Jurnal Mediasas: **Media Ilmu Syari'ah dan Ahwal Al-Syakhsiyyah**
https://journal.staisar.ac.id/index.php/mediasas
Vol. 8, No. 4, 2025, pp. 1008-1028
P-ISSN (Print) 2655-1497 | E-ISSN (Online) 2808-2303
DOI: 10.58824/mediasas.v8i4.501

Regulating the Right to Be Forgotten in Indonesia's Digital Banking: Lessons from the EU GDPR

Winco Librawenson[1], Hari Sutra Disemadi[2*], Windi Afdal[3]

[1-3] Faculty of Law, Universitas Internasional Batam, Indonesia
*Corresponding Author: hari@uib.ac.id

‖ Received : 15-10-2025 ‖ Accepted: 12-01-2026 ‖ Published: 13-01-2026

Abstract

The implementation of the right to be forgotten in digital banking transactions in Indonesia faces complex legal challenges. Legal disharmony among regulations on personal data protection, electronic information and transactions, and banking law creates uncertainty in applying this right. This study aims to evaluate the legal framework of the right to be forgotten in Indonesia and compare it with the European Union's General Data Protection Regulation (GDPR) to identify an ideal normative solution. The research employs a normative legal method with statutory and comparative approaches. The findings indicate that the GDPR provides a more flexible data deletion mechanism, including the existence of an independent supervisory authority and simpler procedures for individuals to request data erasure. To enhance legal certainty in regulating the right to be forgotten in Indonesia, legal reform is necessary. This includes harmonizing existing regulations, formulating technical guidelines for Electronic System Providers (ESPs), and establishing an independent Personal Data Protection Authority similar to the European Data Protection Board (EDPB).

[*Penerapan hak untuk dilupakan (right to be forgotten) dalam transaksi perbankan digital di Indonesia menghadapi tantangan hukum yang kompleks. Disharmonisasi hukum antara regulasi perlindungan data pribadi, regulasi informasi dan transaksi elektronik, serta regulasi perbankan, menciptakan ketidakpastian dalam implementasi hak ini. Penelitian ini bertujuan untuk mengevaluasi pengaturan hak untuk dilupakan di Indonesia dan membandingkannya dengan General Data Protection Regulation (GDPR) Uni Eropa guna menemukan solusi normatif yang ideal. Metode yang digunakan adalah penelitian hukum normatif dengan pendekatan perundang-undangan dan perbandingan hukum. Hasil penelitian menunjukkan bahwa GDPR memiliki mekanisme yang lebih fleksibel dalam penghapusan data, termasuk otoritas independen yang mengawasi kepatuhan serta prosedur yang lebih sederhana bagi individu untuk mengajukan permintaan penghapusan data. Untuk meningkatkan kepastian hukum pengaturan hak untuk dilupakan di Indonesia, diperlukan reformasi hukum yang mencakup harmonisasi regulasi, penyusunan pedoman teknis bagi Penyelenggara Sistem Elektronik (PSE), serta pembentukan Otoritas Perlindungan Data Pribadi yang independen seperti European Data Protection Board (EDPB) di Uni Eropa.*

Keywords: Right to be Forgotten, Personal Data Protection, Digital Banking, Legal System, Ideal Regulation

How to Cite: Librawenson, W., Disemadi, H. S., & Afdal, W. (2026). Regulating the Right to Be Forgotten in Indonesia's Digital Banking: Lessons from the EU GDPR. *Jurnal Mediasas: Media Ilmu Syari'ah Dan Ahwal Al-Syakhsiyyah, 8*(4), 1008–1028. https://doi.org/10.58824/mediasas.v8i4.501

INTRODUCTION

In the ever-evolving digital era, technology has become an inseparable part of human life (Dian Sudiantini et al., 2023; Situmeang et al., 2025), including within the banking sector (Chauhan et al., 2022). Digital banking, as a product of technological and internet advancements, enables financial transactions to be conducted swiftly, conveniently, and effectively (Chaniago & Sari, 2023). In Southeast Asia (ASEAN), digital banking has experienced significant growth, with the number of banking application installations increasing by 32% from 2022 to 2023, driven by rapid developments in Vietnam and Thailand (Adjust, 2023). In Indonesia, digital banking usage rose in Q1/2024, with total financial transactions through digital banking reaching IDR 15,881.53 trillion, underscoring the sector's critical role in the digital economy (Yuliana et al., 2024).

Digital banking constitutes a novel innovation in banking services, relying on technological advancements to provide convenience, speed, and enhanced customer experience (Sudirman & Disemadi, 2023). By optimizing the use of customer data, this service allows banking transactions and activities to be conducted independently, anytime and anywhere, without the need to visit a physical branch. Within digital banking, the use of personal data for account creation is founded upon two fundamental principles in the banking sector: the prudential principle and the know your customer (KYC) principle. The prudential principle, as stipulated in Article 2 of Law Number 10 of 1998 concerning Amendments to Law Number 7 of 1992 on Banking (the Banking Law), obligates banking institutions to ensure the security and validity of collected personal data to prevent risks such as fraud or money laundering. Meanwhile, the KYC principle is regulated under Bank Indonesia Regulation Number: 14/27/PBI/2012 concerning the Implementation of Anti-Money Laundering and Counter-Terrorism Financing Programs for Commercial Banks, which revokes the previous regulations (BI Regulation No. 3/23/PBI/2001 amending BI Regulation No. 3/10/PBI/2001 on the Application of the Know Your Customer Principles).

Table 1. Digital Banking Users and Transactions in Indonesia (2024)

Company	Total Users	Total Transactions	Transaction Value	Applications and Websites
PT Bank Tabungan Negara (Persero) Tbk (BBTN)	2.7 million	415 million	IDR 57.5 trillion	BTN Mobile
PT Bank Rakyat Indonesia (Persero) Tbk (BBRI)	33.5 million	969.9 million	IDR 1,251.1 trillion	BRImo
PT Bank Negara Indonesia (Persero) Tbk (BBNI)	16.9 million	318 million	IDR 347 trillion	BNI Mobile Banking
PT Bank Mandiri (Persero) Tbk (BMRI)	24 million	846 million	IDR 921 trillion	Livin'
PT Bank Central Asia Tbk (BBCA)	28.3 million	7.2 billion	IDR 6,586 trillion	m-BCA and klikBCA
PT Allo Bank Indonesia Tbk	9 million	-	-	allobank

Source: CBNC Indonesia (Setiawati, 2024).

Based on the data above (Table 1), the number of users and transaction volumes in Indonesia's digital banking sector in 2024 illustrate the immense volume of customer data managed by banks as personal data controllers. With tens of millions of users and billions of transactions, banks bear a significant responsibility to safeguard customers' personal data, as regulated under Law Number 27 of 2022 concerning Personal Data Protection (PDP Law). Constitutionally, the right to personal data protection is also recognized under Article 28G paragraph (1) of the 1945 Constitution of the Republic of Indonesia (UUD NRI 1945).

Ideally, customer personal data is legally protected under the PDP Law and the 1945 Constitution. These regulations mandate that data controllers, including banks, must protect customer personal data with adequate security measures. Consequently, banks are obligated to ensure the security of their systems to prevent unauthorized access or data breaches that may harm customers. However, the reality (das Sein) reveals a gap between legal norms and practical implementation. For instance, the data breach incident at Bank Syariah Indonesia in 2022, which affected data of 15 million users and employees, exposed critical weaknesses in data security practices despite existing regulatory obligations (Isnugraheny et al., 2024). This incident reflects a failure to implement effective data protection and highlights the need for regulatory strengthening and stricter enforcement. Without concrete actions, personal data protection risks remaining an ideal norm that fails to provide genuine security in the digital ecosystem.

The right to be forgotten is considered a potential solution to mitigate personal data breaches. In Indonesia, this right is regulated under Article 26 paragraph (3) of Law Number 1 of 2024 concerning the Second Amendment to Law Number 11 of 2008 on Electronic Information and Transactions (hereinafter referred to as the ITE Law), and further reinforced by Articles 8, 16, 43, and 44 of the PDP Law. This right grants data subjects the authority to delete or destroy irrelevant data, whether in the digital realm or specific locations causing harm (Ajiputera & Susetyo, 2024; Farhan et al., 2022; Ramadaani & Muaalifin, 2023). In practice, the implementation of this right faces normative conflicts, such as Article 56 paragraph (1) of OJK Regulation No. 23/POJK.01/2019, which mandates financial service institutions to retain transaction documents, information, and other data related to customers or walk-in clients for a minimum of five years after termination of the customer relationship. Moreover, the requirement for court approval to execute a data deletion request under Article 26 paragraph (3) of the ITE Law also poses a challenge. This process contradicts Article 43 paragraph (1) of the PDP Law, which states that personal data must be deleted if it is no longer necessary for the purpose of processing (i.e., after business relations have ended). The necessity for a court decision is viewed as a lengthy process, thus rendering the initial objective of providing swift protection less effective.

Previous research has extensively discussed the right to be forgotten (RTBF) within the context of Indonesian regulations. Several studies have highlighted deficiencies in Indonesia's legal framework, including unclear deletion mechanisms, absence of a dedicated data erasure authority, weak sanctions for non-compliant electronic system operators, and conflicts between the RTBF and freedom of expression or public access to information. Research by Adinda Setyaning Putri (2023) revealed legal ambiguities in the ITE Law regarding RTBF, particularly the lack of sanctions for electronic system operators refusing data deletion requests. The study compares several countries and suggests that the French regulatory model may serve as a reference for Indonesia (Setyaning Putri, 2023). Syafira Agata Ramadhani (2022) points out Indonesia's inadequate data protection regulations compared to the GDPR but does not specifically address RTBF challenges in digital banking transactions. Although regulatory gaps are a primary issue, this study does not explore how the GDPR establishes a stronger deletion mechanism (Ramadhani, 2022). Meanwhile, research by Muhammad Taufik Ajiputera and Heru Susetyo (2024) identifies challenges in the implementation of RTBF in Indonesia, such as slow deletion processes, blocking-only mechanisms, and the absence of a dedicated institution for personal data deletion. However, their study remains broadly normative and lacks practical legal comparisons with the GDPR (Ajiputera & Susetyo, 2024). Other studies, such as those by Trisoko Sugeng Sulistyo et al. (2024), indicate that RTBF regulations in Indonesia still lack clear procedures, both in terms of submission processes and compliance monitoring mechanisms for electronic system operators (Nugroho & Abdullah, 2020; Sulistyo et al., 2024). However, these studies have yet to analyze how regulatory comparisons with the GDPR can offer practical solutions to enhance the effectiveness of RTBF.

This study offers novelty by addressing the gap in existing literature through an in-depth examination of how the GDPR may contribute to enhancing the effectiveness of the right to be forgotten in Indonesia, particularly in the context of digital banking transactions. The main focus is to compare the RTBF regulations in the European Union and explore how they can be adapted into Indonesia's legal system. Furthermore, this study will utilize the theory of progressive law to formulate adaptive legal solutions aligned with digital developments. This research goes beyond mere regulatory comparison by offering concrete solutions for Indonesia to improve the effectiveness of RTBF implementation within the digital banking sector.

METHOD

The research method employed in this study is normative legal research. Normative legal research is used to address specific legal issues by examining how a legal issue can be resolved and where the relevant legal regulations may be found (Tan, 2021). This method possesses distinct characteristics in its research objectives (Disemadi, 2022), one of which in this study is to examine a comparative legal analysis concerning the regulation of the right to be forgotten between Indonesia and the European Union. This study applies a statutory approach and a comparative legal approach. The data utilized consists of secondary data (indirectly obtained data), specifically legal materials. The data collection technique adopted is library research (bibliography study). The secondary data/legal materials used in this research include: The 1945 Constitution of the Republic of Indonesia (UUD NRI 1945); Law Number 10 of 1998 concerning the Amendment to Law Number 7 of 1992 on Banking; Bank Indonesia Regulation Number 14/27/PBI/2012 concerning the Implementation of the Anti-Money Laundering and Counter-Terrorism Financing Program for Commercial Banks; Law Number 27 of 2022 concerning Personal Data Protection; Law Number 1 of 2024 concerning the Second Amendment to Law Number 11 of 2008 on Electronic Information and Transactions; Law Number 39 of 1999 on Human Rights; Government Regulation Number 71 of 2019 concerning the Implementation of Electronic Systems and Transactions; Law Number 21 of 2011 on the Financial Services Authority; Bank Indonesia Regulation Number 23/7/PBI/2021 concerning Payment System Infrastructure Operators; Law Number 21 of 2008 concerning Sharia Banking; Financial Services Authority Regulation (POJK) Number 23/POJK.01/2019 concerning the Amendment to POJK Number 12/POJK.01/2017 on the Implementation of the Anti-Money Laundering and Counter-Terrorism Financing Program; Financial Services Authority Regulation Number 6/POJK.07/2022 concerning Consumer Protection in the Financial Services Sector; 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, and repealing Directive 95/46/EC (General Data Protection Regulation - GDPR); and The 2014 judgment of the Court of Justice of the European Union (CJEU). For data analysis, the researcher employed a descriptive-qualitative technique, which emphasizes the quality of the research by interpreting the meaning of qualitative, non-numerical data.

RESULTS AND DISCUSSION

Weaknesses in the Regulation of the Right to Be Forgotten in Digital Banking Transactions in Indonesia

The right to be forgotten (RTBF) is a legal principle that grants individuals, as personal data subjects, the ability to protect their personal data or any information related to them as users. This right encompasses the request to delete personal information from online databases, search engines, and digital archives, particularly where such information is outdated, irrelevant, or potentially detrimental to their privacy (Bode & Jones, 2017; Lie et al., 2023; Verheij, 2016). The right was first formally recognized in Article 17 of the European Union's General Data Protection Regulation (GDPR), following the landmark ruling in *Google Spain SL v. Agencia Española de Protección de Datos (AEPD) and Mario Costeja González* (2014). Since its recognition, the right to be forgotten has sparked considerable debate regarding the balance between the right to privacy and freedom of expression, with diverse legal interpretations emerging across jurisdictions, including the United States, the European Union, India, and Pakistan (Asma Jabeen Khan et al., 2025). The implementation of this right has become increasingly complex in the digital age, particularly due to its intersection with technological advancements such as artificial intelligence (AI) and machine learning (ML), which heavily rely on large datasets for optimization and decision-making (Liu & Liu, 2025).

One of the principal challenges in implementing the right to be forgotten is the concept of "machine unlearning," a process whereby AI systems trained on personal data must be retrospectively altered to "forget" specific information (W. Wang et al., 2025). While regulators continue to design data deletion guidelines, concerns have been raised about potential misuse of this right as a tool for censorship or suppression of public information. Some studies suggest that incentive-based compliance models may encourage corporate adherence to data deletion rules while safeguarding user privacy (Q. Wang et al., 2025). Moreover, emerging post-processing frameworks are being developed to ensure that data deletion can be balanced with the integrity of algorithmic functions (Zhang et al., 2025). The evolution of the right to be forgotten at the intersection of law and technology highlights the necessity of ongoing discourse concerning privacy protection, ethical use of AI, and the public's right to access relevant information.

Constitutionally, the right to be forgotten is relevant to several provisions within the 1945 Constitution of the Republic of Indonesia (UUD NRI 1945), particularly those relating to human rights and personal data protection. Article 28G(1) provides that: *"every person shall have the right to the protection of their personal self, family, honor, dignity, and property under their control, and shall have the right to feel secure and be protected from fear of threats in doing or not doing something that constitutes a human right."* This article may be interpreted as a constitutional basis for the individual's right to delete digital traces that may threaten their privacy and dignity. Furthermore, Article 28H(4) affirms that every person has the right to protection of private property, which, in the digital context, may extend to an individual's personal data stored on various online platforms.

Law Number 39 of 1999 on Human Rights (the Human Rights Law) is also relevant to the concept of the right to be forgotten, which has developed in the current digital era. Relevant provisions of the Human Rights Law include Article 12, which guarantees every individual's right to a private life protected from interference, and Article 17, which affirms the right to obtain justice and legal certainty for individuals who feel that their rights have been violated. In the context of the right to be forgotten, these provisions may be interpreted as protecting individuals from the dissemination of personal information in cyberspace that may harm their social or professional lives. Additionally, Article 22 of the Human Rights Law further strengthens the position of the right to be forgotten by providing protection for individuals against defamation or unjustly harmful information.

In today's digital era, the right to be forgotten has increasingly become part of the human rights discourse, due to the vast amount of personal data stored on the internet (Mutiara & Maulana, 2020). Article 71 of the Human Rights Law emphasizes that the State is obligated to respect, protect, and fulfill human rights, including the right to control personal data. Accordingly, the Human Rights Law serves as a normative foundation to reinforce the need for clearer regulation on the right to be forgotten, including how the State and technology companies can be held accountable for ensuring individuals' rights to personal data protection (Nirwana et al., 2024).

Although the right to be forgotten has not yet been fully accommodated within national regulation, it is recognized under Article 26 paragraphs (3) and (4) of Law Number 1 of 2024 concerning the Second Amendment to Law Number 11 of 2008 on Electronic Information and Transactions (the ITE Law). Article 26 of the ITE Law stipulates the obligation of Electronic System Operators (ESOs) to delete electronic information or documents that are deemed "irrelevant," upon the request of the concerned individual, subject to a court decision. Furthermore, ESOs are also required to provide a "data deletion mechanism" in accordance with applicable laws and regulations. This provision adopts the right to be forgotten principle as applied in the European Union through the GDPR, but with a more limited approach due to the requirement of a judicial order.

This article demonstrates that the right to be forgotten in Indonesia is neither automatic nor absolute, but instead requires a formal legal mechanism to be exercised. This means that individuals seeking to delete their personal information from digital platforms must submit a request to the court in advance. This approach aims to strike a balance between the individual's right to privacy and the public's right to information, thereby ensuring that not all information may be unilaterally removed by individuals or digital platforms. However, this mechanism may also pose implementation challenges, particularly with respect to the lengthy legal process and limited public awareness of the procedures involved.

Moreover, Article 14 paragraphs (1) and (2) of Government Regulation Number 71 of 2019 on the Implementation of Electronic Systems and Transactions (PP PSTE) also regulates the right to be forgotten. This article affirms that individuals have the right to request the deletion of harmful personal information in digital spaces. It imposes an obligation on ESOs to delete electronic information and/or electronic documents upon the request of the data owner. This right is generally invoked in the context of privacy protection, particularly for individuals who have been victims of personal data misuse on the internet. However, Siregar & Arifiyanto (2024) note that the application of this provision within Indonesia's legal system still faces execution challenges, especially regarding the involvement of global digital platforms and suboptimal enforcement mechanisms (Simbolon et al., 2025).

Under Law Number 27 of 2022 on Personal Data Protection (the PDP Law), specifically Article 8, it is affirmed that every personal data subject has full rights over their personal data, including the right to terminate processing, delete, and/or destroy personal data relating to them. This provision is consistent with the principles of privacy protection and individual sovereignty over personal information. The right to delete and/or destroy personal data is granted to ensure that an individual's personal data is not continuously used or stored without consent or a legitimate purpose. The regulation of the right to be forgotten is not limited solely to the deletion and destruction of data, but also governs the consent required for the use of personal data belonging to the data subject. Article 20 of the PDP Law stipulates that the basis for personal data processing requires the consent of the personal data subject for the use of their information for one or more agreed purposes. Furthermore, Article 16 paragraph (1), Article 45, Article 48 paragraph (4), and Article 57 paragraph (2) of the PDP Law emphasize that the right to be forgotten constitutes part of an individual's right to control their personal data that has been published online. These provisions regulate the deletion or termination of access to personal data that is no longer relevant or that violates an individual's privacy rights.

The right to be forgotten in digital banking in Indonesia must be examined within the context of Law Number 10 of 1998 concerning the Amendment to Law Number 7 of 1992 on Banking (the Banking Law) and Law Number 21 of 2008 on Sharia Banking (the Sharia Banking Law). As Electronic System Operators (ESOs), digital banks are required to ensure compliance with the ITE Law, the PDP Law, and the PP PSTE, which regulate the individual's right to delete personal data when it is no longer necessary or has been used without consent. Compliance by ESOs with these provisions is also supported by the research of Prastyanti & Sharma (2024). However, although the Banking Law and the Sharia Banking Law impose obligations on banks to store and protect customer data, such obligations may potentially conflict with the principles of data deletion or the right to be forgotten as regulated under the ITE Law, the PDP Law, and the PP PSTE.

In digital banking systems, customer data is often required to be retained for audit purposes, compliance with anti-money laundering regulations, and the prevention of terrorism financing, thereby rendering the right to be forgotten non-absolute (Yuspin et al., 2023). Article 40 of the Banking Law provides that banks are obligated to maintain the confidentiality of information concerning depositors and their deposits, except in certain circumstances stipulated by law. This obligation is closely related to the right to be forgotten, as arbitrary deletion of customer data may conflict with the principle of banking secrecy and legal protection for customers. Additionally, Article 29 of the Banking Law requires banks to apply the prudential principle in their operations, including in the management of customer data. The right to be forgotten must not obstruct banks from fulfilling their legal obligations to retain transaction data for audit purposes, financial investigations, and compliance with anti-money laundering regulations. Similarly, Article 55 of the Sharia Banking Law stipulates that Islamic banks are required to maintain customer confidentiality and are prohibited from disclosing information regarding accounts and financial transactions to third parties, except under specific conditions such as law enforcement requirements or customer consent. This demonstrates that although the right to be forgotten may be granted to customers, there are legal limitations on banks in fully deleting data due to mandatory financial transaction recordkeeping obligations.

The obligation of financial institutions to retain transaction data for a specified period also gives rise to conflicts between customers' rights to delete data and banks' legal obligations to retain such data (Jameaba, 2024). Article 47 of the Banking Law potentially conflicts with the regulation of the right to be forgotten, as it requires banks to retain financial transaction documents for a certain period of time. This provision aims to ensure that transaction data remains available in the event of financial investigations or other legal necessities. If the right to be forgotten were applied absolutely, banks could face legal obstacles when such data is required for investigations or legal disputes. Furthermore, Article 65 of the Sharia Banking Law emphasizes that every transaction conducted under a Sharia contract must be recorded in a complete and transparent manner. This indicates that the right to be forgotten in Sharia banking cannot be applied absolutely, as transaction recordkeeping constitutes part of the principle of *amanah* (trustworthiness), which forms the foundation of Sharia banking operations.

Harahap & Afandi (2023), in their research, also asserted that the right to be forgotten within Sharia banking must be aligned with the principles of justice and transparency, which constitute the operational foundations of the Sharia banking system (Harahap et al., 2023). Several contracts (*akad*) in Sharia banking, such as murabahah or ijarah, carry long-term legal consequences requiring banks to retain customer data to ensure transaction transparency and compliance with the standards of the National Sharia Council – Indonesian Ulema Council (Dewan Syariah Nasional–Majelis Ulama Indonesia or DSN–MUI). Accordingly, requests for data deletion by customers in Sharia banking schemes may present challenges, particularly when they involve unsettled financial transactions or transactions with long-term legal implications (Rusydiana & Kanz, 2024). Furthermore, Sharia banks must ensure that the implementation of the right to be forgotten does not violate the principle of trust (*amanah*) in the management of customer funds, which is a core pillar of the Sharia banking system.

Despite the various limitations in the implementation of the right to be forgotten, both the Banking Law and the Sharia Banking Law recognize the customer's right to manage their personal data. Article 11 of the Sharia Banking Law provides that banks must prioritize transparency and fairness in the provision of financial services, including the protection of customer data. This means that in certain situations, banks may consider customer requests to delete personal data that is no longer relevant, provided that doing so does not violate other regulatory requirements mandating the retention of transaction data. In contrast, while the Banking Law does not explicitly regulate the right to be forgotten, customer protection principles may still be applied by reference to other prevailing laws and regulations in Indonesia.

Regulatory disharmony regarding the right to be forgotten and the banking sector's obligation to retain customer data and transactional records for a specified period, as stipulated in the Banking Law and the Sharia Banking Law, is further reinforced by the Financial Services Authority Regulation (POJK) Number 23/POJK.01/2019, which amends POJK Number 12/POJK.01/2017 on the Implementation of Anti-Money Laundering and Counter-Terrorism Financing Programs (POJK No. 23/POJK.01/2019). Although the ITE Law, the PDP Law, and the PP PSTE guarantee personal data security through provisions allowing the deletion of data subjects' information when it is no longer relevant to the original processing purpose, Article 56 paragraph (1) of POJK No. 23/POJK.01/2019 mandates a minimum five-year retention period for customer-related data. This retention period is intended to ensure the soundness of banking institutions and is aligned with the implementation of the prudential principle and the know-your-customer (KYC) principle. However, the existence of such regulation results in normative inconsistency and the potential for conflict of norms.

This regulatory disharmony reflects the tension between individual interests and public interests. The provisions on the right to be forgotten under the ITE Law, PDP Law, and PP PSTE confer individuals with the right to request the deletion of their personal data from digital banking systems, particularly when such data is no longer relevant or has been used without consent. However, digital banking regulations—such as those contained in the Banking Law, the Sharia Banking Law, and POJK No. 23/POJK.01/2019—require banks to retain transaction records and customer data for a defined period for the purposes of auditing, regulatory compliance, and financial investigations. This creates an imbalance between the individual's right to privacy and the banking sector's obligations to maintain the integrity of the financial system.

From the perspective of public interest, the retention of transaction data for a set period is essential for preserving financial stability and mitigating the risks of financial crimes such as money laundering and terrorism financing. However, from the individual's standpoint, the right to privacy and control over personal data is a fundamental principle in the digital era that must be guaranteed by both the government and financial institutions.

According to Gustav Radbruch, an ideal legal system must reflect three core legal values, one of which is legal certainty (Andrianto, 2020). Within the framework of Legal System Theory, the weakness in the regulation of the right to be forgotten—namely, regulatory disharmony—can be analyzed through the aspect of legal substance. Legal substance encompasses rules governing the rights and obligations of individuals and institutions. Any regulatory framework that demonstrates disharmony between individual privacy rights and public interests creates legal uncertainty, which may hinder the effective implementation of the right to be forgotten.

Another notable weakness lies in the **procedural and technical complexity** of deleting personal data belonging to data subjects. Pursuant to Article 26 of the ITE Law, personal data subjects must first obtain a court decision in order to exercise their right to deletion or delisting from search engines. This requirement causes concern due to the uncertainty surrounding the timing of the court's issuance of such decisions, during which time the dissemination of the information in question may continue to expand.

An additional issue arises within the context of digital banking, where customers' transaction data is often stored in decentralized systems, which are inherently difficult to fully erase (Yuspin et al., 2023). Although the regulation of the right to be forgotten is intended to provide individuals with a sense of data security, its effectiveness is undermined by delays in the actual execution of deletion or delisting processes. Therefore, as Nurulhaq, Junus, and Towadi (2023) argue, there is a need for more specific regulations to establish clear procedures for the implementation of the right to be forgotten, in order to avoid disrupting the integrity of the banking system as a whole (Savira Nurulhaq et al., 2023).

From the perspective of legal substance, the procedural and technical weaknesses in the regulation of the right to be forgotten contribute to legal uncertainty. This uncertainty in the legal process risks prolonging the exposure of information that should be deleted, thereby diminishing the effectiveness of data protection. Moreover, digital banking institutions, as Electronic System Operators (ESOs), face a regulatory dilemma: complying with data deletion orders while simultaneously fulfilling their obligation to retain financial transaction records for audit and supervisory purposes.

In an ideal legal system, legal substance should reflect a balanced consideration between individual rights and the institutional responsibilities of financial entities. However, the current regulatory framework has yet to achieve this balance between the protection of individual privacy rights and the legal obligation to retain data within the digital banking sector. As such, strengthening the legal substance surrounding the right to be forgotten must focus on the harmonization of cross-sectoral regulations and the establishment of clearer legal procedures.

Structural and Legal Culture Challenges in Implementing the Right to Be Forgotten in Digital Banking Transactions in Indonesia

Under Lawrence M. Friedman's Legal System Theory, *legal structure* refers to the institutions and mechanisms that enforce legal rules, including the judiciary, law enforcement agencies, and regulatory bodies responsible for ensuring the implementation of the law. Legal structure plays a central role in ensuring the applicability and effectiveness of legal norms in society (Syafri Hariansah, 2022). In Indonesia, one of the main challenges within the legal system is the lack of harmony among legal institutions involved in regulatory implementation (Pahlevi, 2022). Furthermore, the legal structure often fails to function optimally due to weak inter-agency coordination and limited resources in law enforcement. The complex legal bureaucracy in Indonesia frequently hinders the implementation of legal policies, especially those concerning personal data protection and digital transactions (Muttaqin & Saputra, 2019).

Meanwhile, within Friedman's theory, *legal culture* refers to the attitudes, values, and behaviors of both the public and legal actors toward the prevailing legal rules (Odhy, 2021). A strong legal culture supports legal compliance and fosters a high level of legal awareness within society. However, in Indonesia, a major challenge within the legal culture lies in the low public awareness of legal rights and obligations, as well as limited trust in the legal system (Hutomo & Soge, 2021).

The legal structure in the implementation of the right to be forgotten in digital banking transactions involves key institutions such as the Financial Services Authority (Otoritas Jasa Keuangan or OJK), Bank Indonesia (BI), and the Judiciary. OJK is responsible for supervising and regulating the financial services sector, including digital banking, pursuant to Law Number 21 of 2011 on the Financial Services Authority (OJK Law). Article 4 of the OJK Law states that OJK aims to ensure that the financial services sector—including digital banking—operates in an orderly, fair, transparent, accountable, and stable manner. In addition, OJK bears the responsibility of protecting consumer and public interests to support sustainable financial system growth. As the primary regulator of the financial sector in Indonesia, OJK faces substantial challenges in regulating and enforcing customer data protection, particularly in the context of digital banking.

One of OJK's key limitations as a financial sector regulator is the lack of specific regulations concerning the deletion of customer data within digital banking systems. Consequently, OJK is constrained in enforcing customer data deletion requests due to weaknesses in the legal framework governing personal data protection within the financial sector. In conventional banking, the management of customer data still relies on broader compliance-based regulations, such as OJK Regulation No. 6/POJK.07/2022 on Consumer Protection in the Financial Services Sector. However, in the digital domain, the complexity of data management has increased, particularly with the use of cloud computing technologies and big data systems, which allow customer data to be stored and processed across multiple locations, including outside Indonesia's jurisdiction.

The absence of specific provisions or clear technical standards for handling data deletion requests has resulted in broad discretion for financial institutions to establish their own internal policies. As a result, customers' rights to have their data deleted are often obstructed by internal policies formulated by the banks themselves. Another limitation lies in the lack of regulatory alignment between OJK regulations and broader data protection frameworks, such as the Personal Data Protection Law (PDP Law). Although OJK holds the authority to supervise and impose sanctions on financial institutions that violate data protection regulations, its enforcement capacity remains limited due to overlapping regulatory domains with other institutions, such as Bank Indonesia and the Ministry of Communication and Information Technology (Njatrijani, 2019; Windani & Widiani, 2024). This has led to a lack of clarity in the mechanisms for customers to request deletion of their data from financial institutions.

Technological and infrastructure limitations within the Financial Services Authority (OJK) also present significant barriers to the supervision of customer data protection policies in the digital banking sector (Arifuddin & Yusuf, 2024). The rapid advancement of financial technology (fintech) and cloud-based banking systems has accelerated the digitalization of financial services. However, OJK remains lagging behind in terms of technology-based supervision. Many digital banking institutions and fintech platforms utilize foreign-based infrastructure, which poses challenges to the enforcement of customer data deletion, as such data is often stored on servers located outside Indonesia's jurisdiction and beyond OJK's regulatory reach. As a result, even though Indonesian regulations require Electronic System Operators (ESOs), including digital banks, to delete inactive customer data or data requested to be erased, implementation becomes difficult due to the lack of control over data storage locations.

Furthermore, limitations in law enforcement capacity also constitute a major factor constraining OJK's role as part of the legal structure in the implementation of the right to be forgotten in digital banking transactions. To date, OJK has yet to establish a robust sanction mechanism for financial institutions or digital banks that fail to comply with data deletion policies. As a result, it is anticipated that many digital banks will disregard data deletion requests without facing clear consequences. Currently, OJK lacks sufficient technical infrastructure to conduct comprehensive audits of digital banking data management systems and largely relies on voluntary compliance and self-reporting by banks. Consequently, the implementation of the right to be forgotten in digital banking remains far from the ideal.

Similarly, Bank Indonesia (BI), as the country's monetary and payment systems authority, plays a crucial role in the regulation of the banking sector, including digital banking institutions. BI's role is governed by Law Number 3 of 2004 concerning the Amendment to Law Number 23 of 1999 on Bank Indonesia (BI Law), which mandates BI to formulate and implement monetary policy, maintain financial system stability, and regulate the smooth operation of the payment system. Article 8 of the BI Law establishes BI's core functions in setting monetary policy, managing the payment system, and supervising the banking sector to ensure national economic stability. Moreover, Article 10 affirms BI's authority to regulate payment systems, including those managed by both conventional and digital service providers, to ensure efficiency and security in financial transactions in Indonesia.

However, in the context of customer data protection, BI has yet to issue any specific regulation or guidance on handling customer requests for personal data deletion. This presents a significant challenge in the digital era, wherein customer data is stored within electronic systems often operated by third parties. One of the main regulatory challenges currently faced by BI is the absence of standards aligned with international practices, such as the General Data Protection Regulation (GDPR) of the European Union, which provides individuals with explicit rights to request the deletion of their data.

Although BI has issued several regulations concerning consumer protection in the payment systems and banking services sector—such as Bank Indonesia Regulation (PBI) Number 3 of 2023 on Consumer Protection and PBI Number 23/7/PBI/2021 on Payment System Infrastructure Providers—these regulations do not focus on individual rights related to ownership or deletion of personal consumer data. As a result, the lack of regulatory frameworks or clear guidelines from BI regarding mechanisms for deleting customer data within an increasingly digitized banking system has led to weak enforcement of digital banks' compliance with customer data protection obligations.

Furthermore, the judiciary, as part of the legal structure in implementing the right to be forgotten within digital banking transactions, holds the authority to order the deletion of personal data when requested by individuals who have suffered harm as a result of personal data misuse. This is in line with Article 26 of the ITE Law, which grants individuals the right to request the deletion of data that is no longer relevant, was used without consent, or causes harm.

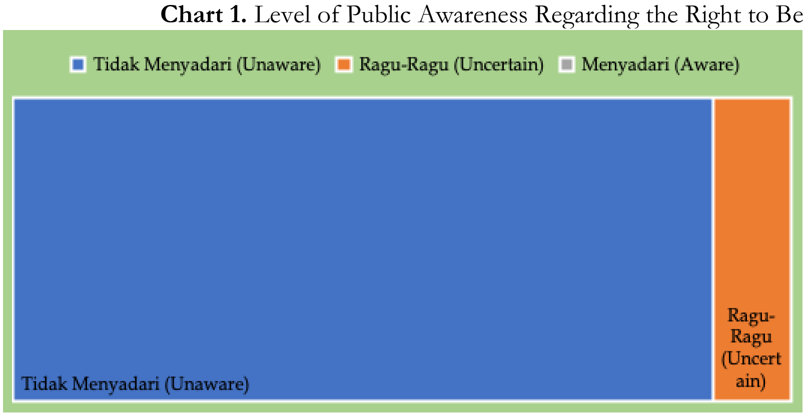
However, the lack of specific regulations governing the implementation mechanism for court-ordered data deletion presents a significant challenge. The enforcement of such court orders is hindered by the absence of an integrated system to ensure compliance by digital banking institutions, which act as Electronic System Operators (ESOs). As a result, court decisions ordering data deletion may not be effectively enforced, especially considering Article 56 paragraph (1) of Financial Services Authority Regulation (POJK) No. 23/POJK.01/2019, which mandates the retention of customer-related data for a minimum period of five years. This data retention requirement serves purposes such as audits, taxation, and compliance with anti-money laundering regulations, which directly conflict with the principle of the right to be forgotten.

Consequently, digital banks may encounter difficulties in determining the scope and timing of data deletion in accordance with court rulings, particularly in cases where regulatory obligations require data retention for a fixed period. The absence of clear regulatory standards on how digital banking institutions, as ESOs, must respond to and implement court orders regarding data deletion is a major factor impeding the enforcement of judicial decisions.

In addition to challenges related to the legal structure, legal culture also serves as a significant barrier to the enforcement of the right to be forgotten in the digital banking ecosystem. Legal culture reflects the perceptions, understanding, and behaviors of the public and stakeholders toward the law (Darmika, 2016; Rumengan et al., 2021), and in this context, it influences the implementation of personal data protection.

One of the primary challenges in legal culture is the low level of public awareness concerning their rights to control personal data (Putri et al., 2024). Many digital banking customers remain unaware that they have the right to request the deletion of data that is no longer relevant or has been used without their consent. For example, based on a randomized survey conducted between November and December 2024 in Batam City, it was found that 90% of digital banking service users were unaware that, upon closing their bank accounts, their data may still be stored within the bank's systems or by third-party partners—data that, under existing data protection regulations, should be eligible for deletion upon request. Meanwhile, 10% of the 170 respondents expressed uncertainty about whether their data remained stored in bank systems or by third-party processors after account closure.

Chart 1. Level of Public Awareness Regarding the Right to Be Forgotten



Source: Research Findings

The lack of public awareness is also attributed to the limited educational efforts from the government, regulatory authorities, and digital service providers regarding the procedures for exercising the right to be forgotten. At present, there are few initiatives aimed at providing easily accessible information to the public on how to request data deletion from digital banking platforms or other financial services. As a result, many consumers who fall victim to data misuse remain unaware of the legal steps they can take to have their personal information removed from digital systems. This highlights the urgent need for stronger regulation to establish a more transparent and user-friendly mechanism for data deletion that is readily accessible to users.

Ideal Regulation of the Right to Be Forgotten in Indonesia with Lessons from the EU GDPR

The Right to be Forgotten (RTBF) is a key provision under the General Data Protection Regulation (GDPR), which governs how personal data must be collected, processed, and erased. This regulation stipulates that data subjects (individuals) have the right to request the erasure of their personal data from data controllers, including online digital platforms, under certain conditions. The concept gained prominence following the 2014 judgment from the EU Court of Justice, which established a legal precedent regarding the right to data erasure (Wolford, n.d.). The RTBF was first recognized by the European Court of Justice (ECJ) in the case of *Google Spain SL v. Agencia Española de Protección de Datos (AEPD)*, 2014, where the ECJ ruled that individuals could request the deletion of search results containing personal information if such information was no longer relevant or necessary (Fabbrini & Celeste, 2020a).

The RTBF is specifically outlined in Recitals 65 and 66 and Article 17(1) of the GDPR, which states:

"1) The data subject shall have the right to obtain from the controller the erasure of personal data concerning him or her without undue delay and the controller shall have the obligation to erase personal data without undue delay where one of the following grounds applies:
(a) the personal data are no longer necessary in relation to the purposes for which they were collected or otherwise processed;
(b) the data subject withdraws consent on which the processing is based according to point (a) of Article 6(1), or point (a) of Article 9(2), and where there is no other legal ground for the processing;
(c) the data subject objects to the processing pursuant to Article 21(1) and there are no overriding legitimate grounds for the processing, or the data subject objects to the processing pursuant to Article 21(2);
(d) the personal data have been unlawfully processed;
(e) the personal data have to be erased for compliance with a legal obligation in Union or Member State law to which the controller is subject;
(f) the personal data have been collected in relation to the offer of information society services referred to in Article 8(1)."

This article implies that data subjects have the right to request that data controllers erase their personal data "without undue delay", and data controllers are obligated to comply as soon as one of the listed conditions applies, such as data no longer being necessary, withdrawal of consent, or unlawful data processing. However, the enforcement of this right must still consider specific exceptions, such as legal or public interest, making it not an absolute right. Although individuals can request deletion of outdated personal information, research by Gstrein (2020) suggests that implementation still heavily depends on technology companies, particularly electronic system providers (PSE), raising concerns about transparency and legal enforcement (Gstrein, 2020).

Under Article 17(1) GDPR, data subjects can request the erasure of their personal data from data controllers without undue delay, and controllers are obligated to act if one of six legal grounds is met (see Table 2).

Table 2. Grounds for Data Erasure Under Article 17(1) GDPR

No.	Grounds for Data Erasure	Description
1	Data No Longer Necessary for Original Purpose	Personal data must be deleted if it is no longer necessary for the original purpose for which it was collected or processed.
2	Withdrawal of Consent	If processing was based on the data subject's consent and that consent is withdrawn, the data must be deleted.
3	Objection to Processing Without Legitimate Grounds	If an individual objects to data processing and there are no overriding legitimate reasons to continue processing, the data must be erased.
4	Unlawful Processing	If data has been processed unlawfully or in violation of the GDPR, it must be erased.
5	Legal Obligation	If there is a legal obligation under EU or Member State law requiring data deletion, the organization must comply.
6	Children's Data in Information Society Services	If data was collected in the context of services aimed at children and was not collected in compliance with the GDPR, it must be erased.

Source: Article 17 GDPR

As stipulated in Article 15 GDPR, the RTBF is closely tied to individuals' rights to access their personal data. This right enables individuals to control their data, including in cases where they withdraw consent, identify inaccuracies, or find the data is being stored unnecessarily (Fabbrini & Celeste, 2020b). However, the RTBF is not absolute. If applied without limitations, it could result in the "erasure of history," a major criticism of the RTBF. Therefore, the GDPR seeks to balance individual rights with public and legal interests.

The RTBF under the GDPR may be denied in certain situations, as outlined in Article 17(3). While Articles 17(1) and 17(2) provide individuals the right to erasure, Article 17(3) specifies conditions under which controllers are not obligated to comply (see Table 3).

Table 3. Exceptions to Data Erasure Under Article 17(3) GDPR

No.	Category of Exception	Description
1	Freedom of Expression and Information	Erasure cannot be enforced if it would infringe on freedom of expression and access to information, such as in journalism, academic research, or public documentation.
2	Legal Obligations or Public Task	If data must be retained for compliance with a legal obligation or public interest task, RTBF does not apply (e.g., tax or civil registry data).
3	Public Health Interest	Personal data used for public health purposes (e.g., medical research, epidemiology, disease control) cannot be erased under RTBF.
4	Archiving, Research, or Statistics	If data is used for national archives, scientific or historical research, deletion may undermine research purposes.
5	Legal Claims and Defense	Data needed in legal disputes or investigations cannot be erased.

Source: Article 17(3) GDPR

Article 17 GDPR grants individuals the right to erasure of personal data, with additional responsibilities for data controllers if the data has been made public (Article 17(2)). However, Article 17(3) imposes critical limitations related to expression rights, legal compliance, public health, research, and legal claims—aiming to strike a balance between privacy and broader societal interests.

Beyond the GDPR provisions, the European Union has established a dedicated oversight body known as the European Data Protection Board (EDPB), formed under Article 68 GDPR, to ensure uniform application of data protection rules across the European Economic Area (EEA) (Board, 2020). The EDPB comprises representatives from national Data Protection Authorities (DPAs), the European Data Protection Supervisor (EDPS), and the European Commission as a non-voting member. It has the mandate to interpret the GDPR, issue guidelines and recommendations, and resolve disputes between national authorities (Kuner et al., 2020). A key role of the EDPB is to oversee the one-stop-shop mechanism, enabling businesses operating across multiple EU states to interact with a single lead supervisory authority (Kranenborg & Lynskey, 2016). This simplifies compliance while upholding strong personal data protection.

Under Articles 70 and 71 GDPR, the EDPB must act independently and is prohibited from accepting instructions from external parties, including governments, except as expressly allowed under the GDPR. Article 70 outlines the EDPB's tasks, including ensuring consistent GDPR application, advising the European Commission, drafting guidance on data erasure procedures (Article 17(2)), defining rules on profiling (Article 22(2)), establishing breach notification standards (Articles 33 and 34), and promoting codes of conduct and certification mechanisms. It also facilitates cooperation among DPAs by exchanging best practices and resolving conflicts under Articles 64 and 65. Furthermore, the EDPB provides assessments for third-country data adequacy decisions, ensuring GDPR compliance worldwide.

Table 4. Key Differences Between the GDPR and Indonesia's Regulation

Aspect	**EU GDPR**	**Indonesian Regulation**
Legal Basis	GDPR	PDP Law & ITE Law
Individual Rights	Individuals can request data deletion without undue delay under certain conditions	Individuals can request deletion, but often require a court order
Exceptions	Not applicable in cases of expression, law, public health, archives, or research	Not explicitly regulated in PDP or ITE Laws
Supervisory Authority	Independent body (EDPB)	No independent supervisory authority
Implementation	Can be directly enforced by data controller	Requires court ruling

Source: GDPR, PDP Law, and ITE Law

Compared to Indonesia, the GDPR offers a broader scope and clearer enforcement mechanisms. It empowers individuals with greater control over their personal data, whereas Indonesia's deletion mechanism is still judicial in nature, making it slower and less accessible. Major challenges in Indonesia include the absence of an independent data protection authority, no direct deletion mechanism, and over-reliance on lengthy legal processes.

Responding to legal challenges regarding RTBF in Indonesia requires normative, progressive, and society-centered solutions aligned with Satjipto Rahardjo's Progressive

Legal Theory, which emphasizes adaptive, justice-driven legal reform. Based on this, the following are proposed:

a. Clear Definition of RTBF

Despite RTBF recognition in Indonesia's PDP Law, ITE Law, and PP PSTE, there is no unified definition, leading to inconsistent interpretations. Regulations should provide a clear definition—aligned with Article 17 GDPR—covering consent withdrawal and harmful information erasure to ensure consistency and international compatibility.

b. Mandatory Data Erasure for PSE

Currently, PSEs in Indonesia can only delete data after court orders. A more efficient model would be administrative-based deletion requirements, with clear criteria and deadlines (e.g., 30 days), technical guidelines (soft/hard delete, anonymization), and exceptions for banking records.

c. Exceptions to RTBF

Lack of explicit RTBF exceptions in Indonesian laws may conflict with press freedom, academia, and legal obligations. Adopting GDPR Article 17(3) exceptions—expression, legal compliance, public health, archives, and legal claims—is essential to maintain a balanced framework.

d. Regulatory Harmonization

Conflicts between data protection and banking regulations (e.g., mandatory data retention) highlight the need for harmonization across PDP Law, ITE Law, PP PSTE, Banking Law, and POJK. Inter-regulator coordination is critical to ensure consistency and legal clarity for global PSEs.

e. Procedural & Technical Guidelines

Absence of standardized RTBF procedures hampers individuals' ability to execute their rights. Indonesia should establish simplified digital request portals, identity verification protocols, response time limits, and secure data deletion methods (e.g., encryption, irreversible deletion).

f. Establishing an Independent Data Protection Authority (DPA)

Indonesia lacks a central, independent body like the EDPB to enforce RTBF. A national Personal Data Protection Authority (OPDP) must be formed to regulate PSEs, including banks, handle disputes, offer a one-stop-shop system, and harmonize laws. An OPDP would allow consistent enforcement, faster resolutions, and privacy protection aligned with international standards (Khansa, 2021; Mahardika, 2021; Halbert et al., 2023; Sutarli & Kurniawan, 2023).

CONCLUSION

The weaknesses in the regulation of the right to be forgotten within digital banking transactions in Indonesia reflect a regulatory disharmony between the individual interest in protecting personal data privacy and the obligation of banking institutions to safeguard the integrity of the financial system. This imbalance arises from the coexistence of provisions under the Electronic Information and Transactions Law (UU ITE), the Personal Data Protection Law (UU PDP), and the Regulation on the Operation of Electronic Systems and Transactions (PP PSTE), which grant individuals the right to request the erasure of their personal data, while banking regulations—such as the Banking Law, the Sharia Banking Law, and Financial Services Authority Regulation No. 23/POJK.01/2019—impose mandatory data retention obligations on banks for a specified period. This legal uncertainty is further exacerbated by complex data erasure procedures that are contingent upon court determinations, thereby undermining the effective implementation of the right to be forgotten. In the context of digital banking, where transaction data are often stored in decentralized systems and utilized for audit purposes and the prevention of financial crimes, inadequately regulated data deletion may potentially disrupt the stability of the financial system.

Challenges within the legal structure and legal culture also constitute significant obstacles to the implementation of the right to be forgotten in digital banking transactions in Indonesia. Regulatory disharmony among the Financial Services Authority (OJK), Bank Indonesia (BI), and the judiciary generates legal uncertainty in customer data erasure mechanisms, particularly due to conflicts with data retention obligations imposed for audit and banking compliance purposes. Deficiencies in technological infrastructure and weaknesses in law enforcement further diminish the effectiveness of supervisory mechanisms in ensuring financial institutions' compliance with this right. Moreover, the low level of public awareness regarding personal data protection rights aggravates the challenges within legal culture, a condition compounded by the lack of adequate education and socialization by regulators and financial institutions concerning data erasure procedures.

To achieve an ideal regulatory framework for the right to be forgotten in Indonesia, lessons drawn from the European Union's General Data Protection Regulation (GDPR) are highly relevant. The GDPR provides a more flexible data erasure mechanism accompanied by clearly defined exceptions, thereby maintaining a balance between privacy rights and public interests. In contrast, the implementation of this right in Indonesia continues to face significant challenges, including regulatory disharmony, excessive reliance on judicial decisions, and the absence of an independent data protection authority. Accordingly, comprehensive legal reform is required, encompassing more precise legal definitions, explicit data erasure obligations for Electronic System Operators (PSE), and the harmonization of the PDP Law, ITE Law, and banking regulations. The establishment of an independent Personal Data Protection Authority is also a crucial measure to ensure compliance by PSEs and financial institutions. By adapting best practices from the GDPR, Indonesia may develop a more effective data protection regime that is responsive to technological developments while ensuring that individual privacy rights are respected without undermining the public interest in maintaining the security and transparency of financial transactions.

REFERENCES

Adjust. (2023). *Aplikasi bank digital semakin populer di Asia Tenggara*. Adjust Blog.

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*. *6*(3), hlm 8063-8065.

Andrianto, F. (2020). Kepastian Hukum dalam Politik Hukum di Indonesia. *Administrative Law and Governance Journal*, *3*(1), 114–123. https://doi.org/10.14710/alj.v3i1.114-123

Arifuddin, I. F., & Yusuf, H. (2024). Peran Kepolisian Dalam Penanggulangan Tindak Pidana Ekonomi Khusus Di Sektor Perbankan. *Jurnal Intelek Insan Cendikia*, *1*(9), 5398–5413.

Asma Jabeen Khan, Shahzada Aamir Mushtaq, Muhammad Ali Siddique, & Muhammad Abdul Wadood. (2025). The Right to be forgotten in the Digital Age: A Pakistani Perspective on Balancing Data Protection & Privacy, Freedom of Expression, and Cyber Security. *Journal for Social Science Archives*, *3*(1), 387–403. https://doi.org/10.59075/jssa.v3i1.126

Board, E. D. P. (2020). *Guidelines 05/2020 on Consent under Regulation 2016/679 (GDPR)*.

Bode, L., & Jones, M. L. (2017). Ready to forget: American attitudes toward the right to be forgotten. *The Information Society*, *33*(2), 76–85. https://doi.org/10.1080/01972243.2016.1271071

Chaniago, N., & Sari, R. R. (2023). Determinan Yang Mempengaruhi Nasabah Bank Syariah Indonesia Dalam Penggunaan Internet Banking. *Ekonomi Digital*, *1*(2), 103–110. https://doi.org/10.55837/ed.v1i2.29

Chauhan, S., Akhtar, A., & Gupta, A. (2022). Customer experience in digital banking: A review and future research directions. *International Journal of Quality and Service Sciences*, *14*(2), 311-348. https://doi.org/10.1108/IJQSS-02-2021-0027

Darmika, I. (2016). Budaya Hukum (Legal Culture) Dan Pengaruhnya Terhadap Penegakan Hukum Di Indonesia. *Jurnal To-Ra*, *2*(3), 429–436.

Dian Sudiantini, Aura Naiwasha, Auranisa Izzati, Avrilia Ayunia W, Brilian Putri A, & Cindy Rindiani. (2023). Penggunaan Teknologi Pada Manajemen Sumber Daya Manusia Di Dalam Era Digital Sekarang. *Digital Bisnis: Jurnal Publikasi Ilmu Manajemen Dan E-Commerce*, *2*(2), 262–269. https://doi.org/10.30640/digital.v2i2.1082

Disemadi, H. S. (2022). Lenses of Legal Research: A Descriptive Essay on Legal Research Methodologies. *Journal of Judicial Review*, *24*(2), 289–304. https://doi.org/10.37253/jjr.v24i2.7280

Fabbrini, F., & Celeste, E. (2020a). The Right to Be Forgotten in the Digital Age: The Challenges of Data Protection Beyond Borders. *German Law Journal*, *21*(S1), 55–65. https://doi.org/10.1017/glj.2020.14

Fabbrini, F., & Celeste, E. (2020b). The Right to Be Forgotten in The Digital Age: The Challenges of Data Protection Beyond Borders. *German Law Journal*, *21*(S1), 55–65. https://doi.org/10.1017/glj.2020.14

Farhan, F., Hamdani, F., Astuti, N. L. V. P., Haekal Fiqry, H. A., & Aulia, M. R. (2022). Reformasi hukum perlindungan data pribadi korban pinjaman online (perbandingan Uni Eropa dan Malaysia). *Indonesia Berdaya*, *3*(3), 567–576. https://doi.org/10.47679/ib.2022264

Gstrein, O. J. (2020). Right to be forgotten: european data imperialism, national privilege, or universal human right? *Review of European Administrative Law*, *13*(1), 125–152. https://doi.org/10.7590/187479820X15881424928426

Halbert, G., Rusdiana, S., & Hutauruk, R. H. (2023). Urgensi Keberadaan Otoritas Pengawasan Independen Terhadap Harmonisasi Hukum Perlindungan Data Pribadi Di Indonesia. *Jurnal Hukum To-Ra : Hukum Untuk Mengatur Dan Melindungi Masyarakat*, *9*(3), 304–321. https://doi.org/10.55809/tora.v9i3.275

Harahap, D., Afandi, A., & Siregar, T. M. (2023). THE ISLAMIC BANKING CUSTOMERS' INTENTION TO USE DIGITAL BANKING SERVICES: AN INDONESIAN STUDY. *Journal of Islamic Monetary Economics and Finance*, *9*(3), 533–558. https://doi.org/10.21098/jimf.v9i3.1673

Hutomo, P., & Soge, M. M. (2021). Perspektif Teori Sistem Hukum Dalam Pembaharuan Pengaturan Sistem Pemasyarakatan Militer. *Legacy: Jurnal Hukum Dan Perundang-Undangan*, *1*(1), 46–68.

Isnugraheny, R. F., Megawati, Z. E., & Susilawati, S. (2024). Optimalisasi Prinsip Kerahasiaan Data Nasabah dan Peranan Otoritas Jasa Keuangan Dalam Mencegah Kebocoran Informasi. *Media Hukum Indonesia*, *2*(4), 258–264. https://doi.org/10.5281/zenodo.14181761

Jameaba, M. (2024). Digitalization, Emerging Technologies, and Financial Stability: Challenges and Opportunities for the Indonesian Banking Sector and Beyond. *SSRN Electronic Journal*. https://doi.org/10.2139/ssrn.4808469

Khansa, F. N. (2021). Penguatan Hukum dan Urgensi Otoritas Pengawas Independen dalam Pelindungan Data Pribadi di Indonesia. *Jurnal Hukum Lex Generalis*, *2*(8), 649–662. https://doi.org/10.56370/jhlg.v2i8.114

Kranenborg, H., & Lynskey, O. (2016). The Foundations of EU Data Protection Law. *International Data Privacy Law*, *6*(4), 324–326. https://doi.org/10.1093/idpl/ipw017

Kuner, C., Bygrave, L. A., Docksey, C., & Drechsler, L. (2020). *The EU General Data Protection Regulation (GDPR): A Commentary*. Oxford University Press. https://doi.org/10.1093/oso/9780198826491.001.0001

Lie, G., Ramadhan, D. A., & Redi, A. (2023). KOMISI INDEPENDEN PERLINDUNGAN DATA PRIBADI: QUASI PERADILAN DAN UPAYA TERCIPTANYA RIGHT TO BE FORGOTTEN DI INDONESIA. *Jurnal Yudisial*, *15*(2), 227. https://doi.org/10.29123/jy.v15i2.530

Liu, F., & Liu, H. (2025). Subgraph Federated Unlearning. *THE WEB CONFERENCE 2025*.

Mahardika, A. M. (2021). DESAIN IDEAL PEMBENTUKAN OTORITAS INDEPENDEN PERLINDUNGAN DATA PRIBADI DALAM SISTEM KETATANEGARAAN INDONESIA. *Jurnal Hukum*, *37*(2), 101. https://doi.org/10.26532/jh.v37i2.16994

Mutiara, U., & Maulana, R. (2020). Perlindungan Data Pribadi sebagai Bagian dari Hak Asasi Manusia atas Perlindungan Diri Pribadi. *Indonesian Journal of Law and Policy Studies*, *1*(1), 49. https://doi.org/10.31000/ijlp.v1i1.2648

Muttaqin, F. A., & Saputra, W. (2019). Budaya Hukum Malu Sebagai Nilai Vital Terwujudnya Kesadaran Hukum Masyarakat. *Al-Syakhsiyyah: Journal of Law & Family Studies*, *1*(2), 187–207. https://doi.org/10.21154/syakhsiyyah.v1i2.2026

Nirwana, D., Nurjannah, E., Marpaung, C. R. A., & Wijaya, H. A. (2024). Analisis Kebijakan Keamanan Cyber: Study Kasus Implementasi Perlindungan Data Pribadi Dalam Era Digital. *JIIP - Jurnal Ilmiah Ilmu Pendidikan*, *7*(7), 7364–7373. https://doi.org/10.54371/jiip.v7i7.4790

Njatrijani, R. (2019). Perkembangan Regulasi Dan Pengawasan Financial Technologydi Indonesia. *Diponegoro Private Law Review*, *4*, 462–474.

Nugroho, R. M., & Abdullah, M. R. (2020). *Urgency of Rights Settings to be Forgotten in Electronic Personal Information with Government Regulations*. *121*(Inclar 2019), 217–221. https://doi.org/10.2991/aebmr.k.200226.044

Odhy, F. (2021). Perspektif Budaya Hukum Dalam Perkembangan Kasus Korupsi di Indonesia. *Dharmasisya*, *1*(1), 634–646.

Pahlevi, F. (2022). Pemberantasan Korupsi di Indonesia Perspektif Legal System Lawrence M. Freidmen. *El-Dusturie*, *1*(1). https://doi.org/10.21154/eldusturie.v1i1.4097

Prastyanti, R. A., & Sharma, R. (2024). Establishing Consumer Trust Through Data Protection Law as a Competitive Advantage in Indonesia and India. *Journal of Human Rights, Culture and Legal System*, *4*(2), 354–390. https://doi.org/10.53955/jhcls.v4i2.200

Putri, A., Sari, N., Fajrina, P., & Aisyah, S. (2024). Keamanan Online dalam Media Sosial: Pentingnya Perlindungan Data Pribadi di Era Digital (Studi Kasus Desa Pematang Jering). *Jurnal Pengabdian Nasional (JPN) Indonesia*, *6*(1), 38–52. https://doi.org/10.35870/jpni.v6i1.1097

Ramadaani, K. F., & Muaalifin, M. D. A. (2023). Analisis Yuridis Pengaturan Hak Untuk Dilupakan (Right To Be Forgotten) Dalam Undang-Undang Nomor 19 Tahun 2016 Tentang Perubahan Atas Undang-Undang Nomor 11 Tahun 2008 Tentang Informasi Dan Transaksi Elektronik. *Legacy: Jurnal Hukum Dan Perundang-Undangan*, *3*(1), 18–41. https://doi.org/10.21274/legacy.2023.3.1.18-41

Ramadhani, S. A. (2022). Komparasi Perlindungan Data Pribadi di Indonesia dan Uni Eropa. *Jurnal Hukum Lex Generalis*, *3*(1), 73–84. https://doi.org/10.56370/jhlg.v3i1.173

Rumengan, C., Palandeng, E. R., & Sondakh, M. T. (2021). Budaya Hukum Yang Mempengaruhi Penanaman Modal di Indonesia. *Lex Crimen*, *10*(11).

Rusydiana, A. S., & Kanz, R. A. D. (2024). Scientometric Analysis on Digital Banking Innovation Model. *Applied Marketing and Sustainability*, *1*(1). https://doi.org/10.58968/ams.v1i1.401

Savira Nurulhaq, L., Junus, N., & Towadi, M. (2023). Juridical Review Legal Protection On The Use Of Customer Data By Bri Bank Kc Gorontalo City. *Journal Evidence Of Law*, *2*(2), 22–36. https://doi.org/10.59066/jel.v2i2.275

Setiawati, S. (2024). *Cashless Makin Digemari, Ini 5 Digital Banking Pilihan Warga RI*. CBNC Indonesia.

Setyaning Putri, A. (2023). Comparison of Right To Be Forgotten (Rtbf) Between Indonesia and Several Countries To Establising Certain Legal Data Protection in Indonesia. *Iblam Law Review*, *3*(3), 53–61. https://doi.org/10.52249/ilr.v3i3.147

Simbolon, E. D., Siregar, M., & Arifiyanto, J. (2025). Pelindungan Korban Pemalsuan Data Diri dalam Transaksi Pinjaman Online melalui Penegakan Hak untuk Dilupakan. *Neoclassical Legal Review: Journal of Law and Contemporary Issues*, *3*(2), 77–88. https://doi.org/10.32734/nlrjolci.v3i2.18351

Situmeang, A., Park, J., Sudirman, L., Silviani, N. Z., & Agustini, S. (2025). Evaluating Data Breach Notification Protocols: Comparative Analysis of Indonesia and South Korea. *Lentera Hukum*, *12*, 42. https://ejlh.unej.ac.id/index.php/ejlh/article/view/47621

Sulistyo, T. S., Utama, Y. J., & Putrijanti, A. (2024). Execution of The Right to be Forgotten in Indonesia: The Urgency of the Requirements for the Determination and Establishment of the Assessment Body. *Pena Justisia: Media Komunikasi Dan Kajian Hukum*, *23*(3), 2934–2944. https://doi.org/https://doi.org/10.31941/pj.v23i3.5596

Sudirman, L., & Disemadi, H. S. (2023). Gig Economy: Unleashing the Potential of Digital Banking in Inonesia's Employment Regulations. *Lentera Hukum*, *10*, 301. https://ejlh.unej.ac.id/index.php/ejlh/article/view/39688

Sutarli, A. F., & Kurniawan, S. (2023). Peranan Pemerintah Melalui Undang-Undang Perlindungan Data Pribadidalam Menanggulangi Phisingdi Indonesia. *Innovative: Journal Of Social Science Research*, *3*(2), 4208–4221. https://doi.org/https://j-innovative.org/index.php/Innovative/article/view/760

Syafri Hariansah. (2022). Analisis Implementasi Nilai-Nilai Budaya Hukum dalam Kehidupan Berbangsa dan Bernegara: Studi Kritis Pendekatan Masyarakat, Budaya dan Hukum. *Krtha Bhayangkara*, *16*(1), 121–130. https://doi.org/10.31599/krtha.v16i1.1000

Tan, D. (2021). Metode Penelitian Hukum: Mengupas Dan Mengulas Metodologi Dalam Menyelenggarakan Penelitian Hukum. *Nusantara: Jurnal Ilmu Pengetahuan Sosial*, *8*(8), 2463–2478. https://doi.org/10.31604/jips.v8i8.2021.2463-2478

Verheij, A. J. (2016). The right to be forgotten – a Dutch perspective. *International Review of Law, Computers \& Technology*, *30*(1–2), 32–41. https://doi.org/10.1080/13600869.2015.1125156

Wang, Q., Xu, R., He, S., Berry, R., & Zhang, M. (2025). Unlearning Incentivizes Learning under Privacy Risk. *THE WEB CONFERENCE 2025*.

Wang, W., Tian, Z., Liu, A., & Yu, S. (2025). {TAPE}: Tailored Posterior Difference for Auditing of Machine Unlearning. *THE WEB CONFERENCE 2025*.

Windani, S., & Widiani, A. (2024). IMPLIKASI HUKUM PERLINDUNGAN KONSUMEN DALAM TRANSAKSI KEUANGAN DIGITAL DAN PENINJAUAN PERATURAN PERBANKAN. *Lex Lectio Law Journal*, *03*(02), 106–117.

Wolford, B. (n.d.). *Everything you need to know about the "Right to be forgotten."* Gdpr.Eu.

Yuliana, R. A., Ningtantri, G. K., Susi, K. S., & Sugiyanto. (2024). Analisis Dampak Penggunaan E-Money, E-Wallet dan Penggunaan Atm Terhadap Perputaran Ekonomi Di Masyarakat. *HUMANITIS: Jurnal Humaniora, Sosial Dan Bisnis*, *2*(6), 582–591.

Yuspin, W., Wardiono, K., Nurrahman, A., & Budiono, A. (2023). Personal Data Protection Law in Digital Banking Governance in Indonesia. *Studia Iuridica Lublinensia*, *32*(1), 99–130. https://doi.org/10.17951/sil.2023.32.1.99-130

Zhang, H., Wu, B., Yang, X., YUAN, X., Liu, X., & Yi, X. (2025). Dynamic Graph Unlearning: A General and Efficient Post-Processing Method via Gradient Transformation. *THE WEB CONFERENCE 2025*.