IJSSR
International Journal of Social Service and Research

Vol. 6, No. 5, May 2026
e-ISSN: 2807-8691 | *p*-ISSN: 2807-839X

A Juridical Analysis of Data Classification under Regulation of The Minister of Communication and Digital (MoCD) Number 5 of 2025 Concerning Public Electronic System Operators for Public Sector AI Governance

Indri Maria*, Megawati Barthos
Universitas Borobudur, Indonesia
Email: mariaindri10@gmail.com*, megawati_barthos@borobudur.ac.id

Keywords

AI Governance; Public Sector; Data Classification; MoCD Regulation No. 5 of 2025.

ABSTRACT:

The use of Artificial Intelligence (AI) in the public sector offers significant improvements in bureaucratic effectiveness but simultaneously raises serious concerns regarding data privacy, security, and algorithmic bias. In response, the Ministry of Communication and Digital (MoCD) issued Regulation No. 5 of 2025 concerning Public Electronic System Operators to address these challenges. This research aims to analyze the juridical status of data classification under this regulation as a foundational element for establishing safe and ethical AI governance in the Indonesian public sector. This research employs a normative legal research method using statutory and conceptual approaches, with qualitative and prescriptive analysis of secondary legal materials, including primary and secondary legal sources. The findings reveal that MoCD Regulation No. 5 of 2025 provides legal safeguards through data classification into three categories: open data, restricted data, and confidential or closed data. These categories serve as essential parameters for AI algorithms when processing public information. The juridical analysis confirms that data classification is not merely an administrative measure but constitutes a conditio sine qua non—an absolute necessity—for mitigating the risks of data leaks and algorithmic bias in government-level AI systems. The study concludes that harmonizing this regulation with Law No. 27 of 2022 concerning Personal Data Protection, commonly referred to as the Personal Data Protection Law, is essential to creating a comprehensive legal framework that ensures AI implementation in the public sector adheres to the principles of data security, privacy protection, and digital sovereignty. This research recommends the development of detailed technical guidelines to operationalize data classification in AI systems and the alignment of consent mechanisms with the Personal Data Protection Law to address the asymmetrical power relationship between the state and citizens regarding the use of public data for AI training.

INTRODUCTION

Recently, the Indonesian government, through the Ministry of National Development Planning/National Development Planning Agency (Bappenas), launched the National Digital Government Master Plan 2025-2045 on February 20, 2026. According to Rachmat Pambudy, Head of the Ministry of National Development Planning, this Master Plan document is the first step towards realizing the ideals of a Digital Government that encourages the digitalization of

government, especially for public services. According to Rachmat Pambudy, digitalization of government is essentially an effort to create a faster, more precise, and fairer state. Faster in responding to community needs. More precise in formulating evidence-based policies. More equitable in ensuring that every citizen, without exception, receives equal public services. Digital government isn't just about moving services to a screen; it's about transforming the way the government operates to be more transparent, accountable, efficient, and responsive (Ministry of National Development Planning/National Development Planning Agency Republic of Indonesia, 2026, p. 4).

The master plan discusses the Digital Government Megatrend 2045. In the next two decades, global digital transformation will take place at an unprecedented speed and scale. The development of advanced technologies such as Blockchain, Robotics, the Internet of Things (IoT), Big Data, AI, Quantum Computing, and quantum-resistant cryptography promises a major transformation in modern governance, changing the way governments interact with citizens and make decisions. These future technologies will not only function as supporting tools, but will also become key drivers in the formation of public policy, service design, and the management of national resources (Ministry of National Development Planning/National Development Planning Agency Republic of Indonesia, 2026, p. 12).

Artificial Intelligence, or AI, is one of the future technologies that is now a priority for many new technologies implemented by several ministries/institutions and local governments for public services. This enables public services to be faster, more personalized, and more proactive. AI developments are moving towards the use of Large Language Models (LLM), Agentic AI, and even the implementation of Physical AI has been initiated (Brohi et al., 2025; Buyya, 2026). For example, the use of AI for population services in liveness detection in biometric security, remote health diagnosis, and disaster prediction systems that can provide early warnings (Luxshi, 2025; Su et al., 2021). The implementation of AI has an impact on reducing queues, speeding up processes, and increasing citizen satisfaction with government services (Ministry of National Development Planning/National Development Planning Agency Republic of Indonesia, 2026, p. 19).

The Ministry of Communication and Digital of the Republic of Indonesia has also completed the public consultation process for the National Artificial Intelligence Roadmap White Paper and the Draft Guidelines for Artificial Intelligence Ethics, scheduled for August 19, 2025. These two documents were prepared as part of efforts to formulate a direction for the development of artificial intelligence technology in Indonesia (Ministry of Communication and Digital of the Republic of Indonesia, 2025).

While these two documents do not directly address the concept of digital government and are general in nature, they serve as the initial steps toward developing technical guidelines for the implementation of Artificial Intelligence by the central and regional governments (Luxshi, 2025; Radu, 2021; Su et al., 2021; Yigitcanlar et al., 2021, 2024).

In the era of digital transformation, the use of Artificial Intelligence in Electronic Government Systems (SPBE) is a significant shift from digitizing manual processes to a smart learning government ecosystem. In line with the policy vision of the Minister of Communication and Digital, the existence of AI is key to efforts to transform the government (Androutsopoulou et al., 2019; Koo, 2019; Pencheva et al., 2020). As outlined in the National AI Roadmap, this technology is a process of building systems with explicit or implicit goals

that are capable of independently or semi-independently processing data and information from inputs to generate outputs in the form of predictions, recommendations, content or other decisions that affect the physical and digital world. As such, this change is no longer simply focused on the digitalization of information, but also on bringing data to life to transform administrative efficiency, to establish responsive public services and to enhance policy making accuracy (Duberry, 2022; Sarker et al., 2018).

This disruptive shift first occurs within the government's bureaucratic system, where Artificial Intelligence (AI) transforms repetitive administrative mechanisms. By automating repetitive tasks, government officials can refocus their time on more strategic activities, such as policy-making. This can be achieved through the deployment of Robotic Process Automation (RPA) and, eventually, AI-based language processing. Government systems can now categorize and highlight the most important information from thousands of documents, as well as validate requests within minutes. At the same time, anomalies in transactions or budget allocations can be detected in real time, allowing them to be addressed as quickly as possible.

The resulting reduction in processing time within government work is directly translated into improved public service quality. The interface of the Electronic-Based Government System (SPBE) is now becoming more user-friendly and continuously accessible through automated services. The presence of virtual assistants built using AI technology enables citizens to receive information about permits, public services, and complaint mechanisms at any time, 24/7. Through AI, the government can identify patterns and tailor service experiences, particularly through virtual assistants. In addition, the integration of new biometric technologies into identity verification processes can make services more efficient, enabling the government to provide services according to citizens' individual needs.

Furthermore, government decision-making processes can no longer rely solely on intuition but must be supported by precise predictive analysis using AI. The impact of this digital ecosystem ultimately depends on how vast amounts of interaction and service data are processed as the basis for policy formulation, commonly known as data-driven policy-making. Through predictive analysis, the government can anticipate crises and reduce negative impacts, such as by predicting disaster-prone areas using geospatial data or identifying citizens' sentiment toward a program or policy based on public interactions. The government can then build simulations of proposed policies and predict their effectiveness before rules or regulations are formally enacted.

In the end, the use of AI in the SPBE ecosystem is one way to enhance government performance in public services. The government is expected not only to be faster and more responsive but also proactive in producing accurate policies. This is a key aspect of implementing fast, transparent, and genuinely public-oriented digital governance.

However, while AI has the potential to transform and improve efficiency within government systems, its integration also faces an unavoidable foundational problem related to data use. The intelligence of an AI system, particularly in its capacity to act on behalf of humans, depends on its training, which is supported by big data. To support public services and enable algorithms to make accurate predictions, recommendations, or decisions, AI systems need to be continuously trained using large volumes of data, including user interactions, personal profiles, medical information, and even population data. This is where

an imbalance emerges: the convergence of technology that seeks to collect as much information as possible to provide the most accurate responses versus individuals' rights to data privacy.

Without limits and rules, massive data processing activities within government systems can create legal and ethical problems. Government data is highly centralized and, in many cases, contains sensitive and personal information. The centralization of such data for machine learning without proper data classification and high-level security measures creates significant risks of privacy violations through data misuse and cyberattacks. The consequences of the use and misuse of citizens' data in the digital space extend beyond administrative costs; they may also result in the loss of legitimacy and public trust in public administration.

Beyond data security, another concern that must be addressed is algorithmic bias. AI can be likened to a mirror because it reflects the data on which it is trained. If historical government datasets used for training contain subconscious social inequalities, bureaucratic bias, or discrimination, the algorithm may learn and replicate the same patterns. AI may then provide a veil of "mathematical objectivity" over these biases, making resulting public service policies or decisions, such as the allocation of social assistance or licensing processes, appear neutral while remaining biased and unfair. These biases are often difficult to trace and challenge because they are hidden behind complex systems, commonly referred to as black boxes. Therefore, the application of AI in the government sector requires regulation as a counterbalance to ensure that AI use does not infringe upon justice and public privacy.

In response to the need for legal certainty amid the rapid innovation of algorithm development and data processing, the existence of Minister of Communication and Digital Regulation No. 5 of 2025 concerning Public Electronic System Operators (PSE) is essential. This regulation serves as a preventive model that reorganizes the information governance architecture in the public sector and can be utilized to address the massive use of AI technology. Beyond establishing structured government data management, this regulation differentiates government data protection into three classifications: open data, limited data, and closed data. This classification provides a clear demarcation of what information may be freely used for the digital economy, what information requires special usage rights and encryption mechanisms, and what critical information must not be used by AI in order to protect citizens, the state, and strategic privacy interests.

However, despite the importance of this regulation, several critical questions remain unanswered. First, how is the juridical status of data classification under this regulation legally constructed? Second, to what extent does this data classification provide adequate legal protection for citizens' personal data when used in AI systems? Third, how does this regulation harmonize with the existing Personal Data Protection Law, namely Law No. 27 of 2022? Fourth, what are the legal liability mechanisms when AI systems experience "hallucinations" or data leaks in the public sector? This study aims to analyze the juridical status of data classification under MoCD Regulation No. 5 of 2025 as a foundational element for establishing safe and ethical AI governance in the Indonesian public sector. Theoretically, this research contributes to the development of administrative law and data protection law, particularly regarding the intersection of AI governance and data classification in the public sector. Practically, this study provides recommendations for policymakers, government agencies, and public electronic system operators on implementing data classification for AI systems while

ensuring compliance with the Personal Data Protection Law and protecting citizens' privacy rights.

METHOD

According to Asshiddiqie, legal norms have the following characteristics: permission to do something (permittere), a positive recommendation to do something, a negative recommendation to refrain from doing something, a positive command to do something or an obligation (obligattere), and a negative command to refrain from doing something (prohibere).

Normative legal research, which examines norms as the main issue, relies heavily on the chosen approach and data. The approach required in normative legal research is qualitative because the focus of the problem lies in legal norms. This means that the expected output of normative research is recommendations regarding norms.

Meuwissen explains that normative qualitative research can be equated with dogmatic research, as it is based on certain dogmas or legal doctrines. Meanwhile, Suyanto explains that the normative legal research method is defined as a research method that examines legal regulations, both from the perspective of the legal hierarchy, namely vertically, and from the perspective of harmony among laws, namely horizontally.

According to Muhaimin, normative research is also known as doctrinal legal research because it is conducted or directed solely at written regulations or legal materials. It is also known as library research or document study because it primarily focuses on secondary data found in libraries.

This study uses normative legal research methods with statutory and conceptual approaches. The legal materials used include primary legal materials, namely Regulation of the Minister of Communication and Digital No. 5 of 2025, Law No. 27 of 2022 concerning Personal Data Protection, and related regulations; secondary legal materials, including textbooks, scientific journals, and academic documents; and tertiary legal materials, such as legal dictionaries. The technique for collecting legal materials is carried out through library research. The data analysis technique uses qualitative descriptive analysis through three stages: data reduction, which involves selecting and grouping relevant data; data presentation, which is arranged in a systematic narrative based on themes; and drawing conclusions, which are strengthened through grammatical, systematic, and teleological interpretation. The analytical framework uses legal certainty theory, legal protection theory, and accountability principles in artificial intelligence governance to assess data classification as the foundation of AI governance in the public sector.

RESULTS AND DISCUSSION

Legal Status of Data Classification in the Regulation of the Minister of Communication and Digital Number 5 of 2025 concerning Public Electronic System Operators as the Foundation for Public AI Governance

Amid the rapid pace of digital transformation, the adoption of Artificial Intelligence (AI) by government institutions offers significant efficiency, particularly in public services. However, AI innovation must be developed on a solid foundation of data and information governance to realize data sovereignty for the purposes of national security and privacy protection. Regulation of the Minister of Communication and Digital No. 5 of 2025 concerning

Public Sector Electronic System Operators can play a strategic role in achieving this data sovereignty. This regulation not only governs technical matters related to government information technology systems but, at a more fundamental level, also regulates the legal status of data classification, which can serve as a foundation for AI governance in the public sector, especially in relation to the utilization of data processed by AI systems.

Legally, MoCD Regulation No. 5 of 2025 explicitly states that every government agency must map and categorize its electronic data based on the impact and level of risk associated with such data. Data is not treated as a single, uniform entity but is instead classified within a clear legal structure: Open Data for low-risk data, Restricted Data for medium-risk data, and Closed Data for high-risk data. This risk assessment is not conducted subjectively but uses measurable tools within an integrated process chain between data producers and data custodians. This legal provision then becomes the primary platform of protection in the implementation of AI.

As is widely understood, AI systems, particularly machine learning and generative AI systems, are highly dependent on data inputs. In this context, data classification serves as a protective measure. When the government develops an AI model or provides an interactive chatbot service for the public, legal certainty is needed to ensure that the AI system is only permitted to process Open Data. This protection addresses the potentially serious risk of AI unintentionally leaking state secrets or citizens' personal data through prompt-based interactions that may be manipulated by data producers or users.

Furthermore, because data classification has legal status, it directly determines how the government should design its AI infrastructure architecture. MoCD Regulation No. 5 of 2025 emphasizes that Closed Data must be protected through high-level security measures, including mandatory encryption and placement in a national data center. This has important implications for AI governance. If an agency is responsible for intelligence, defense, or population administration involving sensitive data, its AI analytical capabilities must be legally bound to its own secure infrastructure, where AI algorithms and computations are executed internally. High-risk data processing should not be outsourced to open third-party commercial cloud computing services.

This ministerial regulation can also serve as an alternative legal instrument to address the weaknesses of AI, particularly its susceptibility to manipulation and its opaque, or black-box, nature. When an algorithmic decision is challenged, the track record of data classification enables the government to conduct a thorough audit. Agencies can trace the data life cycle that informed the machine's recommendations, thereby ensuring that data has not been misused. This transforms AI from an opaque, untraceable, and unaccountable system into one that is transparent, traceable, and capable of holding relevant actors accountable.

For further analysis, the following is a mapping of data references (articles and pages) from the Regulation of MoCD number 5/2025 as a basis of legislation:

1. Article 1 number 10 and article 2 letter e Definition and Scope Data Classification.
   Analysis: This article is legally binding to the implementation of Risk Based Data Classification area of implementation is mandatory, namely, is to determine groups of data based on the risks they pose
2. Attachment to MoCD Regulation No. 5/2025 on Pages 69 Risk Based Data Hierarchy (Open, Restricted, Closed)

Analysis: This appendix acts as a reference for easily understandable data hierarchy, where Open Data is considered as low risk level, Restricted Data marks medium risk levels and Closed Data represent high risk levels.

3. Attachment to MoCD Regulation No. 5/2025 Pages 71-81. Risk Assessment Parameters (Confidentiality, Integrity and Availability)
   Analysis: Impact Area is the parameter of Confidentiality, Integrity, Availability which is used to determine the magnitude of risk. This concept of Integrity is used as an argument for protection against manipulation of data for artificial intelligence systems.
4. Article 89 paragraphs (1) and (2). On Premise Infrastructure & Encryption Requirements for Risky Data
   Analysis: The use of encrypted media for Covert Electronic Data is expressly called for under article 89. Furthermore, it states that such media will have to be housed in a computing center owned by the Agency. This condition forms the basis for the case that the government's processing of sensitive information for sophisticated Artificial Intelligence purposes should not be transferred to open cloud computing.
5. Article 1 number 32, and number 33. and Attachment Appendices Chart (Pages 86-89). Chain of Accountability of Data for *Produsen Data* dan *Walidata*
   Analysis: This reference illustrates the role of *Produsen Data* and *Walidata* in doing multi-level verification and validation. This can be the foundation to make the argument for data lineage transparency when building policy recommendations for an Artificial Intelligence model.

In conclusion, the main points that we can take from the Regulation of MoCD number 5/2025 in particular, are sovereignty and control. This regulation ensures that the implementation of Artificial Intelligence in government does not run with impunity and control. The legal stature of data classification forms a harmonious eco system, where artificial intelligence can be led to accelerate the country's development, and at the same time under the privacy ethics, obeying public accountability and being a good guard of the nation's resilience in the era of digital automation. There is a logical thread that we can draw, because Artificial Intelligence systems (especially Generative AI and Machine Learning) work completely based on consuming data, then the process of limiting security (encryption, determining confidentiality, and the obligation of independent servers) imposed by the Regulation of MoCD number 5/2025 automatically binds and becomes the legal basis for any agency willing to implement an Artificial Intelligence system within the scope of government.

Harmonization of the Regulation of the Minister of Communication and Digital Number 5 of 2025 concerning Public Electronic System Operators with Law Number 27 of 2022 concerning Personal Data Protection (PDP Law)

It is precisely the excessive protection of the sources of the data input, which leads to creating a strong basis of the artificial intelligence rule by the state, that can never be detached from its biggest threat; the privacy of the citizens. This argument about data classification being one of the guardrails over AI machines is essential when it comes to the realization that the personal data of the citizens is the key resource to digital government automation especially regarding the provision of services to the citizens. Given the fact that sensitive information can be exploited by automated processing machines because of high risk, the design of data

classification via Regulation of MoCD number 5/2025 can be applied as a law tool in protecting privacy. This coordination of this ministerial regulation by the Law Number 27 of 2022 regulating Personal Data Protection (PDP Law) will thereby manifest this legal synergy. The two do not work independently but they establish a safety net that is all-inclusive.

The initial and the most primary harmonization can be found in the role and the paradigm of the data classification. Under Personal Data Protection Law, personal data is directly separated into two, including general personal data and specific, sensitive personal data, including biometrics data and health data. Cybersecurity expert, Eryk Budi Pratama explained that many people think personal data is limited to a person's full name or ID number (NIK). However, Law No. 27 of 2022 concerning Personal Data Protection (UU PDP) covers much more broadly. The key lies not only in the data itself, but also in its ability to identify a person. Therefore, personal data in public services must be classified first to determine whether its distribution could violate privacy (Pratama, n.d.). Even residents' emails can be categorized as personal data. However, Alfathi noted that Indonesia ranked third in ASEAN for email hacking in 2024, with a total of 21,769,496 cases (Alfathi, 2025).

In the journal "Legal Responsibility of Electronic System Providers for Leaks of User Personal Data," Amelia stated that the legal responsibility of electronic system providers for leaks of personal data depends on the obligations stipulated in the PDP Law, PP 71/2019, and its derivative regulations, which place electronic system providers as the primary party obligated to maintain the security of user data. Any form of negligence, whether technical or administrative, opens up the opportunity for civil, criminal, and administrative liability, which can result in multiple legal consequences for providers. Analysis of various cases, such as data leaks from e-commerce, public services, and other digital platforms, shows that most of the legal responsibility of Electronic System Providers for leaks of personal data is (Amelia, 2025).

Yusuf, in his scientific journal entitled "Responsibility for Digital Data Security by PSE," stated that the PDP Law actually provides a mechanism for data owners to file a lawsuit if they feel they have been harmed due to negligence. This compensation can take the form of financial compensation or restoration of the rights of users whose data has been illegally circulated. In some circumstances, data owners can also request deletion of the leaked data if it is still under the control of the PSE. This mechanism provides additional protection so users feel in control of their personal information (Yusuf et al., 2024).

According to Budiandru & Hidayat in the scientific journal "Legal Responsibility of Marketplaces for Leaks of User Personal Data from the Perspective of the ITE Law and the Personal Data Protection Law," administrative sanctions stipulated in the PDP Law include written warnings, temporary suspension of services, administrative fines, and termination of system access. These sanctions can be imposed when the E-Commerce Platform is proven to have failed to comply with data protection standards or to have failed to submit incident reports according to procedures. Therefore, E-Commerce Platforms are required to maintain the integrity of their systems to avoid facing greater legal burdens (Budiandru & Hidayat, 2025).

The operational framework, namely that of the public services in the government, can be a derivative of MoCD number 5/2025 regulation. By using this data classification, each instance of personal data, which has been clearly secured by the Personal Data Protection Law in terms of governmental services, is first of all classified into the category of Closed Data or limited data.

With the current extremely high-level of risks, government agencies now have clear parameters on what data about its citizens should or should not be shared with the artificial intelligence systems. This is where MoCD Regulation No. 5/2025 comes into action as an impeding factor to this by imposing advanced encryption and physical storage by the development of National Data Center. The Privacy and Data Protection Law should also enforce the security requirements so that the stored sensitive data about the citizens must be stored in limited accessible data warehouses at will by the public agencies or trusted third party.

The last harmonization is in the internal accountability structure. The Privacy and Data Protection Law require Transparency on the part of Data Controllers. This is organized within the bureaucratic ecosystem, with MoCD Regulation No. 5/2025 organizing it as the leaders of the process of validating the integrity and confidentiality of the data before it is handled by any electronic system, through the roles of *Produsen Data* and *Walidata*.

Legal Liability for Public AI "Hallucinations" or Leaks and Consent Mechanisms in the Context of Utilizing Public Data for Artificial Intelligence

Even though the harmonization of the Personal Data Protection Law (PDP Law) and the MoCD Regulation No. 5/2025 come has furnished the serious architectural framework, introduction of the public AI governance has become a legal challenge that needs critical analysis. The initial and the primary obstacle is the building of a citizen consent on the usage of public data. The state and the citizen in the governance ecosystem is normally asymmetrical in nature; citizens usually do not have an option than to give out their personal data in order to use the simple services of the state.

This has led to a legal controversy, which is whether or not the act of submitting data to help with the provision of basic services amounts to implicit consent to allow the state to use data as AI machine training. It might be a breach of the principle of distributive justice in information governance because the risks of privacy breach are disproportionately transferred to the population forcing them to sign an implicit consent in the context of asymmetrical power. This is where one should take the data classification in MoCD Regulation No. 5/2025 comes as a filtering mechanism. Any data that is classified as either Closed or Restricted cannot be transformed into AI training data, legally, unless the data subject gives his or her, express consent. This is in great accordance to the required principle of limiting purposes, according to which the state should not misuse the data of the citizens as the circumstances under which it was first presented.

This problem of data security and consent in turn paves the way to the next vital problem the issue of legal liability in case of malfunctioning of public AI machines. As a matter of fact, AI does not tend to avoid hallucinations, giving them a fake conclusion, discriminative decision making, or even backfiring sensibilities because of the speedy injection. The AI nature as a black box tends to complicate the cause-and-effect chain, so that it becomes exceptionally complicated to define the party that is culpable in the court of law and in civil affairs. Is it the fault of the third-part developer or the user or is it an anomaly in the algorithms?

Nevertheless, the ambiguity of responsibility can be further resolved by doing a combination of MoCD Regulation No. 5/2025. This rule makes Data Producers and Data Controllers hierarchically separate the responsibility. When it will be proved that the basis of an AI suggestion that will only harm the people is formed on the grounds of manipulated or

incorrectly classified data, the machine anomaly argument cannot be applied to exonerate one. The government agency bears all the legal responsibilities as the Data Controller. The chain of verification through *Walidata* and *Produsen Data* in this regulation in fact serves as a legally binding one to show when the negligence in validation took place.

CONCLUSION

The legal state of classification of data in accordance with the provisions of the MoCD Regulation No. 5/2025 is not only an administrative regulation for information governance but also rather a basis for defense and an absolute prerequisite for the implementation of Artificial Intelligence (AI) in the public sector. Through a use of risk-based approach (Open, Restricted, and Closed Data), this regulation establishes guardrails on AI machines to prevent them from indiscriminately processing sensitive data, while also forcing government agencies to implement secure AI infrastructure (on-premises and encrypted) for high-risk data.

Furthermore, this security architecture is achieved in its best form when harmonized with the Personal Data Protection Law (PDP Law). The two comprise a holistic legal synergy: while the PDP Law creates a normative agricultural ground to ensure the right to privacy for its citizens, the MoCD Regulation No. 5/2025 is a technical-bureaucratic device to ensure that these rights are implemented in government public services. This synergy also balances the asymmetry of the power relations between the state and citizens regarding consent mechanisms so that the situation where public data are used as input for algorithms for purposes other than those for which they were legitimately collected is avoided.

The merging of these two regulations brings legal certainty from the threat of algorithmic malfunctions or hallucinations. The structure of data classification, protected by a chain of verify *Produsen Data* and *Walidata*, is a technique that explains the ambiguity of the concept of the AI "black box" well. This confirms the excuse of machine anomalies cannot eliminate traces of bureaucratic negligence and full legal responsibility (liability) for algorithmic system failures still fully resides with government agencies as Data Controllers.

In the context of good public governance accountability, the setting up of this data taxonomy should never be reduced to an administrative process or document labeling. Rather, this classification process is something an absolute prior requirement to the validity and security of the entire subsequent chain of technology implementation. This data classification status provides a direct draw of clear legal boundaries in respect to Public Electronic System operators (PSEs) undertakes their crucial obligation, that is, conducting independent risk self-assessment. Without a firm, measurable, and accurate foundation of data classification from the initial phase, the self-assessment instrument implemented by the state administrators will lose its objective foundation which, potentially, turns this legal compliance instrument into nothing but a formality that does not offer meaningful protection to the public.

Ultimately, this regulatory harmonization is needed to ensure that the state can move quickly on leveraging AI innovations for efficient provision of public services without jeopardizing public privacy, data sovereignty and national resilience. Public AI governance based on legal certainty is an essential tool in accomplishing fair information governance so that leaps of technological advancement for government do not strip away the basic rights and protection for all of its citizens.

REFERENCES

Alfathi, B. R. (2025, February 5). *Indonesia peringkat ke-3 negara ASEAN dengan kebocoran data terbanyak*. GoodStats. https://data.goodstats.id/statistic/indonesia-peringkatke-3-negara-asean-dengan-kebocoran-data-terbanyak-AtcAs

Amelia, S. P. (2025). Tanggung jawab hukum penyelenggara sistem elektronik terhadap kebocoran data pribadi pengguna. *Studia: Journal of Humanities and Education Studies, 1*(2), 132–141.

Androutsopoulou, A., Karacapilidis, N., Loukis, E., & Charalabidis, Y. (2019). Transforming the communication between citizens and government through AI-guided chatbots. *Government Information Quarterly, 36*(2), 358–367. https://doi.org/10.1016/j.giq.2018.10.001

Brohi, S., Mastoi, Q., Jhanjhi, N. Z., & Pillai, T. R. (2025). A research landscape of agentic AI and large language models: Applications, challenges and future directions. *Algorithms, 18*(8), 499. https://doi.org/10.3390/a18080499

Budiandru, B., & Hidayat, R. S. (2025). Tanggung jawab hukum marketplace terhadap kebocoran data pribadi pengguna dalam perspektif UU ITE dan UU Perlindungan Data Pribadi. *RIGGS: Journal of Artificial Intelligence and Digital Business, 4*(3), 7738–7743.

Buyya, R. (2026). *Agentic artificial intelligence (AI): Architectures, taxonomies, and evaluation of large language model agents* (arXiv Preprint arXiv:2601.12560). arXiv. https://arxiv.org/abs/2601.12560

Duberry, J. (2022). Artificial intelligence and democracy: Risks and promises of AI-mediated citizen–government relations. In *Artificial intelligence and democracy*. Edward Elgar Publishing.

Koo, E. (2019). *Digital transformation of government: From e-government to intelligent e-government*. Massachusetts Institute of Technology.

Luxshi, K. (2025). *AI-driven disaster prediction and early warning systems: A systematic literature review*.

Ministry of Communication and Digital of the Republic of Indonesia. (2025). *White paper on artificial intelligence roadmap*. Ministry of Communication and Digital.

Ministry of Communication and Digital of the Republic of Indonesia. (2025, August 19). *Komdigi holds public consultation on white paper, roadmap, and ethical guidelines for artificial intelligence*. https://djed.komdigi.go.id/news/komdigi-gelar-konsultasi-publik-buku-putih-peta-jalan-dan-pedoman-etika-kecerdasan-artifisial

Ministry of National Development Planning/National Development Planning Agency Republic of Indonesia. (2026). *National digital government master plan 2025–2045*. Bappenas.

Muhaimin. (2020). *Metode penelitian hukum*. Mataram University Press.

Pencheva, I., Esteve, M., & Mikhaylov, S. J. (2020). Big data and AI—A transformational shift for government: So, what next for research? *Public Policy and Administration, 35*(1), 24–44. https://doi.org/10.1177/0952076718780537

Radu, R. (2021). Steering the governance of artificial intelligence: National strategies in perspective. *Policy and Society, 40*(2), 178–193. https://doi.org/10.1080/14494035.2021.1929727

Sarker, M. N. I., Wu, M., & Hossin, M. A. (2018). Smart governance through big data: Digital transformation of public agencies. In *2018 International Conference on Artificial Intelligence and Big Data (ICAIBD)* (pp. 62–70). IEEE. https://doi.org/10.1109/ICAIBD.2018.8396183

Su, Z., McDonnell, D., Bentley, B. L., He, J., Shi, F., Cheshmehzangi, A., Ahmad, J., & Jia, P. (2021). Addressing Biodisaster X threats with artificial intelligence and 6G technologies: Literature review and critical insights. *Journal of Medical Internet*

Research, 23(5), e26109. https://doi.org/10.2196/26109
Suyanto. (2022). *Metode penelitian hukum: Pengantar penelitian normatif, empiris dan gabungan*. Unigres Press.
Yigitcanlar, T., Corchado, J. M., Mehmood, R., Li, R. Y. M., Mossberger, K., & Desouza, K. (2021). Responsible urban innovation with local government artificial intelligence (AI): A conceptual framework and research agenda. *Journal of Open Innovation: Technology, Market, and Complexity, 7*(1), 71. https://doi.org/10.3390/joitmc7010071
Yigitcanlar, T., David, A., Li, W., Fookes, C., Bibri, S. E., & Ye, X. (2024). Unlocking artificial intelligence adoption in local governments: Best practice lessons from real-world implementations. *Smart Cities, 7*(4), 1576–1625. https://doi.org/10.3390/smartcities7040060
Yusuf, P. A., Setiabudhi, D. O., & Tampanguma, M. Y. (2024). Tanggung jawab keamanan data digital oleh penyelenggara sistem elektronik. *Lex Privatum, 13*(5), 1–12.