# Indonesia's Legal Policy on Protecting Personal Data from Artificial Intelligence Abuse

*Abidin* Fikri[1,*], *Tina* Amelia[1]

[1] Faculty of Law, Borobudur University, Indonesia

**Abstract.** The rise of artificial intelligence (AI) has produced advanced tools performing tasks traditionally done by humans, but this progress introduces significant legal, ethical, and security challenges. These challenges encompass concerns about individual privacy, data security, legal liability, biases in AI decision-making, and the necessity for international collaboration on regulatory frameworks that balance innovation with public protection. This research analyzes the roles and responsibilities of governments, companies, and individuals in safeguarding personal data from AI misuse. Employing normative juridical methods with statutory and analytical approaches, it focuses primarily on Indonesia's Law Number 27 of 2022 on Personal Data Protection and Law Number 19 of 2016, which amends Law Number 11 of 2008 on Electronic Information and Transactions. While Indonesia's Personal Data Protection (PDP) Law aims to prevent misuse by AI through comprehensive regulations and clear data protection measures, it does not specifically address challenges posed by AI technology. Given AI's ability to process large-scale data rapidly, there's an increased risk of personal data misuse if not closely monitored. Therefore, reform is needed to develop regulations that are more specific and adaptable to AI developments, including establishing specialized agencies to monitor and prosecute AI-related personal data misuse.
Keywords**:** Artificial Intelligence; Misuse; Personal Data Law

## 1 Introduction

The advent of artificial intelligence (AI) has led to the development of sophisticated tools and systems that are capable of performing tasks that were previously the exclusive domain of humans. However, the implications of AI extend beyond the realm of technology. As AI becomes more sophisticated, it is entering domains that carry profound legal implications. The ability of AI to massively process and analyse data raises a number of legal questions, including those related to individual privacy, system security, legal liability, and more.[1]

The development of artificial intelligence technology has brought about revolutionary changes in various aspects of human life. One aspect that is the subject of much debate is the privacy challenges that arise as a result of the penetration of artificial intelligence in data collection, analysis, and management. Artificial intelligence has transcended the boundaries of conventional technology and changed the way we work, interact and access information.[2] The development of artificial intelligence is fundamentally dependent on

* Corresponding Author: abidinfikri001@gmail.com

data, be it user data, behavioural data, or other data. The use of this data, while critical in advancing technology, opens the door to privacy issues that require serious legal attention.

The advent of artificial intelligence (AI) technology has ushered in a new era of decision-making, prompting profound ethical considerations.[3] AI systems are capable of making intricate decisions, often exceeding the capabilities of humans. Consequently, AI-driven decisions can have a profound impact on individuals, society, and the environment. This calls for a nuanced understanding of the scale of responsibility and ethical considerations associated with AI. Furthermore, AI algorithms, which form the foundation of decision-making, may exhibit certain biases or predispositions. This underscores the need for a comprehensive examination of the ethical implications of AI. This creates ethical challenges, as decisions taken by artificial intelligence may create or perpetuate inequality, discrimination or injustice.[3]

Artificial intelligence decisions are often complex and difficult to understand by users or even by policy makers. Understanding and taking responsibility for these decisions becomes an ethical issue that requires clarification and a clear legal framework. In making decisions that affect everyday life, artificial intelligence raises questions about the social and human impact of its decisions. The ethical challenges here involve considerations about human values, fairness and the long-term impact on society. The importance of developing ethical guidelines and decision standards for the development and use of artificial intelligence is important. This research explores the legal measures that can be taken to formulate guidelines and standards that can accommodate the ethical values of society at large.

The pervasive deployment of artificial intelligence (AI) technology not only engenders innovation but also gives rise to significant security concerns. Threats to AI systems from cyber-attacks and manipulation have the potential to inflict severe consequences and necessitate rigorous legal scrutiny.[4] The advent of increasingly sophisticated AI technologies gives rise to intricate potential risks. Threats may emanate from external cyber-attacks, internal misuse, or even the manipulation of AI algorithms with the aim of undermining the integrity and functionality of the system. The potential for cyberattacks against artificial intelligence systems to cause significant harm extends beyond mere data integrity concerns. Such attacks could also manipulate algorithms to produce undesirable decisions. The legal challenges associated with this phenomenon include data protection, attack detection, and the handling of the consequences of cyberattacks against artificial intelligence.

The security of artificial intelligence also encompasses the protection of user privacy. Threats related to unauthorised data collection or misuse of personal information are a significant concern, necessitating the establishment of an adequate legal framework to protect the rights of individuals. Manipulation of artificial intelligence algorithms can erode public trust in these technologies. Legal challenges arise in the drafting of guidelines and regulations that can prevent manipulation and establish liability in the event of manipulation. Innovation in the field of artificial intelligence frequently entails the development of sophisticated algorithms and technologies. The legal challenges associated with this field include the protection of intellectual property to encourage innovation while avoiding security risks related to theft or misuse. Given the global nature of artificial intelligence development and use, international collaboration in security efforts is crucial. This research reviews the legal measures that can be taken to facilitate international collaboration to counter threats to artificial intelligence systems.

Artificial intelligence software is defined as a system that combines machine learning and the ability to learn from data (autonomy learning) without rule-based programming.[5] Artificial intelligence encompasses a range of disciplines, including machine learning, natural language processing, expert systems, vision, speech, planning, and robotics.[6] The relationship between artificial intelligence and the field of law has a long history, spanning

approximately 30 years. This has resulted in artificial intelligence not being a novel concept in the legal domain. However, the utilisation of artificial intelligence technology in government systems, the legal industry, and legal professionals in the preceding years was relatively slow. With the advent of the fourth industrial revolution, there was a notable increase in interest in artificial intelligence, which occurred due to the necessity to transform legal services and the availability of legal data. The impact of AI technology is also evident in law school curricula, where there is a growing emphasis on computer-based learning, and a proliferation of legal technology start-ups, legal technology associations, and legal technology conferences. Additionally, some American and European law schools have established research and training centres on "law and artificial intelligence technology," and robot lawyers and robots capable of producing legal decisions have begun to be developed.

The exponential growth of artificial intelligence technology necessitates the implementation of intelligent regulatory frameworks to safeguard the public interest while facilitating technological advancement. Effective regulatory measures must strike a delicate balance between safeguarding the public interest and fostering innovation in the field of artificial intelligence, while also addressing concerns related to privacy and data protection in the context of the utilisation of artificial intelligence technologies. Regulations must delineate clear responsibilities for developers and users of artificial intelligence systems. In the context of globalisation, international cooperation in the design of artificial intelligence regulations is becoming increasingly crucial. The challenges of privacy and data protection in the context of artificial intelligence receive special attention from a legal perspective. This research discusses the legal philosophy's assessment of the need to protect individuals' privacy and give users greater control over their personal data. Regulation is a key component in responding to the legal challenges of artificial intelligence.

From the preceding analysis, it can be discerned that there is a need to formulate a problem statement. This can be expressed as follows: What are the current personal data protection policies in Indonesia to prevent misuse by artificial intelligence? What are the roles and responsibilities of governments, companies and individuals in ensuring the protection of personal data from misuse by artificial intelligence?

## 2 Method

This type of research employs normative juridical research methods, utilising a statutory approach and an analytical approach.[7] This methodology will include analysis of laws and regulations, government policies and other legal documents relevant to cybersecurity and personal data protection The research will take an in-depth look at Law Number 27 Year 2022 on Personal Data Protection and Law Number 19 of 2016 concerning Amendments to Law Number 11 of 2008 concerning Electronic Information and Transactions and their implementing regulations to identify the weaknesses and strengths of the existing regulations. In addition, case studies and court decisions related to the misuse of personal data will be analysed to see how the law is applied in practice.[8]

## 3 Discussion and Analysis

### 3.1 Indonesia's Current Personal Data Protection Policies in Preventing Misuse by Artificial Intelligence

Artificial intelligence (AI) is the simulation of human intelligence replicated in machines and programmed to operate similarly to humans. McLeod and Schell define AI as the use of machines such as computers that exhibit intelligent human-like behaviour. Therefore, AI is a computer system capable of performing tasks that would normally require human intervention. AI collects and uses information to increase its knowledge and has the ability to self-correct automatically. In the context of chatbot technology, artificial intelligence assumes the role of providing expedient and pertinent responses to user queries, even in the context of acquiring knowledge about country traditions.[9] Chatbots utilise a range of social media platforms, including LINE, Telegram and Facebook, to operate, offering a diverse array of services that leverage their synthetic intelligence.[10] As a subset of computer programs, artificial intelligence technology shares similarities with regular computer program technology. The distinguishing feature of artificial intelligence is the form of programme execution instructions, which consist of more complex algorithms and programming languages. Artificial intelligence is capable of making decisions according to the judgement of its programme, which resembles the ability of human reason. In contrast, ordinary computer programmes have been directed to certain actions through their predetermined algorithms and programming languages.[11] The rapid advancement of digital technology has brought about significant changes in various sectors, including the financial industry. In Indonesia, the government has taken steps to address the issue of personal data protection in the face of these technological advancements.[12] Artificial intelligence is created to mimic human intelligence and can then be similarly applied to a machine to perform tasks with a high degree of accuracy and consistency.[13]

In general, personal data can be defined as data containing information on a person's identity, which can take the form of personal codes, symbols, letters, or numbers that are only attached to each individual.[14] Currently, within the scope of existing data protection arrangements in Indonesia, there is no specific legal instrument that regulates the utilisation and protection of personal data. In the meantime, the current regulations governing this matter are still contained and scattered in several laws that only reflect aspects of personal data protection in general. Furthermore, regulations that specifically contain aspects of personal data protection have not yet been passed. The aforementioned general personal data protection arrangements include Law No. 8/1997 on Company Documents, Law No. 36/1999 on Telecommunications, Law No. 24/2013 on Population Administration, Law No. 19/2016 on Electronic Information and Transactions, Law No. 36/2009 on Health, and Law No. 43/2009 on Archives. Nevertheless, the present study is confined to the protection of personal data that is directly related to electronic data.

The current personal data protection policies in Indonesia, as outlined by the Personal Data Protection (PDP) Law, aim to prevent misuse of personal data by artificial intelligence (AI) through several key provisions. The PDP Law defines personal data as any data relating to an identified or identifiable natural person that can be identified on its own or in combination with other information, either directly or indirectly through an electronic or non-electronic system. This includes data processed by AI systems. The law recognizes six legal bases for processing personal data, including explicit consent, contractual obligation, legal obligation, vital interests, public interest, and legitimate interest. This ensures that AI systems operate within a legal framework and do not process data without a valid basis.

The law emphasizes data ownership rights and prohibits unauthorized data use. This includes ensuring that AI systems do not misuse or access personal data without proper authorization. The PDP Law requires both prior and post notifications to the regulator for cross-border personal data transfers, which includes data transfers involving AI systems. This helps in monitoring and preventing potential misuse of data. Failure to comply with the PDP Law can result in administrative sanctions, including written warnings, temporary suspension of data processing, orders to erase or destroy personal data, and administrative fines up to 2%

of annual revenue or sales. This serves as a deterrent for potential misuse of personal data by AI systems. Organizations are encouraged to adopt a data-centric security approach, which includes strong authentication and access management solutions. This helps in protecting sensitive data and ensuring that AI systems operate within secure environments.

The misuse of personal data through AI has some important differences compared to the general misuse of personal data. These differences are mainly related to the complexity of AI technology and its impact on the processing of personal data. First, the scale and speed of data processing by AI is much higher than traditional methods. AI can process large amounts of data very quickly and efficiently, and combine multiple data sources in a short period of time. Second, AI has advanced analytics capabilities that can identify complex patterns and make predictions about user behavior based on the data collected, which is difficult to achieve through manual analysis. Third, AI is capable of making automated decisions based on processed data, which can accelerate actions without human intervention and directly affect individuals without sufficient transparency. Fourth, privacy risks increase as AI can combine data from multiple sources and reveal deeper information about individuals, as well as be used for mass profiling and surveillance, which can lead to serious privacy violations.

The regulation of personal data security in Indonesia, particularly regarding the use of various digital services, is covered by several legislative instruments. These include the Electronic Information and Transactions (ITE) Law (Law Number 19 of 2016), the Implementation of Electronic Systems and Transactions (Government Regulation Number 82 of 2012), and the Minister of Communication and Information Technology Regulation Number 20 of 2016. Some of these regulations provide legal definitions for "personal data." Article 26, paragraph (1) of the ITE Law states that "unless otherwise provided by laws and regulations, the use of any information through electronic media concerning a person's personal data must be carried out with the consent of the person concerned." While the law does not explicitly define personal data, Article 26 implies that personal data protection is a facet of privacy rights within the realm of information technology. The existence of information and communication technology in people's lives plays an important role and has changed the behavior of society and human civilization globally.[15] According to Article 26 of the ITE Law, personal rights can be defined as the right to enjoy a private life free from interference, the right to communicate with others without surveillance, and the right to control access to one's personal life and data.

In Indonesia, the protection of personal data is primarily governed by the Personal Data Protection Act (*Undang-Undang Perlindungan Data Pribadi,* UU PDP), which aims to regulate the collection, processing, and storage of personal data to prevent misuse, including by artificial intelligence (AI). This legislation defines personal data and sensitive personal data, applying to all entities (both public and private) that process personal data within Indonesia and to those outside Indonesia that affect Indonesian data subjects. It establishes fundamental rights for data subjects, such as the rights to access, correct, and delete personal data, the right to withdraw consent and object to data processing, and the right to data portability.[16]

Further stipulations regarding the protection of personal data are set forth in Article 1, paragraph 1, of the Regulation of the Minister of Communication and Information Technology Number 20 of 2016, which states, "certain individual data that is stored, maintained, and maintained for the truth and protected for its confidentiality." Based on the definitions of personal data that have been elucidated in various laws and regulations, it can be concluded that the protection of personal data specifically emphasizes the safeguarding of an individual's right to privacy. The key aspects of data protection are the individual's right to determine which data can be revealed, to whom, and to what extent, and the protected object in this case is information about a person's personal data. Therefore, the protection of personal data is important because it relates to a person's right to privacy. The right to privacy

is an inherent human right that is guaranteed in Article 28 G paragraph (1) of the 1945 Constitution. This article states that "everyone has the right to protection of self, family, honour, dignity, and property under his control, and is entitled to a sense of security and protection from threats of fear to do or not do something that is a human right." In light of the aforementioned article, it can be inferred that the state bears a legal obligation to safeguard the personal rights of its citizens. However, the piecemeal approach to regulating the protection of personal data in Indonesia suggests that the legislative focus has not been on the protection of the right to privacy of personal data.[17] The Research Director of the Institute for Community Studies and Advocacy identified this issue and asserted that the absence of adequate regulations has resulted in law enforcement being ineffective in safeguarding the disclosure of personal data.[18]

The Act mandates several data processing principles, including lawfulness, fairness, and transparency. Data must be collected for specified, explicit, and legitimate purposes (purpose limitation), and only data necessary for the intended purpose should be collected (data minimization). Additionally, personal data must be accurate and kept up to date (accuracy), not kept longer than necessary (storage limitation), and protected with appropriate security measures (integrity and confidentiality).[19]

One of the cornerstone requirements of the UU PDP is that personal data processing must generally be based on the consent of the data subject, which must be informed, explicit, and freely given. Data subjects need to be informed about the purposes of data collection and processing, the data retention period, and their rights. Organizations processing large amounts of personal data are required to appoint a Data Protection Officer (DPO), who is responsible for overseeing data protection strategies and ensuring compliance with the UU PDP. In the event of a data breach, organizations must notify the authorities and affected data subjects within a specified timeframe, enhancing transparency and accountability.

Cross-border data transfer is another critical area addressed by the UU PDP. It restricts transferring personal data outside Indonesia unless the destination country has adequate data protection measures or specific consent has been obtained. This provision ensures that personal data remains protected, even when transferred internationally. Sanctions and penalties under the UU PDP include administrative sanctions such as fines, suspension of data processing activities, and revocation of licenses. In severe cases, criminal penalties, including imprisonment, may be imposed.

While there are fundamental similarities between the legal principles and rules governing the misuse of personal data in general and the use of AI, the key differences lie in the scale, speed, analytical capabilities, automation and higher privacy risks associated with the use of AI. Therefore, while the same legal basis may apply, supervisory and enforcement approaches may need to be adapted to address the unique challenges posed by AI technologies.

While the PDP Law and the ITE Law have regulated the protection of personal data in general, they have not specifically addressed the challenges posed by the use of AI technology. AI technology has the ability to process data on a large scale and at high speed, which can increase the risk of misuse of personal data if not closely monitored. For example, AI can be used for profiling or automated decision-making, which can have a significant impact on individuals without their awareness or clear consent.

In addition, oversight and law enforcement related to the protection of personal data through AI still requires technical and regulatory capacity building. Currently, Indonesia does not have a dedicated unit focused on dealing with AI-based cybercrime, resulting in weak detection and prosecution of crimes involving this advanced technology.

Therefore, there is a need to reform regulations that are more specific and adaptable to the development of AI, including the establishment of a specialised agency or unit to monitor and prosecute the misuse of personal data through AI.[20] This reform should include the

revision of the PDP Law and the ITE Law to include provisions relevant to AI technologies, as well as increased cooperation between the government, private sector and society to create a robust personal data protection ecosystem that is responsive to modern technological challenges.

### 3.2 The Roles and Responsibilities of Governments, Companies and Individuals in Ensuring the Protection of Personal Data from Misuse by Artificial Intelligence

The development of regulations related to restrictions on the use of artificial intelligence technology in Indonesia in order to prevent misuse has undergone several significant stages, which demonstrate efforts to provide legal certainty in the use of such technology.[21] The Indonesian government has begun to recognise the importance of regulating artificial intelligence through various initiatives, such as the preparation of a national action plan for the development of artificial intelligence.[22] In order to implement artificial intelligence effectively in Indonesia, the Agency for the Assessment and Application of Technology (BPPT) has issued the National Strategy for Artificial Intelligence Indonesia 2020-2045. However, the strategy is currently still in the general policy discussion stage and has not yet been detailed in terms of implementation. This is a concern, given that many companies in Indonesia have developed and utilised AI technology in their operations. In particular, strategic sectors such as banking, e-commerce, and healthcare have incorporated artificial intelligence technology into their business processes.

As the adoption of artificial intelligence (AI) continues to grow, there is an increasing need to ensure the responsible and ethical use of these technologies, particularly when it comes to the protection of personal data. This is especially important in light of the recent enactment of Law Number 27 Year 2022 on Personal Data Protection and Law Number 19 of 2016 concerning Amendments to Law Number 11 of 2008 concerning Electronic Information and Transactions in Indonesia.[23] The Indonesian government has recognized the importance of data privacy protection, with the Ministry of Information and Technology initiating the Personal Data Protection Bill to address the increasing cases of personal data leakage.[24] However, the existing laws and regulations in the field of information technology in Indonesia do not adequately accommodate all cybercrimes, leaving certain threats, such as data theft through information technology and the subsequent extortion of funds, unresolved.[25]

Businesses also play a crucial role in safeguarding personal data. The implementation of the Personal Data Protection Bill is viewed as a way to enhance Indonesia's business sector, positioning it as a trusted business hub and fostering a favorable environment for data processing activities like cloud computing.[26] Companies are required to implement strong data security measures, comply with data protection regulations, and maintain transparency regarding their data collection and usage practices.

It is evident that the advent of artificial intelligence (AI) has the potential to present a significant challenge to legal practitioners, offering convenience and advantages but also raising concerns about its impact on the legal profession. A number of professions that were previously the exclusive domain of certain professionals due to their specialized knowledge will be transferred to machine labor that has been "educated" with commensurate knowledge. This process will continue until a sufficient quantity of data, or meta-data, has been accumulated in the "brain" of the machine. It can be reasonably assumed that metadata will not make mistakes, will be accurate in completing work, and that systems will be capable of getting the job done. Furthermore, it can be expected that systems will evolve their working capabilities over time, and that the more work experience the system has, the more capable it will become.[27]

Individuals, on the other hand, must be empowered to exercise control over their personal data. The abundance of regulations in Indonesia provides leeway for the violation of consumer rights, underscoring the need for stronger legal protection.[28] Individuals should be informed about their rights, the risks of data misuse, and the steps they can take to protect their personal information.

In Indonesia, there is no specific legal regulation related to artificial intelligence. Consequently, the ITE Law has been expanded to regulate legal regulations related to AI. Article 1, point 8 of the Electronic Information and Transaction Law (ITE Law) defines an electronic agent as "a device of an electronic system that is made to perform an action on certain electronic information automatically organised by a person."

In the realm of artificial intelligence (AI), the protection of personal data from misuse requires clear delineation of roles and responsibilities among governments, companies, and individuals. Governments bear the responsibility of establishing and enforcing robust legislation and regulations designed to safeguard personal data. Laws such as the General Data Protection Regulation (GDPR) in Europe and the California Consumer Privacy Act (CCPA) in the United States set stringent standards for the collection, processing, and use of personal data. Government regulatory bodies monitor compliance with these laws, ensuring that companies adhere to privacy principles and imposing penalties for violations. The roles and responsibilities in ensuring the protection of personal data from AI misuse are defined as follows: Governments develop and enforce legal frameworks, including regulations like the GDPR in the EU and the Personal Data Protection Act (PDPA) in Singapore. They set minimum security standards for organizations, such as encryption, access controls, and incident response protocols, ensuring prioritization of data protection and implementation of robust security measures. Governments also create platforms to facilitate the exchange of threat intelligence and best practices among organizations, keeping them updated on emerging threats and security measures. Governments provide legal remedies for those affected by data breaches, including compensation, penalties for negligence, and legal recourse avenues, fostering accountability and deterrence. They manage and protect data in the public sector through policies and regulations, such as Singapore's Public Sector (Governance) Act, which imposes criminal penalties on public officers who disclose data without authorization. The Indonesia Data Protection System (IDPS) aims to reduce crimes related to personal data and information management, a growing concern as technology advances and regulations lag behind. This highlights the critical need for comprehensive regulations to govern personal data protection and cybercrime.[29]

Companies are required to implement appropriate business practices to protect personal data. This involves ensuring secure data collection and storage, as well as promptly reporting any data breaches. They must obtain explicit consent from individuals before collecting their data, ensuring that people are informed about how their data will be used and can make educated decisions about sharing their information. Transparency is crucial, and companies must clearly communicate how they collect, use, and disclose personal data, including the specific purposes for which it is being collected and used. Companies should invest in robust cybersecurity measures to guard against data breaches and misuse by AI, which includes implementing encryption, access controls, and incident response protocols. Additionally, companies must collaborate with law enforcement to aid in investigations and prevent cybercrime, sharing information and working together to protect against the malicious use of personal data.

Individuals have fundamental rights related to data protection, including the right to information about data processing, the right to object to data processing, and the right to have their data deleted. Individuals must exercise control over their personal data by understanding how it is being used and making informed decisions about sharing it. This includes opting out of data sales and requesting that their data be deleted. Individuals must report data

breaches to the relevant authorities and take steps to mitigate any harm caused by the breach. Individuals must educate themselves on data protection practices and the potential risks associated with sharing personal data. This includes understanding how AI systems can misuse personal data and taking steps to protect themselves.[30]

At the individual level, it is of the utmost importance to cultivate awareness and engage in proactive actions. It is incumbent upon individuals to educate themselves about the manner in which AI systems handle their personal data and to exercise control over their information. This encompasses an understanding of the privacy settings, the provision of informed consent for data use, and the management of preferences regarding data sharing. In the event that an individual suspects that their data has been misused or accessed without consent through an AI system, they should report their concerns to the relevant authorities and utilise the established complaint mechanisms for resolution. The active promotion of enhanced data protection and ethical AI practices enables individuals to contribute to the development of a culture of responsible data utilisation.

The collective implementation of these roles constitutes a comprehensive framework for the protection of personal data from the misuse of AI. By aligning legislative oversight, corporate accountability, and individual empowerment, stakeholders facilitate an environment conducive to the ethical and sustainable innovation of AI technologies. This collaborative approach fosters trust among users, promotes compliance with privacy standards, and ensures that AI advances responsibly serve society in the digital age.

## 4. Conclusion

Indonesia's current personal data protection policies, including the Personal Data Protection (PDP) Law, aim to mitigate misuse by artificial intelligence (AI) through comprehensive regulations. AI, defined as systems that simulate human intelligence and perform tasks requiring human intervention, necessitates robust data protection measures due to its capacity to collect, process, and self-correct information autonomously. Despite significant technological advancements, Indonesia's legal framework for personal data protection has historically been fragmented, with provisions scattered across various laws such as the Electronic Information and Transactions Law and the Population Administration Law. However, the PDP Law consolidates these efforts by establishing clear definitions of personal data, outlining legal bases for data processing, and emphasizing data ownership rights. The law mandates strong authentication and access management solutions, cross-border data transfer notifications, and penalties for non-compliance. These measures are designed to ensure that AI systems operate within legal boundaries and respect individuals' privacy rights, contributing to a safer digital environment in Indonesia.

The protection of personal data from misuse by artificial intelligence (AI) in Indonesia requires coordinated efforts from governments, companies, and individuals. The Indonesian government has initiated measures such as the National Strategy for Artificial Intelligence 2020-2045 and the Personal Data Protection Law to establish legal frameworks, crucial in sectors like banking, e-commerce, and healthcare. Companies must implement robust data security measures, adhere to regulations, and be transparent about data practices to maintain trust and safeguard personal data, integrating privacy by design and conducting regular audits to ensure compliance. Individuals must be educated about their data rights, understand privacy settings, exercise control over their personal data, and report any misuse to authorities. A collaborative approach involving legislative oversight, corporate accountability, and individual empowerment is essential to protect personal data from AI misuse, ensuring ethical and sustainable innovation in Indonesia's digital landscape.

Based on the findings of this study, it is recommended that the Indonesian government strengthen the regulatory framework and enhance cybersecurity capabilities to address the misuse of personal data through AI. The establishment of a dedicated unit focused on the prosecution of AI-based cybercrime is necessary to address the increasing scale and speed of the threat. There is also a need to strengthen cooperation between the public and private sectors in efforts to secure personal data, as well as to increase public awareness and digital literacy. The revision and enforcement of Law No. 27 of 2022 on the Protection of Personal Data and Law No. 11 of 2008 on ITE must be carried out consistently to ensure that these regulations are able to keep pace with the development of AI technology and the threats it poses.

## References

[1] Anshori, "Gagasan Artificial Intelligence Dalam Penerapan Hukum Di Era 4.0 Perspektif Penyelesaian Perkara Model Restorasi Justice Dan Hukum Progresif," *Leg. Stud. J.*, vol. 2, no. 2, pp. 1–13, 2022.

[2] A. P. C. Z. Aditya Kurniawijaya, Alya Yudityastri, "Pendayagunaan Artificial Intelligence Dalam Perancangan Kontrak Serta Dampaknya Bagi Sektor Hukum Di Indonesia," *J. Khatulistiwa Law Rev.*, vol. 2, no. 1, p. 261, 2021.

[3] Y. Paulus Wisnu, "Kecerdasan Buatan (Artificial Intelligence) Sebagai Alat Bantu Proses Penyusunan Undang-Undang Dalam Upaya Menghadapi Revolusi Industri 4.0 Di Indonesia," *Simp. Huk. Indones.*, vol. 1, no. 1, pp. 574–586, 2019.

[4] E. N. A. M. Sihombing and M. Y. A. Syaputra, "Implementasi Penggunaan Kecerdasan Buatan Dalam Pembentukan Peraturan Daerah (The Implementation Of Artificial Intelligence Usage In Local Legislation Forming)," *J. Ilm. Kebijak. Huk.*, vol. 14, no. 3, pp. 419–434, 2020.

[5] N. J. Nilsson, *The Quest for Artificial Intelligence: A History of Ideas and Achievements*. Cambridge University Press.

[6] L. Tsang *et al.*, "The impact of artificial intelligence on medical innovation in the European Union and United States," *Intellect. Prop. Technol. Law J.*, vol. 29, no. 8, pp. 3–12, 2017.

[7] Peter Mahmud Marzuki, *Penelitian Hukum Edisi Revisi*. Jakarta: Kencana, 2019.

[8] S. Mertokusumo, *Mengenal Hukum Suatu Pengantar,*. Yogyakarta: Liberty.

[9] M. F. Ramadhani, "Pembangunan Aplikasi Informasi, Pengaduan, Kritik, Dan Saran Seputar Kota Cimahi Pada Platform Android," *J. Ilm. Komput. dan Inform.*, p. 9, 2018.

[10] P. Dewonoto Laut Santoso, I. Riski, N. Kholik, M. Raffi Akbar, and A. Saifudin, "Penerapan Artificial Intelligence dalam Aplikasi Chatbot sebagai Media Informasi dan Pembelajaran mengenai Kebudayaan Bangsa," *J. Inform. Univ. Pamulang*, vol. 6, no. 3, pp. 579–589, 2021.

[11] R. C. Indra, *Mengenal Software for Beginers*. Yogyakarta: Andi Offset, 2014.

[12] H. Alshenqeeti and R. Inderawati, "Importance of Financial Technology Implications for Professionals in Indonesia," *Financ. Account. Res. J.*, vol. 2, no. 2, pp. 45–52, 2020, doi: 10.51594/farj.v2i2.103.

[13] KOMINFO, *Big Data, Kecerdasan Buatan, Blockchain, dan Teknologi Finansial di Indonesia: Usulan Desain, prinsip, dan Rekomendasi Kebijakan*. Jakarta: Direktorat jenderal Aplikasi informatika Kementerian Komunikasi dan Informatika, 2018.

[14] R. E. Latumahina, "Aspek Hukum Perlindungan Data Pribadi di Dunia Maya," *J. Gema Aktual. 3*, vol. 3, no. 2, 2014.

[15] M. Amirulloh, *Cyberlaw: Perlindungan Merek Dalam Cyberspace (Cybersquatting*

*Terhadap Merek)*. Bandung: Refika Aditama, 2017.
[16] C. Vania, M. Markoni, H. Saragih, and J. Widarto, "Tinjauan Yuridis terhadap Perlindungan Data Pribadi dari Aspek Pengamanan Data dan Keamanan Siber," *J. Multidisiplin Indones.*, vol. 2, no. 3, pp. 654–666, 2023, doi: 10.58344/jmi.v2i3.157.
[17] C. Ristianto, "DPR Didesak Sahkan RUU Perlindungan Data Pribadi," 2019.
[18] M. J. Rizki, "Rentetan Kebocoran Data Pribadi, Perangkat Regulasi Belum Memadai," *Huk. Online*, 2020.
[19] M. P. Aji, "Sistem Keamanan Siber dan Kedaulatan Data di Indonesia dalam Perspektif Ekonomi Politik (Studi Kasus Perlindungan Data Pribadi)," *J. Polit. Din. Masal. Polit. Dalam Negeri dan Hub. Int.*, vol. 13, no. 2, pp. 222–238, 2023.
[20] T. Prasetyo, *Pembaharuan hukum : Perspektif teori keadilan bermartabat*. Malang: Setara Press, 2017.
[21] Q. D. Kusumawardani, "Hukum Progresif Dan Perkembangan Teknologi Kecerdasan Buatan," *Verit. Justitia*, vol. 5, no. 1, pp. 166–190, 2019, doi: 10.25123/vej.3270.
[22] Zahrasafa P Mahardika and A. Priancha, "Pengaturan Hukum Artificial Intelligence Indonesia Saat Ini," Hukumonline.
[23] D. P. Anugerah and M. Indriani, "Data Protection in Financial Technology Services: Indonesian Legal Perspective," *IOP Conf. Ser. Earth Environ. Sci.*, vol. 175, no. 1, 2018, doi: 10.1088/1755-1315/175/1/012188.
[24] D. Setiawati, H. A. Hakim, and F. A. H. Yoga, "Optimizing Personal Data Protection in Indonesia: Lesson Learned from China, South Korea, and Singapore," *Indones. Comp. Law Rev.*, vol. 2, no. 2, 2020, doi: 10.18196/iclr.2219.
[25] N. Ishak, "Guarantee of Information and Communication Technology Application Security in Indonesia: Regulations and Challenges?," *Audit. Comp. Law J.*, vol. 4, no. 2, pp. 108–117, 2023, doi: 10.22219/aclj.v4i2.26098.
[26] G. Kumalaratri and Yunanto, "Urgency of the Personal Data Protection Bill on Privacy Rights in Indonesia," *J. Huk. Unissula*, vol. 37, no. 1, pp. 1–13, 2021, doi: 10.26532/jh.v37i1.13604.
[27] M. Ashley and N. Sahota, *Own the A.I. Revolution: Unlock Your Artificial Intelligence Strategy to Disrupt Your Competition*. New York: McGraw Hill Publishing, 2019.
[28] V. W. S. Soemarwi and W. Susanto, "Digital Technology Information in Indonesia: Data Privacy Protection is a Fundamental Right," *Proc. Int. Conf. Econ. Business, Soc. Humanit. (ICEBSH 2021)*, vol. 570, 2021, doi: 10.2991/assehr.k.210805.088.
[29] R. Aswandi, P. R. N. Muchsin, and M. Sultan, "Perlindungan Data Dan Informasi Pribadi Melalui Indonesian Data Protection System (IDPS)," *Legistaltif*, no. 14, pp. 63–65, 2018.
[30] A. Soraja, "Perlindungan Hukum Atas Hak Privasi dan Data Pribadi dalam Prespektif HAM," *Angew. Chemie Int. Ed.*, pp. 20–32, 2021.