuart and Norvig, 2020). The presence of AI has a positive impact on various sectors, such as production efficiency in industry, medical diagnosis in the world of health, optimization of transportation systems, to utilization in the education and legal sectors.

However, along with these developments, the dark side of AI utilization has also emerged. On the one hand, AI provides convenience and efficiency, but on the other hand, this technology is also a potential means for various crimes, especially digital-based ones. Crimes involving AI are complex and difficult to detect conventionally. The forms are also diverse, ranging from the creation of deepfake content to destroy someone's reputation, the spread of false information through intelligent algorithms, the misuse of chatbots to commit online fraud, to the use of AI to break into digital security systems and target users' personal data (Pratama, Aditya Rizky, 2023).

Furthermore, the misuse of AI not only harms individuals or economic sectors, but also has the potential to threaten global environmental sustainability. AI, when used to manipulate environmental monitoring data, disguise illegal industrial activities, or spread false information about environmental impacts, can undermine international monitoring systems and hinder climate change mitigation efforts. In this context, the misuse of

AI becomes an intersection between criminal law and international environmental law, which requires an interdisciplinary approach and cross-border regulation.

In a global framework, the precautionary principle in international environmental law requires caution in the application of new technologies that pose risks to the environment (Birnie, Patricia W., Boyle, Alan E., and Redgwell, Catherine, 2009). Unfortunately, to date there has been no international legal instrument that comprehensively regulates the impact of AI use on the environment. Therefore, a study of the misuse of AI as a criminal act and its implications for global environmental law is very important to support legal reform that not only supports digital justice and security, but also the survival of the planet's ecosystem.

Floridi et al. (2023) stated that AI can have a major ecological impact if used without ethical control (Geller, N., 2023). Pratama (2023) examined how AI is used in cybercrime in Indonesia, but has not discussed much about its impact on environmental law (Dwork, C. & Mulligan, D., 2021).

The UNEP report (2023) highlights that the misuse of AI by companies has an impact on the global monitoring system for carbon emissions (World Economic Forum, 2024). Adams (2024) found that AI was used to modify environmental data to avoid regulations (Kusuma, D., 2024). Another study by Smith (2024) and Geller (2023) shows that international law still has gaps regarding the accountability of AI for environmental damage (Yusuf, M., 2024).

In the context of criminal law in Indonesia, the misuse of AI as a crime has not been explicitly regulated. The current legal framework, such as the Criminal Code (KUHP) and Law Number 11 of 2008 concerning Information and Electronic Transactions (UU ITE), has not been able to comprehensively respond to increasingly complex and transnational AI-based crimes (Law of the Republic of Indonesia Number 11 of 2008 concerning Information and Electronic Transactions (ITE), in conjunction with Law No. 19 of 2016). The mismatch between the speed of technological innovation and the slow adaptation of regulations creates a legal vacuum and the potential for multiple interpretations in the law enforcement process (Arief, Barda Nawawi, 2017).

This phenomenon poses serious challenges for law enforcement, both in terms of technical understanding of the modus operandi of AI-based crimes, as well as in the process of providing evidence and preparing appropriate charges. Moreover, modern AI is not always directly controlled by humans, but can be autonomous, which complicates conventional criminal liability. This raises fundamental legal questions:

can AI be considered a perpetrator of a crime, and if not, who can be held legally responsible? (Dwork, Cynthia and Mulligan, Deirdre K., 2021).

Therefore, this study is very relevant and important, especially in facing the ever-evolving digital era. This study aims to analyze the forms of criminal acts that arise from the misuse of artificial intelligence, review the adequacy and relevance of existing criminal law regulations, and offer normative and practical solutions to strengthen the national legal system to be more adaptive to the dynamics of technology. With an interdisciplinary approach between law and technology, it is hoped that this study can contribute to the formation of progressive legal norms that favor legal certainty, justice, and protection of the digital community.

2. Methods

This study uses a normative and conceptual legal approach, supported by a comparative approach to AI regulation in the European Union, the United States, and Singapore (OECD, 2023). Data were obtained from legal literature, scientific journals, and reports from international organizations between 2023–2025. The analysis technique was carried out qualitatively, with a focus on strengthening adaptive criminal and environmental law regulations to technology. The data collection technique was carried out through library research, namely by reviewing various literature, journals, laws and regulations, and scientific publications both nationally and internationally that are relevant to the topic of AI abuse. Data analysis was carried out qualitatively, by interpreting and compiling data systematically to answer the formulation of the problems that had been set. This analysis is aimed at revealing the normative gaps in the Indonesian legal system and evaluating the effectiveness of existing legal instruments in tackling AI-based digital crimes (Ishaq, 2021).

With this method, it is hoped that research can contribute not only theoretically to the development of legal science, but also practically in compiling recommendations for criminal law policies that are responsive to the dynamics of global environmental law involving artificial intelligence technology.

3. Results and Discussion

3.1. Forms of AI Abuse in Environmental Context

Table 1:

Types of AI Abuse	Modus Operandi	Sample case
Emission Data Manipulation	Changing carbon data to pass regulations	Deepfake Carbon, WEF (2024)[12]
Environmental Disinformation	Bots spread climate hoaxes	Climate Denial Hoax, UNEP (2023)[13]
Activist Deepfake	Fake video to damage activists' credibility	Deepfake Greta Thunberg (2024)[14]
Blurring of Industrial Activities	AI covers up waste disposal tracks	Heavy metal factory, fake satellite imagery case[15]

This situation is contrary to the principles of international environmental law, especially the precautionary principle. Without strict oversight of the use of AI, countries may fail to meet their international obligations to protect the environment.

Forms of Abuse of Artificial Intelligence

Artificial intelligence (AI) has become a multifunctional tool in supporting various human activities. However, its unauthorized use or beyond ethical and legal boundaries creates various forms of abuse that are classified as criminal acts. Based on the results of literature studies and global case analysis, there are several forms of crime that predominantly utilize AI, including:

a. Deepfake

AI technology is used to manipulate video and audio to resemble other people's voices and faces. Deepfakes are often used for defamation, blackmail, non-consensual pornography, and political manipulation (Chesney, Robert & Citron, Danielle K., 2019).

b. AI-Driven Phishing and Chatbot Fraud

Cybercriminals are using AI-based chatbots to run online scams that mimic human conversations. AI-assisted phishing is becoming more convincing and difficult to distinguish from legitimate communications (Barda Nawawi Arief, 2017).

c. Spread of Disinformation

AI algorithms are used to spread fake news (hoaxes) massively through social media bots, influencing public opinion and election results (Tufekci, Zeynep, 2014).

d. Autonomous Hacking and Malware

AI is used to carry out automated attacks on cybersecurity systems with rapid adaptation to defense devices, creating the potential for major losses to personal data and digital infrastructure (Vinay, Singh, 2021).

This crime pattern shows that AI is not only used as a tool, but has become an actor that plays an active role in the stages of crime execution. This changes the criminal landscape from conventional crimes to crimes that are autonomous, automatic, and difficult to track.

3.2. The Void of Positive Legal Regulation in Indonesia

The results of the review of national legal instruments show that Indonesia does not yet have specific regulations that explicitly and in detail regulate crimes involving AI. Law Number 11 of 2008 concerning Information and Electronic Transactions (UU ITE), although it regulates several forms of cybercrime, does not include terminology or technical frameworks related to AI (Law No. 11 of 2008 concerning Information and Electronic Transactions, amended by Law No. 19 of 2016). Meanwhile, the Criminal Code (KUHP) is still general in nature and is not designed to deal with the dynamics of digital crimes based on sophisticated technology.

Due to this gap, law enforcement against AI abuse relies on the interpretation of legal analogy and the principle of lex generalis, which in practice creates legal uncertainty. For example, in the case of the spread of deepfakes, the perpetrator can be charged with defamation or the spread of immoral content in the ITE Law, but the AI technology aspect is not touched at all, so it does not reflect substantive justice (Laily Rahmawati, 2022).

3.3. Law Enforcement Challenges

Law enforcement against AI abuse faces challenges from various aspects, including:

a. Technical Aspects

Law enforcement officers still experience limitations in understanding and tracing the traces of crimes committed with the help of AI. Conventional digital forensics is not yet adequate to detect and prove crimes committed by AI systems that are able to disguise the identity of the perpetrator automatically (Luhut MP Pangaribuan, 2020).

b. Legal Aspects

There is no legal basis for determining who is criminally responsible when crimes are committed by autonomous systems. This raises debate about whether responsibility should be placed on developers, operators, owners, or those who use AI (Hildebrandt, Mireille, 2018).

c. Ethical and Philosophical Aspects

AI raises new moral issues, such as algorithmic fairness, automated discrimination, and potential abuse by states or corporations. Therefore, the law must start thinking about forms of collective accountability and proactive regulation based on human rights (Floridi, Luciano et al., 2018).

3.4. International Practice as a Reference

Several countries have taken progressive steps in regulating and anticipating the risks of AI misuse:

a. The European Union through the Artificial Intelligence Act categorizes AI based on risk (minimal, limited, high and prohibited) and establishes legal obligations for AI developers and providers (European Commission, 2021).

b. The United States is developing AI ethics guidelines through the Blueprint for an AI Bill of Rights, and strengthening the capabilities of the FBI and other law enforcement agencies to address smart technology-based crimes.

c. Singapore adopts a collaborative approach between regulators, developers and civil society within the framework of the Model AI Governance Framework, which is more adaptive to technological changes.

d. Indonesia can learn from this practice by establishing a national legal framework that specifically regulates AI and digital crime, so as not to be left behind in facing the rapid and dynamic wave of technological transformation.

3.5. The Urgency of Integrated Regulation Based on Interdisciplinarity

The development of AI and its cross-sectoral impacts require an integrative legal approach between criminal law, environmental law, and information technology law. Some relevant policy proposals include:

a. Preparation of specific regulations regarding the misuse of AI and its impact on the environment;

b. Establishing ethical and safety standards for AI used in high-risk industries;

c. Establishment of a cross-sector AI oversight body;

d. Strengthening international cooperation in developing a global legal regime that is responsive to the challenges of smart technologies.

With adaptive regulation, AI can not only become a safe innovation tool, but can also contribute to environmental monitoring and the fulfillment of the principles of ecological justice.

4. Conclusion

The misuse of AI is a multidimensional threat that has not been fully anticipated by the Indonesian legal system. In the environmental context, AI is used to hide facts and obscure ecological violations, hampering global efforts to mitigate climate change. Current regulations are inadequate to regulate AI as a legal entity. Therefore, it is necessary to design specific laws that regulate the use, supervision, and legal accountability of AI. Global collaboration is also absolutely necessary to formulate international legal standards that protect ecological justice.

References

[1] Dwork, Cynthia and Mulligan, Deirdre K. "It's Not Just About the Algorithm: AI and Criminal Responsibility." *Stanford Law Review*, Vol. 73, accessed on June 2, 2025, at 8:00 p.m. WIB; 2021.

[2] Floridi, Luciano, et al. "AI4People—An Ethical Framework for a Good AI Society." *Minds and Machines,* Vol. 28, accessed on June 2, 2025, at 21.00 WIB; 2018.

[3] Geller, N., AI and the Rule of Law. *Harvard Journal of Law & Tech,* accessed on June 4, 2025, at 19.00 WIB; 2023.

[4] Pratama, Aditya Rizky. "The Threat of Cybercrime through Deepfake and AI Chatbot: Challenges of Law Enforcement in Indonesia." *Journal of Criminology and Technology*, Vol. 3 No. 1, accessed on June 1, 2025, at 17.00 WIB; 2023.

[5] Yusuf, M. International Challenges of AI and the Environment. *Journal of International Law*, accessed on June 4, 2025, at 20.00 WIB; 2024.

[6] Adams J. AI Manipulation in Environmental Monitoring. Environ Law Rev. 2024.

[7] Arief BN. Kebijakan Legislatif dalam Penanggulangan Kejahatan. Jakarta: Kencana; 2017.

[8] Birnie PW, Boyle AE, Redgwell C. International Law and the Environment. 3rd ed. Oxford University Press; 2009.

[9] Ishaq, *Dasar-Dasar Ilmu Hukum,* Jakarta: Sinar Grafika; 2021.

[10] Kusuma D. Kebijakan Global dan AI. Global Policy Review; 2024.

[11] OECD, 2023, AI and Environmental Governance

[12] Russell, Stuart dan Norvig, Peter. *Artificial Intelligence: A Modern Approach.* 4th Edition. Pearson; 2020.

[13] Smith E. Legal Gaps in AI Environmental Regulation. Environmental Law International; 2024.

[14] UNEP. 2023, *AI and Environmental Monitoring*: Risk Report. Nairobi

[15] World Economic Forum. Deepfake Carbon. Geneva; 2024.

[16] Law of the Republic of Indonesia Number 11 of 2008 concerning Electronic Information and Transactions (ITE), in conjunction with Law No. 19 of 2016

[17] Alegre, S.: Freedom to Think - The Long Struggle to Liberate our Minds. Atlantic Books; 2022.

[18] Teo, S.A.: Human dignity and AI: Mapping the contours and utility of human dignity in addressing challenges presented by AI. Law Innov. Technol. 15, 241–279; 2023. https://doi.org/10.1080/17579961.2023.2184132

[19] Bell, E.: A fake news frenzy: why ChatGPT could be disastrous for truth in journalism. The Guardian; 2023.

[20] Achiume, E.T.: Racial Borders. Georget. Law J. 110; 2022.