JIHAD: Jurnal Ilmu Hukum dan Administrasi
Vol. 8 No. 1 Maret 2026
p-ISSN : 2745-9489, e-ISSNl 2746-3842
DOI: *10.36312/jihad.v8i1.10352/https://ejournal.mandalanursa.org/index.php/JIHAD/issue/archive*

Challenges and Reconstruction of Regulations on the Responsibility of Digital Platforms for the Misuse of Personal Data in the Artificial Intelligence Ecosystem: a Contemporary Cyber Law Perspective

Indra Gatot Sihombing[1], Hana Krisnamurti [2], Nugaraha Pranadita[3], Arie Azhari[4], Dini Eka Setia Gunawan[5], Dinda P Bunga[6], Ade Farida[7]
Universitas Langlangbuana Bandung

Article Info

Article history:
Accepted: 15 January 2026
Publish: 1 March 2026

Keywords:
Cyber Law;
Personal Data;
Artificial Intelligence.

Abstract

This study examines cyber law issues in regulating the responsibility of digital platforms for the misuse of personal data based on Artificial Intelligence. The focus of the study is on the inconsistency between the development of autonomous technology and a legal framework that is still based on a conventional paradigm. This study uses a normative legal method with a legislative and conceptual approach to analyse the regulation of personal data protection and the legal responsibility of digital platforms. The results of the study show that existing regulations do not provide adequate legal certainty, particularly in terms of algorithm control and the division of legal responsibility. Therefore, it is necessary to reconstruct cyber law regulations that place digital platforms as active legal subjects with risk-based obligations and prevention principles. This reconstruction is expected to strengthen the protection of data subjects' rights and ensure the responsible use of Artificial Intelligence.

Corresponding Author:
Arie Azhari
Universitas Langlangbuana Bandung
Email Coresspondent: *arieazhariii@gmail.com*

1. INTRODUCTION

Cyber law is the legal basis for law enforcement against crimes that use electronic and computer means, including money laundering and terrorism (Nugraha Pranadita, 2026). Cyber law is a branch of law that regulates all activities, relationships, and legal consequences arising from the use of information and communication technology in cyberspace (Situmeang, 2020). It covers regulations on electronic transactions, information security, personal data protection, and the responsibilities of digital actors (Ardyawati et al., 2025). The emergence of cyber law is a response to changes in human interaction patterns that are increasingly dependent on digital systems. In this case, cyberspace is understood as a new legal space that transcends national territorial boundaries. Its cross-border, fast-paced, and anonymous characteristics require an adaptive legal approach. Therefore, cyber law cannot be separated from the dynamics of ever-evolving technology (Anwar & Nepri, 2025).

The current development of digital technology is marked by the rapid use of Artificial Intelligence in various sectors of life. Artificial Intelligence is used in financial services, health, education, government, and digital platforms. However, the use of AI is highly dependent on the availability and processing of users' personal data. Personal data is

the main source for training, developing, and optimizing AI systems. This condition creates a new relationship between technology, data, and legal subjects.

Personal data in a legal perspective is understood as any information that can identify a person directly or indirectly. This data has very high economic, social, and strategic value in the digital age. Irresponsible management of personal data has the potential to violate privacy rights and cause serious harm to individuals. In the digital ecosystem, personal data is often collected on a massive scale by digital platforms. This process is often carried out without transparency and the fully informed consent of users. This shows an imbalance of power between data owners and data managers.

Digital platforms, as electronic system operators, play a central role in the collection and processing of personal data. They act as both controllers and processors of data in many digital activities. In practice, digital platforms utilize user data for business interests, recommendation algorithms, and AI development. However, the legal responsibility of digital platforms is often not commensurate with the amount of power they wield. Regulatory loopholes are still found in determining the limits of their obligations and responsibilities. This condition is a crucial issue in contemporary cyber law (Isdayani et al., 2024).

The issue becomes even more complex when the misuse of personal data involves Artificial Intelligence systems (Sri et al., 2025). AI can process data automatically without direct human intervention. As a result, it is difficult to determine who is responsible when a violation occurs. Does the responsibility lie with the AI developer, the platform provider, or the system user? This ambiguity raises serious legal issues. Cyber law is required to be able to answer questions of legal responsibility in autonomous systems. On the other hand, personal data protection regulations in many countries are still in the development stage. Existing regulations often lag behind the pace of technological innovation. Some regulations still focus on conventional data processing and do not fully anticipate the characteristics of AI. This results in legal norms that are ineffective in preventing the misuse of personal data. The disconnect between regulations and technological reality has the potential to create a legal vacuum. This vacuum can be exploited by digital businesses to avoid responsibility (Nugraha Pranadita, 2026).

Globally, differences in data protection standards between countries also pose a challenge. Digital platforms operate across jurisdictions by exploiting regulatory differences. Countries with weak data protection are often targets for data exploitation (Mardiyanti, 2025). This raises issues of jurisdiction and cross-border law enforcement. Cyber law faces limitations in reaching violations that occur outside national jurisdictions. This situation highlights the urgency of harmonizing cyber laws at the international level.

In addition to regulatory aspects, ethical issues cannot be ignored in the use of AI and personal data. AI algorithms have the potential to reinforce bias, discrimination, and social injustice. Personal data that is processed without supervision can be used to manipulate behavior and public opinion. This practice threatens democratic values and human rights. Cyber law should not only be oriented towards legal certainty, but also justice and the protection of fundamental rights. Thus, a normative approach needs to be combined with an ethical approach (Fatimah et al., 2025).

The responsibility of digital platforms in the AI ecosystem is a central issue that requires legal reconstruction. The traditional concept of responsibility based on human error is becoming less relevant. AI systems can make decisions independently based on algorithms and data. Therefore, a more progressive concept of legal responsibility is needed. The concepts of strict liability or shared liability are beginning to be considered in cyber law discourse. This aims to ensure effective protection for data owners. In Indonesia, regulations related to personal data protection and the implementation of electronic systems have

undergone significant developments. However, regulations regarding AI and the responsibility of digital platforms are still general in nature. Existing norms do not specifically regulate the risk of data misuse in AI systems. As a result, law enforcement often faces normative and technical obstacles. This condition shows the need to strengthen the national cyber law legal framework. This strengthening must be in line with global technological developments.

Academic studies at the doctoral level need to take on a strategic role in responding to these issues. A critical and interdisciplinary approach is needed to analyze the relationship between law, technology, and digital power. Cyber law should not be understood merely as a set of norms, but as an instrument of social engineering. Through in-depth study, a more adaptive and equitable regulatory model can be formulated. This is important to ensure that the law does not lag behind technological innovation. Thus, academic contributions become highly relevant.

2. METHOD

This study uses a normative (doctrinal) legal approach, which places law as a set of prescriptive norms. This type of research was chosen because the focus of the study is directed at analyzing regulations, concepts, and principles in cyber law, particularly regarding the responsibility of digital platforms for the misuse of personal data based on Artificial Intelligence (Sugiyono, 2022). The research is not intended to assess public behavior, but rather to examine the consistency and adequacy of applicable legal norms (Muhaimin, 2020). Thus, this approach is appropriate for theoretical and normative studies.

The research data sources are legal materials, not empirical data. Primary legal materials include laws and regulations related to information technology, personal data protection, and electronic systems (Alliarrahman, 2023). Secondary legal materials include legal literature, scientific articles, dissertations, and the views of experts relevant to cyber law and artificial intelligence. Meanwhile, tertiary legal materials, such as legal dictionaries and encyclopedias, are used to clarify terms and concepts. These sources are selected selectively to ensure that the analysis remains valid and in-depth (Napitupulu, 2023).

Data collection techniques are carried out through literature studies by searching, inventorying, and classifying primary, secondary, and tertiary legal materials. The data obtained was then analyzed qualitatively using legal reasoning, through legal interpretation and conceptual studies of applicable norms (Sari & Irawaty, 2023). The results of the analysis were used to develop arguments and normative recommendations (Nadya et al., 2025).

3. RESULTS AND DISCUSSION

RESULTS

Cyber law regulations essentially aim to provide legal certainty for all activities involving the use of information technology as an extension of legal activities in the real world. Through the Electronic Information and Transactions Law, digital space is recognized as a legal space that is valid and binding for every legal subject. This recognition affirms that electronic interactions have legal consequences equivalent to conventional interactions.

Cyber law regulations essentially aim to provide legal certainty for all activities involving the use of information technology as an extension of legal activities in the real world. Through the Electronic Information and Transactions Law, digital space is recognized as a legal space that is valid and binding for every legal subject. This recognition affirms that electronic interactions have legal consequences equivalent to conventional interactions.

However, the constructed norms are still oriented towards conventional electronic systems that are linear in nature and under direct human control. The development of Artificial Intelligence (AI) has introduced data processing mechanisms that are automatic, adaptive, and continuous without direct human intervention. This change in the nature of technology has led to a mismatch between the normative assumptions of lawmakers and the operational reality of technology. This mismatch has weakened the effectiveness of norms in providing legal protection.

The Personal Data Protection Law recognizes personal data as a legal right that must be respected and protected. This protection includes the principles of legality, purpose limitation, accuracy, security, and accountability of data controllers. However, the application of these principles faces serious challenges in AI systems that process data massively, in layers, and continuously evolve through machine learning. This condition makes it difficult to control the purpose of data processing as required by law and has the potential to systematically reduce the protection of data subjects' rights.

Within the national legal framework, digital platforms are positioned as controllers and processors of personal data. This position carries active, preventive, and ongoing legal obligations. Platforms are not only obliged to secure data, but also to ensure that data is used in accordance with its purpose.

Within the national legal framework, digital platforms are positioned as controllers and processors of personal data. This position carries legal obligations that are active, preventive, and ongoing. Platforms are not only obliged to secure data, but also to ensure that data is used for legitimate purposes. In practice, platforms often prioritize economic interests and algorithmic efficiency, and use standard clauses to limit legal liability. This practice has the potential to conflict with the principles of legal protection and balance between parties.

AI expands the function of digital platforms from service providers to algorithm-based decision makers that directly impact the rights and interests of data subjects. In positive legal systems, decision making is always associated with legal subjects who can be held accountable. However, AI obscures the relationship between actions, actors, and legal consequences, making it difficult to apply the classic concept of accountability.

Analysis shows that digital platforms have dominant control over the entire life cycle of AI systems, from design and operation to determining system objectives. This control places platforms as the main legal subjects responsible. Platforms' claims of neutrality are not in line with the facts of technological control.

The misuse of personal data in AI systems carries high risks and has far-reaching consequences, including privacy violations, excessive profiling, algorithmic discrimination, and behavioral manipulation. Although the law emphasizes prevention as a key principle, existing regulations do not specify AI risk mitigation obligations in detail. As a result, legal protection tends to be reactive rather than preventive.

Analysis shows that digital platforms have dominant control over the entire life cycle of AI systems, from design and operation to determining system objectives. This control places platforms as the main legal subjects responsible. Platforms' claims of neutrality are not in line with the facts of technological control.

The misuse of personal data in AI systems carries high risks and has far-reaching consequences, including privacy violations, excessive profiling, algorithmic discrimination, and behavioral manipulation. Although the law emphasizes prevention as a key principle, existing regulations do not specify AI risk mitigation obligations in detail. As a result, legal protection tends to be reactive rather than preventive.

AI expands the function of digital platforms from service providers to algorithm-based decision makers that directly impact the rights and interests of data subjects. In

positive law systems, decision making is always associated with legal subjects who can be held accountable. However, AI obscures the relationship between actions, actors, and legal consequences, making it difficult to apply the classic concept of accountability.

Analysis shows that digital platforms have dominant control over the entire life cycle of AI systems, from design and operation to determining system objectives. This control places platforms as the main legal subjects responsible. Platforms' claims of neutrality are not in line with the facts of technological control.

The misuse of personal data in AI systems carries high risks and has far-reaching consequences, including privacy violations, excessive profiling, algorithmic discrimination, and behavioral manipulation. Although the law emphasizes prevention as a key principle, existing regulations do not specify AI risk mitigation obligations in detail. As a result, legal protection tends to be reactive rather than preventive.

DISCUSSION

The discussion regarding the responsibility of digital platforms in the Artificial Intelligence ecosystem cannot be separated from the framework of the Personal Data Protection Theory, which places personal data as a fundamental right of legal subjects. This theory provides a normative basis for assessing the suitability of data processing practices with the principles of legality, fairness, transparency, purpose limitation, data minimisation, and accountability. In the context of automated and adaptive AI, the application of these principles faces structural challenges that require in-depth analysis to ensure that the protection of data subjects' rights remains guaranteed.

1. Principles of Lawfulness, Fairness, and Transparency

A review of the literature shows that the principles of legality, fairness, and transparency are the main foundations of personal data protection. In the context of artificial intelligence systems, these principles face significant challenges because data processing is complex and not easily understood by data subjects. Several studies confirm that closed algorithms (black boxes) hinder transparency, so that data subjects do not know how their data is collected, analysed, and used in automated decision-making. Research findings also show that user consent is often a formality through standard clauses that are difficult to understand, thereby reducing the meaning of fairness in data processing. This condition shows that the application of the principle of transparency in the AI ecosystem is still normative and has not been fully realised in substance.

2. Purpose Limitation Principle

Based on the results of the study, the principle of purpose limitation faces serious pressure in AI systems designed to continuously learn from data. The literature shows that data initially collected for a specific purpose is often reused for algorithm training, product development, or user behaviour analysis. This practice is known as function creep, which is the expansion of data use beyond the original purpose agreed upon by the data subject. Interviews with technology practitioners in several studies revealed that the business models of digital platforms depend on the continuous use of data, making it difficult to strictly enforce purpose limitation. This situation highlights the tension between the need for technological innovation and the legal obligation to limit the purpose of data processing.

3. Data Minimisation Principle

A literature review shows that the data minimisation principle is difficult to apply in AI ecosystems that rely on big data. Machine learning systems require large amounts of data to improve the accuracy and performance of algorithms. Several studies reveal that digital platforms tend to collect data on a massive scale, including data that is not directly relevant, on the grounds that it may be needed for future analytics. This practice demonstrates a shift from the principle of data restriction towards the logic of

data accumulation as an economic asset. These findings indicate a conflict between the technical requirements of AI and the legal obligation to limit data collection to what is relevant and proportionate.

4. Principle of Accountability

The study shows that the principle of accountability is becoming increasingly complex in an AI ecosystem involving many actors. The literature confirms that AI development and operation involves software developers, infrastructure providers, data controllers, and other third parties. This complexity makes it difficult to determine who is responsible when data breaches or algorithmic decisions occur that harm data subjects. Several studies have also found that digital platforms often claim to be neutral intermediaries, even though they have dominant control over the design and purpose of AI systems. This situation shows that accountability in AI systems requires a new approach that emphasises responsibility based on the level of control and economic benefits obtained.

4. CONCLUSION

. The development of Artificial Intelligence has posed fundamental challenges for cyber law regulation, particularly in the protection of personal data and the accountability of digital platforms. The existing legal framework is not yet fully capable of addressing the autonomous, complex, and high-risk nature of this technology. The imbalance between technological mastery and legal control has the potential to weaken the protection of data subjects' rights. Therefore, it is necessary to reconstruct regulations that place digital platforms as legal subjects with proportional obligations and responsibilities. Legal reforms must be oriented towards risk prevention, legal certainty, and the protection of human rights. With this approach, cyber law can function effectively in overseeing the fair and responsible use of Artificial Intelligence.

5. ACKNOWLEDGMENTS

The authors gratefully acknowledge the Master of Law Program, Universitas Langlangbuana, for its institutional and financial support, which made this research possible

6. BIBLIOGRAPHY

Alliarrahman, M. S. (2023). *Perlindungan hukum terhadap pengguna layanan penyelenggara sistem elektronik akibat penyalahgunaan data pribadi*. Jakarta.

Anwar, S., & Nepri, J. E. (2025). Harmonisasi hukum digital: Tantangan global dan strategi adaptif Indonesia dalam era kedaulatan siber. *STAI Bumi Silampari, 4*(1), 69–88.

Ardyawati, A. H., et al. (2025). The role and existence of law in society in the digital era. *MHI, 3*(4), 433–439.

Fatimah, F., et al. (2025). Communication ethics in the collection and use of personal data in the digital era. *Jurnal Bisnis Mahasiswa, 5*(6).

Isdayani, Thamrin, A. N., & Milani, A. (2024). Implementasi etika penggunaan kecerdasan buatan (AI) dalam sistem pendidikan dan analisis pembelajaran di Indonesia. *Digital Transformation Technology, 4*(1), 714–723. https://doi.org/10.47709/digitech.v4i1.4512

Mardiyanti, S. (2025). Konstitusionalitas perlindungan data pribadi sebagai bagian dari hak atas rasa aman. *Disiplin, 31*(3), 209–222.

Muhaimin. (2020). *Metode penelitian hukum*. Mataram University Press. https://eprints.unram.ac.id/20305/1/Metode%20Penelitian%20Hukum.pdf

Muladi, & Arief, B. N. (2010). *Teori-teori dan kebijakan pidana*. Alumni.

Nadya, R., Amalia, I., & Rachman, I. F. (2025). Analisis potensi dan tantangan dalam penggunaan AI di bidang pendidikan. *Semantik: Jurnal Riset Ilmu Pendidikan, Bahasa dan Budaya, 3*(2).

Napitupulu, D. (2023). Kajian peran cyber law dalam memperkuat keamanan sistem informasi nasional. *Medianeliti, 1*(3).

Nugraha Pranadita. (2026a). *Hukum siber / cyber law*. Universitas Lang Lang Buana.

Nugraha Pranadita. (2026b). *Internet sebagai sarana interaksi*. Bandung.

Sari, I. N., & Irawaty. (2023). Tinjauan yuridis terhadap perlindungan konsumen atas produk digital dalam transaksi elektronik. In *Hukum dan lingkungan* (pp. 774–805).

Situmeang, S. M. T. (2020). *Cyber law*. CV Cakra.

Sri, F., Latowa, M., & Sunadi, I. G. E. (2025). Pemanfaatan artificial intelligence (AI) sebagai inovasi digital dalam tata kelola pemerintah daerah. *J-Multitechno (Jurnal Multi Technology), 3*(2), 44–53.