Hasanah in Law
ISSN(Online): XXXX-XXXX
Vol 1 No 2 (2026): Oktober 2026
https://hasanah.gerakanedukasi.com/index.php/HIL/index

The Right to Erasure in Indonesian Law: Reconstructing Data Subject Protection in the Age of Artificial Intelligence

[1]Diki Darmawan
[1]*Universitas Islam Negeri Sayyid Ali Rahmatullah Tulungagung, Indonesia*
[1]*dikydarmawan149@gmail.com*

**Correspondence Email: dikydarmawan149@gmail.com*

Abstract: *The increasing use of artificial intelligence (AI) creates new challenges for exercising the right to erasure, particularly when personal information is incorporated into trained models and cannot readily be removed through conventional data-deletion procedures. This study examines the adequacy of Indonesia's personal data protection framework in addressing these challenges and develops a conceptual model for reconstructing data subject protection in AI-based processing environments. The study employs normative legal research using statutory, conceptual, and comparative approaches. Legal materials are collected through library research and analyzed qualitatively through legal interpretation and normative evaluation, with particular attention to Indonesia's Law No. 27 of 2022 concerning Personal Data Protection and Article 17 of the European Union's General Data Protection Regulation. The findings indicate that Indonesian law provides a statutory foundation for erasure rights, but questions remain regarding their implementation in AI systems, the allocation of responsibility among relevant actors, and the verification of compliance. The comparative analysis further demonstrates the importance of clarifying erasure grounds, applicable exceptions, and the relationship between legal obligations and technical measures such as machine unlearning. This study proposes a conceptual model comprising five components: statutory foundation, legal assessment, implementation of erasure, verification and accountability, and rights-based safeguards. The model contributes a normative framework for connecting data subjects' legal entitlements with appropriate implementation measures and demonstrable compliance while maintaining a proportionate balance between privacy protection and legitimate competing interests. The study provides a basis for further legal and regulatory development concerning personal data protection in Indonesia's evolving AI governance landscape.*

Keywords: *Right to Erasure, Personal Data Protection, Artificial Intelligence, Indonesian Law, Machine Unlearning*

INTRODUCTION

The expansion of digital technologies has fundamentally changed the way personal information is collected, stored, processed, and circulated. Digital platforms, search engines, cloud services, and artificial intelligence (AI) systems enable personal data to be retained and reused beyond the circumstances in which it was originally disclosed. Information that was once

temporary can consequently become a persistent digital record, accessible and reproducible long after its initial purpose has been fulfilled. This development raises a fundamental legal question concerning the extent to which individuals can exercise control over information relating to themselves. In this context, the right to erasure has become an important instrument of personal data protection because it seeks to prevent the indefinite retention and continued processing of personal information when legitimate grounds for such processing no longer exist. However, the practical meaning of this right becomes increasingly complex when personal information is incorporated into interconnected digital systems and AI technologies.

The legal significance of the right to erasure is reflected in the European Union's General Data Protection Regulation (GDPR), particularly Article 17, which establishes the right of data subjects to obtain the erasure of personal data under specified circumstances. This provision recognizes that personal data should not remain available indefinitely when the original purpose of processing has ceased, consent has been withdrawn without another applicable legal basis, or processing has been unlawful. Nevertheless, the right is not absolute, as exceptions apply to circumstances such as freedom of expression, legal obligations, public interests, and certain research activities (European Parliament & Council of the European Union, 2016). This framework demonstrates that the right to erasure involves more than the technical removal of information; it requires a legal assessment of competing interests, legitimate grounds for retention, and the responsibilities of data controllers. Such considerations provide an important foundation for examining how the right should operate within legal systems confronting increasingly complex forms of data processing.

In Indonesia, the recognition of personal data protection as a fundamental legal concern has been strengthened through Law No. 27 of 2022 concerning Personal Data Protection (UU PDP). Article 8 recognizes the right of data subjects to terminate processing, delete, and/or destroy personal data concerning themselves, subject to applicable legislation. This protection is reinforced by Articles 42–45, which regulate the termination of processing, deletion, destruction, and notification to data subjects. In particular, Article 43 establishes circumstances in which personal data controllers are required to delete personal data, including when the information is no longer

Hasanah in Law
ISSN(Online): XXXX-XXXX
Vol 1 No 2 (2026): Oktober 2026
https://hasanah.gerakanedukasi.com/index.php/HIL/index

necessary for its processing purposes, consent has been withdrawn, a request for deletion has been submitted, or the data was obtained or processed unlawfully (Republic of Indonesia, 2022). These provisions provide a statutory basis for exercising control over personal information. Nevertheless, the existence of a legal entitlement does not automatically ensure that individuals can effectively exercise that right across different technological environments.

The central difficulty arises from the distinction between deleting personal data stored in conventional databases and addressing information that has been incorporated into AI systems. In traditional data processing, deletion may involve removing identifiable records from a database or withdrawing information from a particular platform. AI systems, particularly large language models (LLMs), present a more complicated situation because information may be embedded in model parameters through training processes rather than retained solely as separately identifiable records. Zhang et al. (2025) explain that implementing the right to be forgotten in LLMs raises challenges involving model opacity, the identification of affected information, and the technical feasibility of removing its influence without retraining the entire model. Consequently, deleting the original data source may not necessarily eliminate the possibility that a model will reproduce information associated with an individual. This distinction exposes a potential limitation in conventional understandings of erasure: legal compliance may require more than deleting a visible record if the relevant personal information remains recoverable or influential within an AI system.

The problem becomes more significant when the legal obligation to erase data encounters the technical limitations of AI development. Research on machine unlearning has begun to explore methods for reducing or removing the influence of selected training data from machine-learning models without repeating the entire training process. Yao et al. (2024), for example, examine machine unlearning methods for pretrained LLMs and demonstrate the importance of developing technical approaches that address the removal of information from trained models. However, the availability of technical methods does not independently determine what constitutes legally sufficient erasure. Questions remain concerning the degree of removal required, the evidence needed to demonstrate compliance, the allocation of responsibility between data controllers and AI providers, and the remedies available when deletion requests cannot be fully implemented.

Hasanah in Law
ISSN(Online): XXXX-XXXX
Vol 1 No 2 (2026): Oktober 2026
https://hasanah.gerakanedukasi.com/index.php/HIL/index

From a legal perspective, these issues require a framework capable of translating the general right to erasure into obligations that remain meaningful within AI-based data processing.

Previous studies have examined different aspects of this problem, but their analytical emphases vary. Sanjaya and Prasada (2025) investigate the legal framework for personal data deletion on social media in Indonesia and identify uncertainty surrounding the procedures for exercising deletion rights. Fachmi et al. (2025), meanwhile, examine the challenges of reconciling the right to be forgotten with records management and organizational retention obligations. At the international level, Zhang et al. (2025) explore the implications of the right to be forgotten for LLMs, particularly the technical and conceptual difficulties associated with removing information from trained models. These studies establish important foundations for understanding deletion rights, institutional responsibilities, and technological challenges. However, the intersection between Indonesia's statutory framework and the specific implications of erasure in AI systems requires further examination, particularly regarding how existing legal provisions can be interpreted and operationalized when personal information is embedded in model parameters. This article therefore approaches the issue as a problem of legal reconstruction rather than merely a comparison of existing regulations.

The research gap lies in the need to connect the normative structure of Indonesia's personal data protection law with the practical and conceptual challenges of AI-based information processing. Although the UU PDP recognizes deletion rights, the relationship between statutory erasure obligations and the removal of personal information from trained AI models requires a more clearly articulated legal interpretation. This issue encompasses at least three interrelated dimensions: the scope of personal data subject to erasure, the standard by which compliance with a deletion request should be assessed, and the balance between individual privacy rights and competing interests, including freedom of expression, legitimate data retention, and technological development. The GDPR provides a comparative reference for examining the conditions and limitations of erasure, while developments in machine unlearning illuminate the technical distinction between deleting source data and reducing its influence within a model. Bringing these

Hasanah in Law
ISSN(Online): XXXX-XXXX
Vol 1 No 2 (2026): Oktober 2026
https://hasanah.gerakanedukasi.com/index.php/HIL/index

dimensions together can support the development of a contextually appropriate framework for Indonesia without assuming that a technical solution alone resolves the underlying legal problem.

Accordingly, this study aims to reconstruct the legal protection of data subjects' right to erasure under Indonesian law in the age of artificial intelligence. It examines the normative basis and scope of erasure under the UU PDP, identifies the legal and conceptual challenges arising when personal information is incorporated into AI systems, and evaluates the relevance of the GDPR and emerging machine-unlearning approaches for strengthening the interpretation of Indonesian law. The central research question is: How should the right to erasure under Indonesian law be reconstructed to provide effective protection for data subjects in the age of artificial intelligence? Using a normative legal research approach, the study employs statutory and conceptual approaches, complemented by a comparative examination of the GDPR and relevant developments in AI research. Its intended contribution is a legal framework that clarifies the scope of erasure, the responsibilities of relevant actors, and the standards for assessing compliance while maintaining a proportionate balance between personal data protection and legitimate competing interests.

METHOD

This study adopts a normative legal approach to analyze how the right to erasure can be reconstructed within the Indonesian legal framework in response to the development of artificial intelligence (AI). The research relies on library-based inquiry, involving the collection and examination of relevant legal and academic materials, including statutory provisions, judicial decisions, scholarly books, and peer-reviewed journal articles. These materials are systematically selected, reviewed, and interpreted to identify applicable legal principles and assess their adequacy in addressing the legal issues under investigation (Hutchinson & Duncan, 2012; Hariani, P. E., & Jabbar, 2026).

The study applies statutory, conceptual, and comparative approaches. The statutory approach examines Law No. 27 of 2022 concerning Personal Data Protection, particularly its provisions on data subjects' rights, termination of processing, deletion, and destruction of personal data. The

conceptual approach clarifies the distinction between the right to erasure and the right to be forgotten, including their implications for AI-based data processing. The comparative approach examines Article 17 of the European Union's General Data Protection Regulation (GDPR) to identify relevant principles and regulatory considerations for Indonesia. Primary legal materials comprise relevant legislation and judicial decisions, while secondary materials include scholarly publications on data protection, AI governance, and machine unlearning.

Data are collected through documentary research by identifying, selecting, and classifying relevant legal materials according to their authority and relevance to the research questions. The materials are analyzed qualitatively using legal interpretation and normative analysis. The analysis proceeds by examining the scope of erasure rights under Indonesian law, identifying challenges associated with removing personal information from AI systems, and comparing the Indonesian framework with the GDPR. The findings are subsequently synthesized to formulate a normative reconstruction addressing the scope of erasure, data controller accountability, compliance standards, and the balance between data protection and legitimate competing interests. This analysis evaluates legal adequacy rather than empirically testing the technical effectiveness of AI erasure methods.

RESULT AND DISCUSSION

1. The Legal Construction of the Right to Erasure under Indonesian Law

The right to erasure constitutes an important instrument of personal data protection because it enables individuals to seek the removal of personal information when the legal grounds for its retention or processing no longer apply. In Indonesia, Law No. 27 of 2022 concerning Personal Data Protection (UU PDP) provides the statutory foundation for exercising this right. The law recognizes the rights of data subjects and establishes corresponding obligations for personal data controllers, including obligations concerning the termination of processing, deletion, destruction, and notification. Nevertheless, the practical effectiveness of these provisions depends on how their legal scope is interpreted and applied to different data-processing environments (Republic of Indonesia, 2022).

Hasanah in Law
ISSN(Online): XXXX-XXXX
Vol 1 No 2 (2026): Oktober 2026
https://hasanah.gerakanedukasi.com/index.php/HIL/index

An important distinction must be maintained between the right to erasure and the broader concept of the right to be forgotten. The former concerns the removal of personal data under legally specified conditions, whereas the latter is frequently associated with the broader objective of limiting the continued accessibility or dissemination of personal information. These concepts overlap but are not interchangeable in every legal context. The distinction is particularly relevant when personal information remains available through third-party platforms or has been incorporated into AI systems. Prabasari et al. (2024), in their examination of personal data deletion in Indonesia, identify concerns regarding the regulation and implementation of the right to be forgotten. Their discussion provides a starting point for examining whether the existing legal framework adequately addresses more complex forms of digital information processing.

The interpretation of erasure rights also requires consideration of competing legal interests. Privacy protection cannot always be understood as an unconditional obligation to eliminate every instance of personal information. In some circumstances, continued retention or processing may be justified by applicable legal obligations, public interests, freedom of expression, or other recognized grounds. The European Union's General Data Protection Regulation (GDPR) illustrates this approach by recognizing the right to erasure while providing specific exceptions to its exercise (European Parliament & Council of the European Union, 2016). This comparative perspective demonstrates that effective protection requires both recognition of the individual's right and a clear framework for assessing when that right must prevail over competing interests.

From the perspective of Indonesian law, the central issue is therefore not the absence of a statutory basis for deletion, but the extent to which existing obligations can be applied effectively to AI-based processing. The legal framework needs to distinguish the termination of further processing from the deletion of stored records and the possible removal of information incorporated into trained models. This distinction forms the basis for the subsequent analysis of the legal and technical challenges associated with exercising erasure rights in AI environments.

2. Legal and Technical Challenges of Erasure in Artificial Intelligence Systems

The application of erasure rights becomes more complicated when personal information is incorporated into machine-learning models. In conventional databases, deletion can often be

Hasanah in Law
ISSN(Online): XXXX-XXXX
Vol 1 No 2 (2026): Oktober 2026
https://hasanah.gerakanedukasi.com/index.php/HIL/index

directed toward identifiable records. In trained AI systems, however, information may influence model parameters through training processes, making the relationship between specific data and the model's subsequent outputs difficult to establish. Politou et al. (2018) identify significant challenges in implementing erasure and consent withdrawal within complex digital infrastructures. Their analysis highlights the need to consider both legal requirements and the technical characteristics of the systems through which personal information is processed.

These difficulties are particularly evident in large language models (LLMs), which may reproduce information derived from their training data. Zhang et al. (2025) examine the implications of the right to be forgotten for LLMs and discuss potential approaches, including machine unlearning, differential privacy, model editing, and output safeguards. Their analysis demonstrates that AI systems introduce challenges that differ from those associated with conventional search engines, particularly because information may not remain confined to an identifiable record or index. Consequently, removing an original data source does not necessarily establish that the information can no longer influence the model's outputs.

One technical approach to this problem is machine unlearning, which seeks to remove or reduce the influence of selected training data without retraining an entire model from scratch. Cao and Yang (2015) introduced an early framework for enabling learning systems to forget selected data through modifications to the learning process. Subsequent developments have explored the feasibility of applying such methods to increasingly complex models. Bourtoule et al. (2021), for example, proposed a machine-unlearning framework that partitions training data and model training into more manageable components, allowing targeted retraining when deletion is required.

More recent work has examined the application of machine unlearning to pretrained language models. Yao et al. (2024) evaluate different unlearning methods and demonstrate the potential to reduce the computational burden associated with removing selected training information. Nevertheless, technical efficiency does not automatically establish legal sufficiency. The effectiveness of an unlearning procedure depends on the data targeted, the model architecture, the method employed, and the criteria used to evaluate the outcome. Accordingly, machine

unlearning should be treated as a possible means of implementing erasure obligations rather than as an automatic guarantee of complete data removal.

A related concern is whether AI models can reveal personal information that was included in their training data. Carlini et al. (2021) demonstrate that language models can memorize and reproduce training examples, including information that may not have been intended for disclosure. This finding reinforces the importance of distinguishing between the removal of source records and the reduction of privacy risks arising from trained models. It also raises questions about what evidence should be required to demonstrate that an erasure request has been addressed adequately.

These challenges reveal three interrelated legal concerns. First, the scope of erasure requires clarification regarding whether the relevant obligation concerns source records alone or may also require additional measures where personal information remains recoverable from a trained model. Second, accountability requires an appropriate allocation of responsibilities among controllers, AI developers, and other actors involved in processing. Third, verification requires a defensible method of demonstrating compliance without assuming that a notification of deletion proves the complete removal of all relevant information. These concerns indicate that meaningful protection requires a connection between statutory interpretation, organizational accountability, and proportionate technical measures.

3. Comparative Analysis and Normative Reconstruction

The comparison between Indonesian law and the GDPR provides a basis for identifying opportunities to strengthen the implementation of erasure rights. Although both frameworks recognize personal data protection, their provisions and legal contexts differ. The comparison should therefore identify relevant principles rather than assume that the European framework can be transferred directly into Indonesian law.

The development of the right to be forgotten in European jurisprudence provides an important reference point. In Google Spain SL and Google Inc. v. Agencia Española de Protección de Datos and Mario Costeja González (2014), the Court of Justice of the European Union considered the responsibilities of search engine operators in relation to the processing of personal

Hasanah in Law
ISSN(Online): XXXX-XXXX
Vol 1 No 2 (2026): Oktober 2026
https://hasanah.gerakanedukasi.com/index.php/HIL/index

information and the removal of links from search results. Although this case concerned search engines rather than trained AI models, it illustrates how the continued accessibility of personal information can create legal concerns distinct from the publication of the original information.

The broader significance of erasure rights also relates to the changing relationship between individuals and digital information. Solove (2006) explains that privacy encompasses multiple types of harm and cannot be reduced to a single concept. This perspective is relevant to AI governance because personal information may create risks through its retention, aggregation, reproduction, or use in subsequent decisions. A legal assessment of erasure must therefore consider not only whether a record remains stored, but also the potential consequences of its continued processing.

A further consideration is the distinction between the legal entitlement to request erasure and the technical possibility of implementing it. The study Algorithms that Forget: Machine Unlearning and the Right to Erasure (2023) examines the relationship between Article 17 of the GDPR and the technical feasibility of removing personal information from machine-learning models. The analysis highlights the difficulties of determining whether and how training data influence model parameters, suggesting that legal obligations require interpretation in light of technological capabilities without allowing technical complexity to negate the underlying right.

Table 2. Comparative Analysis of Erasure Rights under Indonesian Law and the GDPR

Comparative dimension	Indonesian legal framework	European Union framework	Implications for normative reconstruction
Legal recognition	Recognizes data subjects' rights to terminate processing, delete, and/or destroy personal data.	Explicitly recognizes the right to erasure.	Clarify the relationship between data subject rights and controllers' obligations.
Conditions for erasure	Establishes statutory grounds for deletion and related actions.	Specifies grounds for erasure and the circumstances in which the right applies.	Develop consistent criteria for evaluating requests involving AI processing.

Hasanah in Law
ISSN(Online): XXXX-XXXX
Vol 1 No 2 (2026): Oktober 2026
https://hasanah.gerakanedukasi.com/index.php/HIL/index

Exceptions and competing interests	Assessed under applicable Indonesian legislation.	Explicitly identifies exceptions to the erasure obligation.	Establish a transparent and proportionate approach to balancing privacy and competing interests.
Implementation in AI systems	Existing obligations must be interpreted in light of AI processing characteristics.	General erasure obligations apply, although technical implementation remains challenging.	Distinguish legal obligations from the technical methods used to implement them.
Accountability and verification	Provides a statutory basis for controller accountability and notification.	Accountability obligations operate alongside the right to erasure and other data protection requirements.	Strengthen documentation, verification, and remedies for inadequate compliance.

Source: Author's comparative analysis of Indonesia's Personal Data Protection Law and Regulation (EU) 2016/679.

Table 2 indicates that the principal opportunity for strengthening Indonesian law lies in clarifying how existing erasure obligations should be implemented in AI-related contexts. The comparison does not imply that the UU PDP lacks a statutory foundation for erasure. Rather, it highlights the need to clarify the relationship between the scope of a data subject's rights, the obligations of controllers, and the measures reasonably required to implement a legally valid request.

The normative reconstruction should distinguish between deleting source data, stopping further processing, restricting access, and reducing the influence of information within a trained model. These measures address different problems and may not be equally appropriate in every case. The required response should therefore depend on the applicable legal grounds, the nature of the information, the purpose of processing, the degree of control exercised by relevant actors, and the feasibility of the proposed measure.

The assessment must also consider competing rights and legitimate interests. An erasure request may concern information subject to legal retention obligations or other recognized

exceptions. In such circumstances, an automatic requirement to remove all related information may be inappropriate. Instead, the decision should be based on a transparent assessment of the legal grounds, the purpose of continued retention, the interests of affected parties, and the proportionality of the proposed measures. This approach would allow Indonesian law to strengthen data subject protection while maintaining legal certainty for organizations processing personal information through AI.

4. A Conceptual Model for Reconstructing Data Subject Protection in the Age of AI

The preceding analysis indicates that the effectiveness of erasure rights depends on the relationship between statutory recognition, legal interpretation, technical implementation, and institutional accountability. Accordingly, this study proposes a conceptual model that connects these dimensions within a coherent framework for protecting data subjects in AI-based processing environments. The model is developed through normative legal analysis and comparative reasoning; it is not presented as an empirically validated regulatory mechanism.

The need for such a model is also reflected in Indonesian scholarship concerning the relationship between personal data protection and records management. Fachmi et al. (2025) highlight the challenges of reconciling the right to be forgotten with organizational obligations to retain records. Similarly, Ajiputera and Susetyo (2024) examine the implementation of deletion rights within Indonesia's positive legal framework. These discussions reinforce the importance of considering the legal grounds for deletion, the interests supporting continued retention, and the procedures through which requests are implemented.

The conceptual model consists of five interconnected components: statutory foundation, legal assessment, implementation of erasure, verification and accountability, and rights-based safeguards. The first component identifies the applicable legal basis. The second determines whether a request satisfies the relevant legal conditions and whether an exception applies. The third identifies appropriate measures for addressing the affected information, while the fourth establishes the documentation and verification needed to assess compliance. The fifth ensures that decisions remain consistent with privacy protection, proportionality, legal certainty, and legitimate competing interests.

Hasanah in Law
ISSN(Online): XXXX-XXXX
Vol 1 No 2 (2026): Oktober 2026
https://hasanah.gerakanedukasi.com/index.php/HIL/index

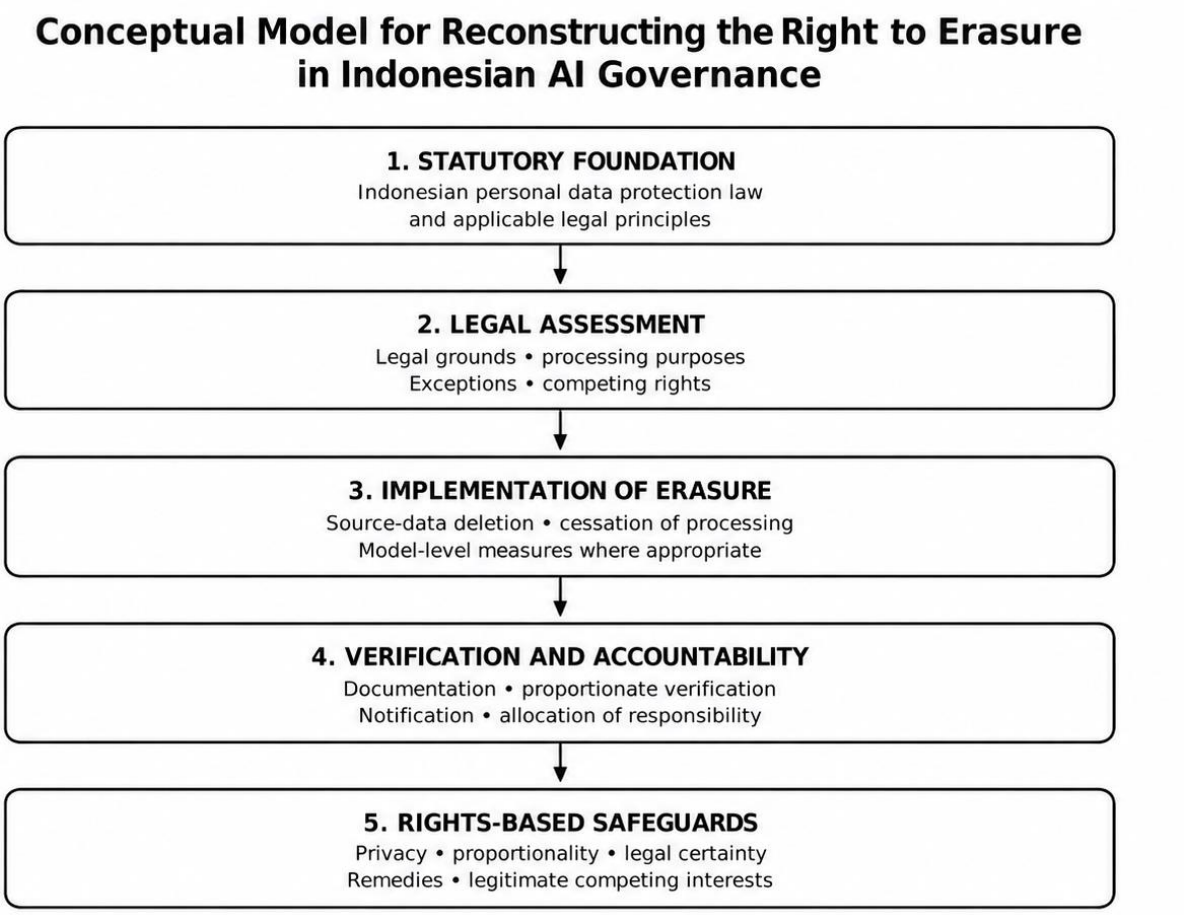


Figure 1. Conceptual Model for Reconstructing the Right to Erasure in Indonesian AI Governance. Source: Author's conceptual development.

The first component establishes the normative foundation for the entire process. The second component evaluates the validity of an erasure request by considering the applicable legal grounds and any relevant exceptions. This assessment is necessary because privacy protection must be reconciled with the legitimate purposes for which information may continue to be retained or processed. Nissenbaum's (2010) contextual approach to privacy provides a useful conceptual perspective for understanding why the legitimacy of information flows depends on their social and institutional context, rather than solely on whether information is publicly accessible.

The third component translates the legal determination into appropriate implementation measures. These may include deleting source records, removing personal information from

associated storage systems, terminating further processing, or applying model-level measures when legally justified and technically appropriate. Mayer-Schönberger (2009) emphasizes the consequences of persistent digital memory, providing a broader conceptual basis for understanding why the ability to remove information is important in digital environments. However, the proposed model does not assume that every erasure request requires machine unlearning. The appropriate response depends on the nature of the data, the applicable legal obligation, and the characteristics of the relevant system.

The fourth component addresses verification and accountability. Controllers should document the measures undertaken, assess whether those measures adequately address the request, and provide notification in accordance with applicable law. Where complete technical removal cannot be established, the response should distinguish between completed actions, residual risks, and any legally justified limitations. The work of Wachter et al. (2017) on transparency and accountability in automated decision-making further illustrates the importance of examining the practical limits of individual rights in complex algorithmic environments. Although their analysis concerns the right to explanation rather than erasure specifically, it reinforces the need to avoid assuming that formal recognition of a right automatically guarantees effective implementation.

Finally, rights-based safeguards operate throughout the model. The exercise of erasure rights must protect personal privacy while considering legal certainty, proportionality, and the rights of other affected parties. This orientation is consistent with the international recognition of privacy under Article 17 of the International Covenant on Civil and Political Rights (United Nations, 1966). The safeguards therefore function not as an additional procedural stage alone, but as principles governing the interpretation and implementation of every component.

The proposed model contributes a normative framework for connecting the legal recognition of erasure rights with their practical implementation in AI-based processing. Its principal contribution is the distinction between the existence of a legal entitlement, the measures adopted to implement it, and the evidence required to assess compliance. By connecting these dimensions, the model provides a foundation for clarifying the responsibilities of relevant actors and

strengthening data subject protection under Indonesian law. Its application to specific AI systems and regulatory practices remains an important subject for further research.

CONCLUSION

This study concludes that Indonesia's Law No. 27 of 2022 concerning Personal Data Protection provides a statutory foundation for exercising the right to erasure, but its implementation in artificial intelligence (AI) environments raises significant interpretive and practical challenges. The distinction between terminating processing, deleting stored data, and addressing personal information incorporated into trained AI models demonstrates that conventional approaches to deletion may not always be sufficient to address the risks associated with AI-based data processing. The central issue is therefore not the absence of legal recognition, but the need to clarify the scope, implementation, and verification of existing erasure obligations.

The comparative analysis of Indonesian law and the European Union's General Data Protection Regulation indicates that strengthening data subject protection requires a clear relationship between the grounds for erasure, applicable exceptions, controller accountability, and competing legal interests. Technical approaches such as machine unlearning may support the implementation of erasure obligations in appropriate circumstances; however, their availability does not automatically establish legal compliance. The adequacy of any measure must be assessed in relation to the applicable legal requirements, the characteristics of the AI system, and the evidence available to demonstrate the outcome.

As its principal contribution, this study proposes a conceptual model comprising five interconnected components: statutory foundation, legal assessment, implementation of erasure, verification and accountability, and rights-based safeguards. The model provides a normative framework for connecting legal entitlements with implementation measures and demonstrable compliance. It also emphasizes that privacy protection must be balanced proportionately with legitimate competing interests, rather than treating erasure as an unconditional obligation to eliminate every instance of information. Future research should examine the applicability of this model to specific AI systems and regulatory practices in Indonesia, including the development of

practical standards for evaluating erasure requests and verifying compliance. Such work would help translate statutory recognition into more effective protection of data subjects in an increasingly AI-driven digital environment.

REFERENCE

Ajiputera, M. T., & Susetyo, H. (2024). Implementasi pengaturan hak untuk dilupakan melalui sistem penghapusan data pribadi dan/atau dokumen elektronik menurut perspektif hukum positif di Indonesia. *UNES Law Review*, *6*(3), 8051–8067. https://doi.org/10.31933/unesrev.v6i3.1706

Bourtoule, L., Chandrasekaran, V., Choquette-Choo, C. A., Jia, H., Travers, A., Zhang, B., Lie, D., & Papernot, N. (2021). Machine unlearning. In *2021 IEEE Symposium on Security and Privacy* (pp. 141–159). IEEE. https://doi.org/10.1109/SP40001.2021.00019

Cao, Y., & Yang, J. (2015). Towards making systems forget with machine unlearning. In *2015 IEEE Symposium on Security and Privacy* (pp. 463–480). IEEE. https://doi.org/10.1109/SP.2015.35

Carlini, N., Tramèr, F., Wallace, E., Jagielski, M., Herbert-Voss, A., Lee, K., Roberts, A., Brown, T., Song, D., Erlingsson, Ú., Oprea, A., & Raffel, C. (2021). Extracting training data from large language models. In *30th USENIX Security Symposium* (pp. 2633–2650). USENIX Association. https://www.usenix.org/conference/usenixsecurity21/presentation/carlini-extracting

Court of Justice of the European Union. (2014). *Google Spain SL and Google Inc. v. Agencia Española de Protección de Datos (AEPD) and Mario Costeja González* (Case C-131/12). https://curia.europa.eu/juris/liste.jsf?num=C-131/12

European Parliament & Council of the European Union. (2016). Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation). *Official Journal of the European Union, L 119*, 1–88. https://eur-lex.europa.eu/eli/reg/2016/679/oj

Fachmi, A., Rahmi, R., & Cholil, A. (2025). Perspektif Perkumpulan Profesi Pengelola Rekod Indonesia (P3RI) tentang *right to be forgotten* dalam pelindungan data pribadi. *BACA: Jurnal Dokumentasi dan Informasi*, *46*(1), 15–32. https://doi.org/10.55981/baca.2025.8952

Hariani, P. E., & Jabbar, M. R. A. A. (2026). Research Approaches and Methods in Educational Management Studies: A Literature Review and Future Research Directions. *Journal of Policy Review and Innovation in Educational Management, 1*(1), 71-83. https://doi.org/10.56404/priem.v1i1.454

Hutchinson, T., & Duncan, N. (2012). Defining and describing what we do: Doctrinal legal research. *Deakin Law Review*, *17*(1), 83–119. https://doi.org/10.21153/dlr2012vol17no1art70

Juliussen, B. A., Rui, J. P., & Johansen, D. (2023). Algorithms that forget: Machine unlearning and the right to erasure. *Computer Law & Security Review, 51*, Article 105885. https://doi.org/10.1016/j.clsr.2023.105885

Mayer-Schönberger, V. (2009). *Delete: The virtue of forgetting in the digital age*. Princeton University Press.

Nissenbaum, H. (2010). *Privacy in context: Technology, policy, and the integrity of social life*. Stanford University Press.

Politou, E., Alepis, E., & Patsakis, C. (2018). Forgetting personal data and revoking consent under the GDPR: Challenges and proposed solutions. *Journal of Cybersecurity, 4*(1), tyy001. https://doi.org/10.1093/cybsec/tyy001

Prabasari, N. K. D. A., Sudharma, K. J. A., & Angelo, M. (2024). The right to be forgotten: Regulation of personal data deletion in Indonesia. *KRTHA BHAYANGKARA, 18*(3), 541–558. https://doi.org/10.31599/krtha.v18i3.3291

Republic of Indonesia. (2022). *Undang-Undang Republik Indonesia Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi*. https://peraturan.bpk.go.id/Details/229798/uu-no-27-tahun-2022

Sanjaya, I. P. G. A., & Prasada, D. K. (2025). The legal framework for personal data deletion on social media in Indonesia: A new chapter in digital privacy protection. *Jurnal Magister Hukum Udayana (Udayana Master Law Journal), 14*(4), 840–852. https://doi.org/10.24843/JMHU.2025.v14.i04.p01

Solove, D. J. (2006). A taxonomy of privacy. *University of Pennsylvania Law Review, 154*(3), 477–564. https://doi.org/10.2307/40041279

United Nations. (1966). *International Covenant on Civil and Political Rights*. https://www.ohchr.org/en/instruments-mechanisms/instruments/international-covenant-civil-and-political-rights

Wachter, S., Mittelstadt, B., & Floridi, L. (2017). Why a right to explanation of automated decision-making does not exist in the General Data Protection Regulation. *International Data Privacy Law, 7*(2), 76–99. https://doi.org/10.1093/idpl/ipx005

Yao, J., Chien, E., Du, M., Niu, X., Wang, T., Cheng, Z., & Yue, X. (2024). Machine unlearning of pre-trained large language models. In *Proceedings of the 62nd Annual Meeting of the Association for Computational Linguistics (Volume 1: Long Papers)* (pp. 8403–8419). Association for Computational Linguistics. https://doi.org/10.18653/v1/2024.acl-long.457

Zhang, D., Finckenberg-Broman, P., Hoang, T., Pan, S., Xing, Z., Staples, M., & Xu, X. (2025). Right to be forgotten in the era of large language models: Implications, challenges, and solutions. *AI and Ethics, 5*, 2445–2454. https://doi.org/10.1007/s43681-024-00573-9

Hasanah in Law

ISSN(Online): XXXX-XXXX
Vol 1 No 2 (2026): Oktober 2026
https://hasanah.gerakanedukasi.com/index.php/HIL/index