SYURA: JOURNAL OF LAW
https://ejournal.staiduba.ac.id/index.php/syura
E-ISSN: 2986-5670

Regulatory Gaps in Data Protection and Proportionality in Digital Banking: Legal Issues in ASEAN

Agustianto
Universitas Internasional Batam, Indonesia
agustianto.lec@uib.ac.id

Michael T. Sacramed
Mariano Marcos State University, Philippines
mtsacramed@mmsu.edu.ph

Winda Fitri
Universitas Internasional Batam, Indonesia
winda@uib.ac.id

Nadia Carolina Weley
Universitas Internasional Batam, Indonesia
nadia.carolina@uib.ac.id

Hari Sutra Disemadi
Universitas Internasional Batam, Indonesia
hari@uib.ac.id

Keywords:
Data Proportionality, Digital Banking, Legal Gaps, Data Protection, ASEAN

Abstract

This study examines the legal gaps in regulating data proportionality in ASEAN digital banking, particularly in Indonesia, the Philippines, and Malaysia. The main legal issue lies in the absence of clear standards governing the limitation, justification, and classification of personal data, which leads to excessive and potentially invasive data processing practices in digital banking systems. This research aims to examine the concept of data proportionality in digital banking and to assess the adequacy of legal frameworks governing data proportionality in

Indonesia, the Philippines, and Malaysia in order to identify existing regulatory gaps. This study employs a normative legal research method with a comparative approach. The findings reveal that although all three countries have established data protection frameworks, none comprehensively integrate data proportionality into digital banking regulations, resulting in fragmented and ineffective legal protection. Indonesia lacks detailed standards and risk-based mechanisms, while the Philippines and Malaysia show regulatory gaps in governing conventional digital banking services. These weaknesses contribute to increased risks of privacy violations and legal uncertainty. Therefore, this study suggests the need for regulatory reform, including clearer data classification, proportionality standards, and mandatory risk assessments, to ensure a balance between digital banking innovation and the protection of consumer privacy rights.

Abstrak

Kata Kunci:
Proporsionalitas Data; Perbankan Digital; Kesenjangan Hukum; Perlindungan Data; ASEAN

Penelitian ini mengkaji kesenjangan hukum dalam pengaturan prinsip proporsionalitas data pada perbankan digital di ASEAN, khususnya di Indonesia, Filipina, dan Malaysia. Permasalahan hukum utama terletak pada belum adanya standar yang jelas terkait pembatasan, justifikasi, dan klasifikasi data pribadi, yang menyebabkan praktik pengolahan data yang berlebihan dan berpotensi melanggar privasi. Penelitian ini bertujuan untuk mengkaji konsep proporsionalitas data dalam perbankan digital serta menilai kecukupan kerangka hukum yang mengatur proporsionalitas data di Indonesia, Filipina, dan Malaysia guna mengidentifikasi kesenjangan pengaturan yang masih ada. Penelitian ini menggunakan metode penelitian hukum normatif dengan pendekatan komparatif. Hasil penelitian menunjukkan bahwa meskipun ketiga negara telah memiliki kerangka perlindungan data, belum ada integrasi yang komprehensif terhadap prinsip proporsionalitas data dalam regulasi perbankan digital. Indonesia masih lemah dalam standar dan mekanisme berbasis risiko, sementara Filipina dan Malaysia mengalami kekosongan pengaturan pada layanan perbankan digital konvensional. Kondisi ini menimbulkan risiko pelanggaran privasi dan ketidakpastian hukum. Oleh karena itu, diperlukan reformasi regulasi melalui penguatan klasifikasi data, standar proporsionalitas, serta kewajiban penilaian risiko guna mencapai keseimbangan antara inovasi perbankan digital dan perlindungan hak privasi konsumen.

Received: 18-02-2025, Revised: 10-03-2026, Accepted: 05-04-2026

Doi: https://doi.org/10.58223/syura.v4i1.811

Introduction

The rapid development of digital technology has significantly transformed various sectors, including the financial and banking industry, which is increasingly digitalized. This transformation has fundamentally changed how individuals access financial services while also introducing new legal challenges, particularly in relation to data protection and privacy. In the context of the digital economy, data has become a strategic asset with substantial value for business actors, including financial institutions. However, the extensive use of data is often not accompanied by adequate and adaptive legal regulation. This condition creates risks of data misuse and increasingly complex violations of consumer privacy rights (Agustianto et al., 2025). At the same time, regulatory developments across different countries reveal inconsistencies in governing data processing practices in digital banking. Such inconsistencies contribute to legal uncertainty and open the possibility for excessive data practices. Therefore, a legal approach required to address these problems should emphasize the protection of data while facilitating a balanced and proportional data governance in digital banking systems.

The advent of digital banking has brought fundamental changes to how people do many kinds of banking transactions (El Achari & Hattab, 2024), bringing the banking system as an indispensable part of the financial system closer to many people while also stimulating immense economic growth (Melnyk, 2024). The convenience brought by the digital technology behind digital banking is what has truly improved the accessibility of banking services (Amin, 2016). These developments are seen as beneficial for both bank consumers and perhaps even more so

for banks due to how they significantly reduce operational costs (Windasari et al., 2022). However, upon closer look, these developments do not come truly without a cost (Kiayias et al., 2022). Like other forms of digital technologies, digital banking requires a subsequent amount of data to operate smoothly and provide the relevant digital banking services (Hassani et al., 2018). The main legal issue regarding this is the risks associated with bank consumers' privacy rights and how they are, as consumers, are at risks of having their data excessively utilized by the banking sector. The principle of data proportionality plays an important role in ensuring that the financial institutions are using the least possible amount of data for digital banking purposes to operate smoothly, to lower the risks of privacy breaches without losing key capabilities of digital banking.

Recent banking trends around the globe do not only suggest the rising popularity of digital banking (Wewege et al., 2020), but also the deliberate push by the banking industry to move towards further digitalization of banking services (Kaur et al., 2021), heightening the risks of data privacy issues (Ahmed et al., 2024). Indonesia, for example, has created QRIS, which has become one of the best instruments utilized by many businesses through fintech services (Kumalasari & Pratama, 2025), supported by a great synchronization with the nation's digital banking system (Sulfaunsilah et al., 2025), with cross-border banking continues to be developed by Indonesia's central bank (Rachmalia, 2025). The Philippines and Malaysia have also benefited greatly with digital banking, with data showing digital payment transactions accounting for 52.8% of total monthly retail payments in the Philippines as of 2024, surpassing the central bank's target of 50%, while the country's six digital banks collectively serve 8.7 million depositors with deposits reaching PHP 82 billion by mid-2024 (Fintech News Philippines, 2024). In Malaysia, according to a data collected in Q4 2024, approximately 93% of consumers are reported to be

aware of digital banks, and 60% were familiar with them (Lee, 2025).

Despite these developments, the issue regarding data proportionality is not often discussed comprehensively. The emphasis on privacy in many data protection regimes often focuses mainly on security around data handling, leaving gaps in proper data classification and loose justification criteria for data collection and processing. In essence, this is deeply tied to the principle of data proportionality, which posits that the collection and processing of data should be as minimal as possible and according to the required amount needed to run a website or an application. Ultimately, the quest for an equilibrium emerges as the main goal regarding this analysis, particularly in the context of ASEAN members like Indonesia, the Philippines, and Malaysia, with their digital economies continuing to sustain economic growth and development.

The concept of privacy has been continuously developed within the legal academic sphere, with literature such as the study done by (Nissim & Wood, 2018) and another one, conducted by (Reis et al., 2024), highlighting how evolving technological and normative frameworks have shaped both the theoretical and practical challenges of privacy protection in law. One of the key theoretical frameworks of privacy rights in the digital realm today is 'privacy by design', which according to a study carried out by (Wong & Mulligan, 2019), is a proactive approach, to make occurrences of privacy harms impractical in the first place. It demands that privacy be 'built in' during the design process, embedding privacy protections into products during the initial design phase, rather than retroactively. The emphasis on design is mainly based on the fact that it is imperative to critique, speculate, or present alternatives in solving privacy rights issues when the status quo is no longer working effectively.

Another study, carried out by (Mazurek & and Małagocka, 2019),

highlighted the rapidly evolving perception of privacy in the digital landscape, from its original form as a prerequisite to enjoy other human rights such as freedom of association, expression, and choice. It also highlighted the increasingly sophisticated aggregation of data in many forms of digital technology, including key aspects of life such as financial, which has caused further concerns regarding data protection and privacy. From the context of digital banking, privacy and security are still often discussed as two aspects that cannot be separated, as noted in a study conducted by (Shukla & Puranik, 2025). This can be an oversimplification when looked at critically, as the protection of privacy rights in the banking sector or the broader financial world often involves comprehensive risk management. Data proportionality can bring significant value to this dynamic, as noted by a study carried out by (Patel, 2024), because of how it can lower the exposure accompanying data vulnerability and increases customer protection, leading to the principle of collecting the bare minimum data.

A significant legal gap can be identified from the literature review above, which is the lack of emphasis on the specific principles of data protection and privacy in the context of digital banking. Despite the extensive development of literatures around data protection and privacy, literature doesn't typically focus on a specific principle of data protection and privacy, especially not in a specific context such as digital banking. This specificity is the main novelty of this study; a critical gap authors are trying to fill. The comparison of Indonesia, the Philippines, and Malaysia adds even more novel values to this study, providing insights regarding how these ASEAN members are trying to reach legal equilibrium regarding data collection and processing. It is also important to note that the focus of digital banking in this study is narrowed to only digital banking services provided by conventional banks, not digital banks with no branch, or what are often referred to

as neobanks. Furthermore, an important limitation of this study needs to be noted, particularly regarding how it may not be able to capture the full picture of enforcement realities, as the study does not collect and utilize empirical data to focus on doctrinal comprehension and analysis of the existing frameworks. Most importantly, based on the research background and the regulatory issues discussed above, this study focuses on answering the following questions:

1) How is the principle of data proportionality conceptualized in the context of digital banking and privacy protection? 2)To what extent do the legal frameworks in Indonesia, the Philippines, and Malaysia regulate data proportionality in digital banking? 3) Are there regulatory gaps in the implementation of data proportionality in digital banking in these countries?

Method

This paper employs the normative legal research method, often also referred to as doctrinal research method, to assess the legal norms of the relevant legal frameworks (Disemadi, 2022). This typically involves a black letter law analysis, where legal norms are assessed based on how they are framed and stipulated, to then be utilized as a legal lens for a deeper analysis of a legal topic of the study (Tan, 2021). The analysis is also supported by comparative approach to ensure that the identified and analyzed primary law sources, along with the assessments made based on them, can be compared with other legal systems to identify the common denominators and key differences for more legal insights (Negara, 2023). To deepen the analysis even further, this paper supplements it with the theoretical framework for privacy by design, which has now become one of the main theoretical frameworks for data protection and data privacy analysis. This is to open ways for the critique, assessment, and even

speculate associated risks of privacy rights in the context of digital banking, which presents a high stake.

The primary law sources analyzed in this study include Indonesia's Law No. 27 of 2022 on Personal Data Protection and Financial Services Authority Regulation No. 21 of 2023 on Digital Services by Commercial Banks which formed the foundation for examining data proportionality principles in Indonesian digital banking regulation. The Philippines section examined the Data Privacy Act (RA 10173), Bangko Sentral ng Pilipinas Circular No. 1105 (2020), General Banking Law of 2000 (RA 8791), and Internet Transactions Act (RA 11967) to assess the regulatory framework governing digital banking services and data protection in Philippine financial institutions. Malaysia's regulatory analysis focused on the Personal Data Protection Act 2010 and its 2024 Amendment, Electronic Commerce Act 2008, and Financial Services Act 2013 to evaluate the country's approach to data proportionality in digital banking operations and privacy protection mechanisms.

Result and Discussion

Data Proportionality and The Legal Dynamics of Privacy Rights in Digital Banking

Data privacy is a legal field that is currently rapidly evolving as digital technologies continue to dominate many aspects of everyday life (Ruslan, 2023), directly tackling the increasing instances of data breaches and the subsequent growing risks of it (Fitri et al., 2024). From the purely legal standpoint, the conceptualization of data privacy serves as a wall of compliance against the possible breaches of the broader traditional sense of privacy rights (Nasir, 2025). However, this fundamental legal aspect is not often clear, as data privacy is often mistaken as data protection and vice versa, despite the fact that data protection often puts more emphasis on the first line of protection against cyber-related risks, aligning it more closely with the realm of cyber-security and the relevant legal risk

management (Cele & Kwenda, 2025). The importance of understanding this distinction is not about ensuring that data privacy is understood as an isolated legal issue, but rather a problem that is heavily reliant on data protection yet easily sidelined. Therefore, the legal analysis regarding the interplay between data protection and data privacy, particularly in the context of digital banking, must be done through careful analysis with a firm understanding on what aspects of data protection are directly relevant to the protection of privacy rights in the digital world.

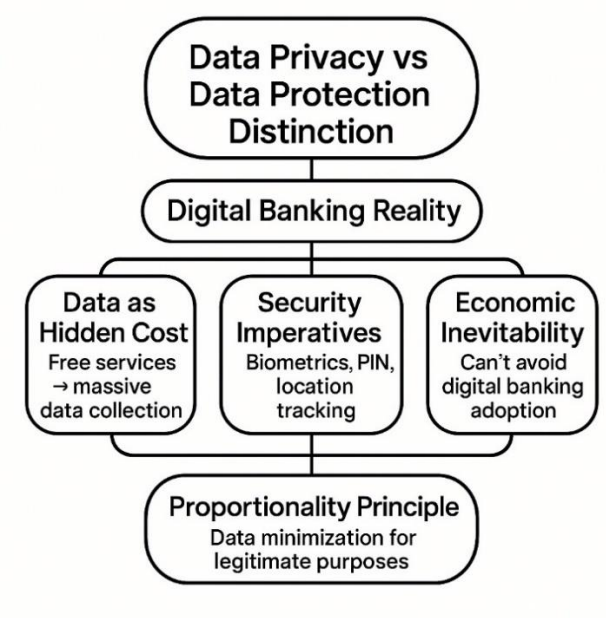
Digital banking, like other digital technologies, is developed to increase convenience and the overall productivity of those who utilize them. For this to manifest, there needs to be a certain degree of smoothness and stability to be met in the development of the relevant technologies, be it through a website or an application that is installed on a smartphone. Aside from the monetary cost of these developments, data can also be considered a cost that is actively being paid by those that use the websites or apps for digital banking services, which are often offered for free as the basic and, for some, essential feature of today's banking system. This dynamic has created the normalization of massive data collection and processing, which has raised significant risks regarding the privacy of the data subjects. Legal frameworks for data protection and privacy must carefully navigate around these complex legal terrains to reach an equilibrium resembling a balance between smooth utilization of digital banking and minimized data management risks.

The first essential feature that must exist within every single digital banking system in the world is a high level of security, to ensure that bank accounts are not accessed without legitimate authorization or even hacked directly, which can threaten an insurmountable amount of cashflow and ultimately shatter the finances of many bank consumers. For security purposes, banks are left with no choice but to collect and process a considerable amount of

data to protect their consumers' money, by developing security features such as password or PIN (Alcantara et al., 2025), biometric data like retina or fingerprints (Morake et al., 2021), or location tracking to detect suspicious activity that might have been an authorized attempt to access the consumer's finances (Fang & Quintos, 2023). However, this must be done with cautious, as it also places a bigger burden for banks to handle massive volumes of data, which can create further legal risks, especially within the context of today's privacy conscious world, where consumers demand a certain degree of transparency and accountability in data collection and processing practices from banks (Gupta & Shukla, 2024). Additionally, significant risks are also faced by data subjects, due to the catastrophic impacts that can potentially happen when these highly sensitive data are breached, often leading to significant financial loss, reputational damage, and identity theft (Situmeang, Park, et al., 2025). This, in turn, creates a significant legal risk for banks and any other firm that utilizes massive amount of data, as they are tied to legal liabilities when they fail to protect the rights of data subjects (Situmeang, Weley, et al., 2025).

Due to the significant impacts of digital banking to economic growth (Mecerhed & Guettar, 2023), it is no longer feasible to avoid or be reluctant in adopting it due to data protection and privacy concerns. Instead, countries around the world should focus on how digital banking can be utilized responsibly by adhering to the key principles of data protection and privacy. The principle of proportionality can serve as an essential part of regulating data collection and processing around digital banking, as it focuses on the minimization of data to what is necessary and adequate for the specified, explicit and legitimate purposes, ensuring that each byte of data that are processed and stored is filtered through a series of objectives and discarded if it does not fit the intended purposes (Malek, 2021). These issues are summarized into the following mind map below.

Figure 1: Mind map of the main issues that need normative attention



Source: Authors' illustration.

An idealized normative framework, in its essence, must be able to balance individual rights with the institutional responsibilities, particularly in regard to sensitive data (Librawenson et al., 2026). For this, it must fundamentally embrace the principle of Privacy by Design, to ensure that data protection considerations are embedded into the architectural foundation of all digital banking systems from their initial development processes. This principle must be embedded within the digital banking infrastructure regardless of the existing intertwined challenges associated with it, namely as the balancing between operational efficiency, regulatory compliance, and the protection of sensitive consumer data (Andrade et al., 2022). This approach requires financial institutions to conduct comprehensive Privacy Impact Assessments during the design phase of any new digital service by implementing technical and organizational measures to carefully minimize data collection to only what is strictly necessary for legitimate banking purposes, without damaging functional capabilities of the digital banking platform. The framework should mandate that privacy-enhancing technologies, such as differential privacy, homomorphic encryption, and secure multiparty computation, become standard components of digital banking infrastructure, enabling institutions to derive necessary insights while preserving individual privacy.

The normative framework must also establish clear data governance hierarchies that prioritize consumer

autonomy and informed consent while recognizing the practical realities of modern banking operations (Ruslan, 2023). Financial institutions should be required to maintain transparent data inventories and processing maps, enabling both regulators and consumers to understand the full scope of data collection and usage. For this to be applied effectively, there is also a serious need to supplement data protection and privacy framework to have a sophisticated data classification to ensure that data are handled separately according to each of their associated risks. This can enhance the standard of quality in Privacy Impact Assessments, as it maps out the detailed aspects of data collection and mechanisms in a way that does not require extensive knowledge regarding data management from consumers, which in turn can enhance overall transparency and accountability.

A comprehensive normative approach must also integrate ethical data stewardship by requiring financial institutions behind digital banking services to implement algorithmic accountability measures, ensuring that automated decision-making systems used in digital banking are transparent and fair (Zainal, 2023), and most importantly, subject to human oversight. Human oversight plays perhaps the most critical part in this interplay, particularly within the context of increasingly utilized advanced technology like Artificial Intelligence (AI), as data interpretation and the decision making associated with it may be affected by certain biases (Agustiawan, 2024; Union et al., 2024). A critical point that needs to be covered normatively regarding this is how the data proportionality principle can be applied to the processes of data aggregation, which would benefit from a sophisticated data classification to clearly separate it as non-personal data (Onik et al., 2019). Application of this principle should be present in the development of the algorithm itself and in the creation of new data from the aggregation processes to ensure that data collection and processing within

the context of algorithm processing remains rigorously documented for accountability purposes. This should also be supported by anonymization to open ways for data utilization without breaching the privacy rights of bank consumers as data subjects, providing a middle ground for data protection and data utilization.

Furthermore, in the case that digital banking services operate outside of the national border, there should also be a safeguard installed to guarantee that consumers data are not easily collected and processed without concrete partnerships between the relevant financial institutions and state actors involved. This includes developing harmonized regulatory standards that facilitate innovation while ensuring consistent privacy protections across different jurisdictions. Most importantly, the principle of data proportionality should continue to be upheld in the relevant partnerships. Throughout all of the elements above, bank consumers should also be educated properly by being given relevant, easy-to-digest information regarding their data-related rights and how their data are being processed, along with what they should consider in their decision-making process of giving consent to data collection and processing mechanisms for digital banking purposes.

Legal challenges associated with data protection and digital banking

While data proportionality has been previously highlighted as a significant principle in data collection and processing in today's digital banking dynamics, it is not a concept that can easily fix the existing challenges that are inherent with digital technologies in general, which are then further accentuated with the sensitive nature of digital banking. Below is the mind map elaborating the challenges associated with data protection and digital banking, which are all important to be identified to ensure that the idealized framework remains grounded in the reality of highly sensitive legal implications in digital banking today.

Figure 2. Legal Challenges in Data Protection and Digital Banking

Source: Authors' illustration.

Digital banking has become a central component of modern financial systems, driven by rapid technological advancements and the increasing integration of digital technologies into everyday transactions. This transformation enhances accessibility, efficiency, and convenience for users, but it also intensifies the reliance on data as a fundamental operational resource. In this context, data is no longer merely a supporting element but has evolved into a strategic asset for financial institutions. However, the extensive use and processing of data inevitably raise significant concerns regarding privacy and data protection. As digital banking systems continue to expand, the balance between innovation and the protection of consumer rights becomes increasingly complex. These dynamics underscore the importance of legal frameworks that can address both technological developments and emerging risks. Without adequate regulation, the rapid growth of digital banking may lead to unintended legal consequences. Therefore, understanding the legal implications of data use in digital banking is essential in ensuring sustainable and responsible financial innovation.

The growing dependence on data in digital banking has led to the normalization of extensive data collection and processing practices. Financial institutions often rely on various forms of personal data, including biometric and behavioural information, to enhance security and service efficiency. While these practices may improve user experience and system reliability, they simultaneously increase the risk of privacy violations and data misuse. The principle of data proportionality emerges as a crucial legal concept to address this issue, emphasizing that only necessary and relevant data

should be collected and processed. Despite its importance, the application of this principle remains inconsistent across different jurisdictions. In many cases, legal frameworks focus primarily on data security rather than limiting the scope of data collection. This imbalance creates vulnerabilities in protecting consumer privacy rights, which is further exacerbated by the asymmetrical knowledge regarding the implications of data collection and processing between consumers as data subjects and banks that utilize those data.

Regulatory gaps represent one of the most critical challenges in governing digital banking systems, particularly in ASEAN countries such as Indonesia, the Philippines, and Malaysia. Although these countries have established legal frameworks for data protection, significant inconsistencies and limitations persist in their implementation. In Indonesia, the lack of detailed standards and risk-based mechanisms weakens the effectiveness of data proportionality principles. In the Philippines, the absence of comprehensive regulations for conventional digital banking services creates a fragmented legal landscape. Meanwhile, Malaysia faces challenges due to outdated legal provisions that do not fully accommodate the realities of digital banking. These inconsistencies contribute to legal uncertainty and hinder the development of a coherent regulatory approach. Furthermore, the lack of clear guidelines on data classification and justification criteria exacerbates the problem. As a result, financial institutions may engage in excessive data practices without sufficient legal accountability. Addressing these regulatory gaps is essential to ensure a more consistent and effective legal framework.

The existence of legal challenges in digital banking highlights the need for a more balanced and integrated regulatory approach. Issues such as data misuse, consumer privacy violations, and inadequate legal safeguards demonstrate the limitations of current legal

frameworks. These challenges are further compounded by the rapid evolution of technology, which often outpaces regulatory developments. To address these issues, it is necessary to adopt a more comprehensive legal perspective that incorporates principles such as data proportionality, risk-based assessment, and privacy by design. Such an approach would enable regulators to better manage the complexities of digital banking while ensuring the protection of consumer rights. Additionally, strengthening transparency and accountability mechanisms can help build trust between financial institutions and consumers. Ultimately, achieving a balance between innovation and regulation is key to the sustainable development of digital banking. This balance will ensure that technological progress does not come at the expense of fundamental legal protections.

Not only that, the subsequent idealized framework previously conceptualized to ensure the application of data proportionality should also realistically align with these identified challenges, particularly because the increasing reliance on biometric authentication, automated profiling, cross-border data flows, and extensive data aggregation in digital banking may generate privacy risks that cannot be adequately addressed through a purely formal proportionality standard. Therefore, the normative analysis should take into account the extent to which each jurisdiction translates proportionality into operational safeguards, including clearer data classification, mandatory impact assessments, and risk-based compliance obligations, so that the proposed framework remains theoretically coherent and institutionally workable within the regulatory realities of digital banking.

Assessment of legal frameworks for data protection and privacy in digital banking

Data protection and privacy have been developed in many countries as a response to the growing concerns regarding digital issues such as cybersecurity and the

threat of cybercrimes. Over time, the narrative around legal developments for data protection and privacy becomes more nuanced, as concerns are also raised from the more privacy-centric perspective, especially with the development and utilization of Big Data and IoT, which has unlocked an accelerated speed of development for many digital technologies (Cifaldi, 2023). In the context of digital banking, this shift is also identified, as there is a strong emphasis on protection of data against external, cyber-related threats, as a broader part of data protection. Now, concerns have also been raised about data management practices of financial institutions, as consumers are increasingly aware of their privacy rights in the digital world. This development still goes hand-in-hand with the initial focus on protection against cyber-related threats, as the principle of data proportionality bridges the broader data protection concept with data privacy, through data minimization and its impacts on risks assessment.

In Indonesia, the main framework for data protection is Law No. 27 of 2022 on Personal Data Protection (PDP Law) (Romadiah et al., 2025), which was enacted after years of developing legal frameworks regarding the digital world (Bimantara et al., 2024). The PDP Law defines data protection as the "*the overall effort to protect Personal Data in the course of processing Personal Data in order to guarantee the constitutional rights of Personal Data subjects.*" Normatively, the principle of data proportionality is partially manifested in Article 27, which governs that data processing should be 'limited' in nature. This is further supported by Article 28, which reflects a certain degree of purpose limitations. However, these two frameworks did not reflect the full picture of data proportionality, as it would involve concrete elaboration on what 'limited' means, supported with standards or criteria for what can be deemed as 'justified' purposes, as an essential support of purpose limitations. Most importantly, the PDP Law, as governed in Article 4,

has a binary classification: specific and general personal data. This overly simplistic data classification can significantly impede the effectiveness of data proportionality principle, even if Article 27 and Article 28 were far more comprehensive.

These normative gaps also directly translate into the lack of risk-based assessment mechanism for data management processes, which is significantly relevant in the case of digital banking. As Privacy Impact Assessment requires all the normative elements that the PDP Law lacks, creating such mechanism would effectively require a drastic set of changes to the gaps that exist within the PDP Law, particularly regarding the lack of emphasis on data proportionality. In turn, this creates a significant practical implementation gap as financial institutions are left to operate in way that either overexploits personal data for the sake of digital banking-related services, or overprotects personal data, which impedes the smoothness and overall utilization of the digital banking platform.

From the banking perspective, Indonesia has a web of regulations that govern many aspects of fintech, including digital banking. However, Financial Services Authority Regulation No. 21 of 2023 on Digital Services by Commercial Banks (POJK/21/2023) is perhaps the most relevant one to be analyzed, due to its specific objective of regulating digital banking (Sudarso & Yusuf, 2024). The regulation is directly tied to the legal framework for data protection, as stipulated in Article 29(1): *"Banks operating Digital Services are obligated to implement personal data protection principles in conducting personal data processing in accordance with statutory provisions regarding personal data protection."* However, as identified previously, the lack of emphasis on data proportionality in the PDP Law makes this provision ineffective in addressing the need to lower the risks associated with data management. This problem is also further manifested in Article 21, which details the key principles needed to

be applied, without mentioning data proportionality.

The biggest gap found in this regulation is the provision of Article 15, which allows banks to share personal data of their consumers with a third party if they have the required three aspects: consent, consumer benefit justification, and compliance with data protection laws. As the regulation has zero elaboration on the limits of 'consumer benefit justification', the overall use of this provision can become arbitrary and open the doors for invasive data management practices among banks. While an argument can be made that consumers are made aware with informed consent, this is not in line with the theoretical framework of Privacy by Design, as it requires extensive knowledge on data-related issues and risks on the consumer side, allowing banks to exploit knowledge gaps that exist among their consumers. As elaborated previously, this does not only harm the consumer, as it can simultaneously increase the legal risks faced by banks, in the face of countless, constantly evolving threats of cybercrime.

The Philippines, on the other hand, relies on Data Privacy Act (RA 10173) as its main framework for data protection and privacy (Ching et al., 2018). Contrasting Indonesia's PDP Law, the Data Privacy Act explicitly mentions data proportionality in Section 11, which mentions three key principles: transparency, legitimate purpose, and proportionality. Unfortunately, the Data Privacy Act also has a binary system of data classification, with only general personal information as described in Section 3(g) and sensitive personal information as described in Section 3(l). Even more concerning is that financial data is not described as a part of sensitive personal information in Section 3(l), which effectively renders the other provisions ineffective, as financial institutions such as banks are not required to comply with the data protection in the case of financial information. While the Philippines DPA acknowledges existing financial sector laws like the Bank Deposit

Secrecy Act, Credit Information System Act, and Anti-Money Laundering Act in Section 4(e)-(f), these exemptions only cover narrow regulatory compliance activities rather than comprehensive digital banking operations. Despite this fragmented legal framework, the DPA itself fails to classify financial data as sensitive personal information, creating inconsistent protection where tax returns receive stronger safeguards than real-time transaction patterns or behavioral analytics commonly processed in digital banking platforms.

The fact that financial data is not expressly classified as sensitive personal information under the DPA does not, in itself, exclude banks from data protection obligations, as the DPA operates alongside sector-specific regimes such as bank secrecy and anti-money laundering laws, which permit data processing and disclosure for limited regulatory and compliance purposes. However, digital banking practices extend beyond traditional banking records and increasingly involve the collection of device identifiers, login metadata, behavioral analytics, geolocation data, and transaction-pattern profiling (Găbudeanu et al., 2021). These categories of data do not fall squarely within the conventional scope of bank secrecy or AML compliance, yet they remain highly privacy intrusive. Seen from this perspective, this creates another layer of regulatory gap, where certain forms of digital-banking data are neither clearly classified as sensitive personal data nor fully addressed by sector-specific banking regulations. Consequently, this reinforces the need for a comprehensive application of the proportionality principle, because of how it can act as an anchor that ties data to its collection and processing purposes, as specified strictly by the relevant consent forms.

The Philippines regulates some aspects of digital banking services through *Bangko Sentral ng Pilipinas* Circular No. 1105 (2020). However, this regulation only applies to digital banks with no physical branch, despite its important provisions, such as the one in in Section 102(c), which

governs risk management in the context of technology and cyber security. The Philippines does have its main framework for banking, which is the General Banking Law of 2000 (RA 8791), but in the context of digital banking the law only spells the authority of the Bangko Sentral (Philippine Central Bank) to regulate it, which to this day, still has no concrete manifestation. Even in the more recent Internet Transactions Act (RA 11967), there is no provision regarding banking transactions, further conclusively showing that this is indeed a normative gap that has long been unaddressed in the Philippines.

For Malaysia, the data protection and privacy legal landscape has recently received new updates, with the enactment of the Personal Data Protection Act (Amendment) 2024, bringing key changes to the framework's previous 2010 version (Ab Rahim & Ab Rahman, 2025). This framework applies the principle of data proportionality directly into Section 6(3), by stipulating that personal data that are processed have to be *"adequate but not excessive in relation to that purpose."* This application of the data proportionality principle is further supplemented by Section 10 which governs storage limitation, mandating the deletion of data that are no longer in use. However, the PDPA framework also suffers from a simplistic binary classification as provisioned in Section 4, with no further risk-based divergent protection mechanisms and no mention of financial data as a part of the 'sensitive' categorization.

For specifically the banking contexts, Malaysia refers to an older regulation, which is Electronic Commerce Act 2008, which explicitly mentioned banking as part of its broader definition of 'commercial transactions' in Section 5. This support is further elaborated in the Financial Services Act 2013, albeit limited. Section 134 stipulates that, *"Nothing in section 133 (prohibition of unauthorized access to data) shall prohibit the disclosure of any customer information by any person... (f) where the disclosure is for such other purposes as*

may be prescribed by the Bank." This only partly covers the principle of data proportionality, as it governs the strict adherence to disclosure terms, but without any mechanism to justify those terms, especially in divergent use cases for digital banking purposes. This issue is rooted in Section 133, which governs many kinds of data that should be protected, with examples given focusing on physical documents and no mention of any electronic formats. This framework remains archaic in nature and only touches on a small portion of data protection and privacy conceptualization, with even basic norms such as transparency and consent remain unaddressed.

To assess whether data proportionality has been comprehensively integrated into digital banking regulations, this study applies several analytical criteria. These include the existence of a legal definition or standard of proportionality, the presence of a data classification system based on risk levels, the requirement to conduct Data Protection Impact Assessments (DPIA) or Privacy Impact Assessments (PIA), the existence of risk-based regulatory or enforcement mechanisms, and the presence of sector-specific rules governing digital banking. These criteria are used as indicators to evaluate and compare the legal frameworks of Indonesia, the Philippines, and Malaysia. The comparative outlook based on these criteria is presented in Table 1 below.

Table 1. Comparative Outlook of the Identified Normative Gaps

Criteria	**Indonesia**	**Philippines**	**Malaysia**
Legal definition of proportionality	Partial	Yes	Yes
Data classification system	Basic	Basic	Basic
Mandatory DPIA/PIA	No	Partial	Partial
Risk-based	No	Limited	Limited

mechanism			
Digital banking specific rules	Yes	Limited	Limited
Level of integration	Low	Medium	Medium

Source: Authors' analysis

As shown in Table 1, none of the three countries fully satisfy all of the criteria for comprehensive integration of data proportionality in digital banking regulations. While the Philippines and Malaysia demonstrate a moderate level of integration due to the presence of general proportionality principles and partial DPIA requirements, Indonesia shows a lower level of integration, particularly due to the absence of mandatory impact assessments and risk-based regulatory mechanisms. Furthermore, although Indonesia has specific regulations related to digital banking, these regulations do not yet clearly incorporate risk-based data proportionality standards. From this comparative outlook, it is evident that Indonesia is the most behind when it comes to capturing these issues, which positions the country's banking industry to face significant uncertainty. While it can be argued that the lack of enforcement leaves firms with less compliance pressure, the long-term legal risk management might present a different picture. With the continued reliance on data, more concerns around data in fintech will be raised and to close the already wide regulatory lag, Indonesian banks might be looking at an overhaul of previous regulatory approach regarding this issue, which in the end will put significant pressure for the banks to comply. On the other hand, while the legal liability risks still exist (Anggriani et al., 2026), banks that operate under a legal system with a more developed legal frameworks around this issue, such is the case with Malaysia and the Philippines, will face a more predictable legal risks in the short-term or long-term.

Conclusion

From the analysis through this study, it is apparent that the principle of data proportionality has not yet been applied comprehensively in all the three countries analyzed. Indonesia, despite being the only country with a dedicated framework for conventional bank's digital banking services, falls short in acknowledging the importance of risk minimization as its PDP framework and its digital banking framework also lack synchronization in the context of data protection and privacy. The Philippines, on the other hand, is the only country in comparison that directly addresses the principle of data proportionality but lacks data provisions in the context of digital banking services provided by conventional banks. Malaysia has adequate manifestations of data proportionality principles but unfortunately also suffers from the same problem as the Philippines regarding the lack of data provisions for conventional bank's digital services. All three countries also have the same, oversimplistic data classification, which can present further normative issues for the real application of data proportionality in the future.

It is advised that the countries implement key changes to their legal frameworks regarding data privacy and digital banking services. Enhancement of data classification, mandatory privacy impact assessments, and divergent risk-based data handling requirements should be the prioritized normative aspects to be added. For the specific case of Indonesia, the proper integration of data proportionality principles remains the issue with utmost urgency, as the other two countries have adequately integrated this principle in their foundational data protection and privacy framework. Ultimately, findings of this study can serve as insights to be considered for future legal developments of the banking sector in an ever-so-digitalized world, to reach an equilibrium between digital banking utility and data privacy protection.

References

Ab Rahim, S. F., & Ab Rahman, M. F. (2025). To Share or Not to Share Patient Health Data Without Consent for Public Interest Purposes: A Critical Comparative Analysis of EU GDPR 2018 and Malaysia PDPA 2010. *Akademika*, *95*(01), 391–408. https://doi.org/10.17576/akad-2025-9501-22

Agustianto, A., Sohheng, N., Sudirman, L., Seroja, T. D., & Nurlaily, N. (2025). Consumer Privacy and Data Tracking in the Digital Economy: Legal Frameworks and Future Challenges in Indonesia and Thailand. *Kosmik Hukum*, *25*(3), 573–588. https://doi.org/10.30595/kosmikhukum.v25i3.25948

Agustiawan, D. A. (2024). Digital Banking Transformation AI Enhances Efficiency And Customer Experience Seminar Perspective Industry. *WACANA: Jurnal Ilmiah Ilmu Komunikasi*, *23*(1), 191–200. https://doi.org/10.32509/wacana.v23i1.4130

Ahmed, F., Hussain, A., Khan, S. N., Malik, A. H., Asim, M., Ahmad, S., & El-Affendi, M. (2024). Digital Risk and Financial Inclusion: Balance between Auxiliary Innovation and Protecting Digital Banking Customers. *Risks*, *12*(8), 1–21. https://doi.org/10.3390/risks12080133

Alcantara, Y. F. B., Casas, C. B., Dela Torre, R. D., & Flores, G. C. (2025). Security and Vulnerability: Using One-Time Pin to Access Data for Online Transactions. *Multidisciplinary International Journal of Research and Development*, *4*(3), 167–181.

Amin, M. (2016). Internet banking service quality and its implication on e-customer satisfaction and e-customer loyalty. *International Journal of Bank Marketing*, *34*(3), 280–306. https://doi.org/10.1108/IJBM-10-2014-0139

Andrade, V. C., Gomes, R. D.,

Reinehr, S., Freitas, C. O. D. A., & Malucelli, A. (2022). Privacy by Design and Software Engineering. *Proceedings of the XXI Brazilian Symposium on Software Quality*, 1–10. https://doi.org/10.1145/3571473.3571480

Anggriani, D., Febriyani, E., & Situmeang, A. (2026). Pertanggungjawaban Pidana Korporasi Atas Kebocoran Data Pribadi di Indonesia: Studi Komparatif dengan Amerika Serikat dan Uni Eropa. *Jurnal Fundamental Justice*, *7*(1), 127–146. https://doi.org/10.30812/fundamental.v7i1.6237

Bimantara, G., Handayani, T. A., & Al Irsyad, M. A. Y. (2024). The Corporate Legal Responsibility for The Leak of Personal Data of Application Consumers in Indonesia. *Jurnal Akta*, *11*(4), 1213–1221. https://doi.org/10.30659/akta.v11i4.41409

Cele, N. N., & Kwenda, S. (2025). Do cybersecurity threats and risks have an impact on the adoption of digital banking? A systematic literature review. *Journal of Financial Crime*, *32*(1), 31–48. https://doi.org/10.1108/JFC-10-2023-0263

Ching, M. R. D., Fabito, B. S., & Celis, N. J. (2018). Data Privacy Act of 2012: A Case Study Approach to Philippine Government Agencies Compliance. *Advanced Science Letters*, *24*(10), 7042–7046. https://doi.org/10.1166/asl.2018.12404

Cifaldi, G. (2023). Evolution of Concepts of Privacy and Personal Data Protection under the Influence of Information Technology Development. *Sociology and Social Work Review*, *7*(1), 35–60. https://doi.org/10.58179/sswr7103

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.v2

4i2.7280

El Achari, S., & Hattab, S. (2024). L'impact de la transformation digitale sur le secteur bancaire. *Journal of Economics, Finance and Management (JEFM)*, *3*(3), 873–886. https://doi.org/10.5281/zenodo.12723055

Fang, L., & Quintos, D. G. (2023). Security Measures Applied on Digital Banking Towards Service Improvement Proposal. *Journal of Business and Management Studies*, *5*(5), 47–77. https://doi.org/10.32996/jbms.2023.5.5.5

Fintech News Philippines. (2024, November). *5 Key Highlights from the Philippines Fintech Report 2024*. Fintech News Philippines.

Fitri, W., Disemadi, H. S., & Rindiyani, M. (2024). Data Leakage of Consumer Personal Data in Telecommunications Services Customer Registration: Who Is Responsible? *Yustisia Tirtayasa: Jurnal Tugas Akhir*, *4*(1), 98–112. https://doi.org/10.51825/yta.v4i1.22518

Fitzgerald, E., Pioro, M., & Tomaszwski, A. (2018). Energy-Optimal Data Aggregation and Dissemination for the Internet of Things. *IEEE Internet of Things Journal*, *5*(2), 955–969. https://doi.org/10.1109/JIOT.2018.2803792

Găbudeanu, L., Brici, I., Mare, C., Mihai, I. C., & Şcheau, M. C. (2021). Privacy Intrusiveness in Financial-Banking Fraud Detection. *Risks*, *9*(6), 1–22. https://doi.org/10.3390/risks9060104

Gupta, V., & Shukla, S. (2024). Consumer Trust in Digital Banking: A Qualitative Study of Legal and Regulatory Impacts. *Interdisciplinary Studies in Society, Law, and Politics*, *3*(2), 18–24. https://doi.org/10.61838/kman.isslp.3.2.4

Hassani, H., Huang, X., & Silva, E. (2018). Digitalisation and Big Data Mining in Banking. *Big Data and Cognitive Computing*, *2*(3), 1–13.

https://doi.org/10.3390/bdcc2030018

Kaur, S. J., Ali, L., Hassan, M. K., & Al-Emran, M. (2021). Adoption of digital banking channels in an emerging economy: exploring the role of in-branch efforts. *Journal of Financial Services Marketing*, *26*(2), 107–121. https://doi.org/10.1057/s41264-020-00082-w

Kiayias, A., Kohlweiss, M., & Sarencheh, A. (2022). PEReDi: Privacy-Enhanced, Regulated and Distributed Central Bank Digital Currencies. *Proceedings of the 2022 ACM SIGSAC Conference on Computer and Communications Security*, 1739–1752. https://doi.org/10.1145/3548606.3560707

Kumalasari, E. N., & Pratama, P. A. (2025). Analysis of the Role of Increasing Financial Inclusion Through Digital Transformation on the Stability of the Financial System in Indonesia. *Journal of Accounting, Finance, and FinTech Advancements*, *1*(2), 55–69.

Lee, V. (2025, May). *Beyond Cash: Growth of E-Wallets and Digital Banks in Malaysia [Infographic] – Progressive Market Research Company In Malaysia*. Oppotus.

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

Malek, A. (2021). Bigger is always not better; less is more, sometimes: the concept of data minimization in the context of Big Data. *European Journal of Privacy Law and Technologies*, *2021*(1), 212–223.

Mazurek, G., & and Małagocka, K. (2019). Perception of privacy and data protection in the context of the development of artificial intelligence. *Journal of Management Analytics*, *6*(4), 344–364.

https://doi.org/10.1080/23270012.2019.1671243

Mecerhed, B., & Guettar, F. Z. (2023). The Impact of Digital Transformation in Banks on Economic Growth: A Study of a Sample of Countries from 2012 to 2021. *The Journal of Contemporary Issues in Business and Government*, *29*(4), 248–262.

Melnyk, V. (2024). Transforming the nature of trust between banks and young clients: from traditional to digital banking. *Qualitative Research in Financial Markets*, *16*(4), 618–635. https://doi.org/10.1108/QRFM-08-2022-0129

Morake, A., Khoza, L. T., & Bokaba, T. (2021). Biometric technology in banking institutions: 'The customers' perspectives'. *SA Journal of Information Management*, *23*(1), 1–9. https://doi.org/10.4102/sajim.v23i1.1407

Nasir, K. (2025). The Evolution of Privacy Laws in the Digital Age. *International Journal of African Sustainable Development Research*, *7*(2), 269–278. https://doi.org/10.70382/tijasdr.v07i2.033

Negara, T. A. S. (2023). Normative Legal Research in Indonesia: Its Originis and Approaches. *Audito Comparative Law Journal (ACLJ)*, *4*(1), 1–9. https://doi.org/10.22219/aclj.v4i1.24855

Nissim, K., & Wood, A. (2018). Is privacy privacy? *Philosophical Transactions of the Royal Society A: Mathematical, Physical and Engineering Sciences*, *376*(2128), 1–17. https://doi.org/10.1098/rsta.2017.0358

Onik, M. M., Kim, C.-S., Lee, N.-Y., & Yang, J. (2019). Personal Information Classification on Aggregated Android Application's Permissions. *Applied Sciences*, *9*(19), 1–24. https://doi.org/10.3390/app9193997

Patel, U. (2024). Data Privacy and Security in Financial Services. *Journal of Artificial Intelligence & Cloud Computing*, *3*(5), 1–13.

https://doi.org/10.47363/JAICC/2024(3)E204

Rachmalia, M. (2025, May). *Mulai 17 Agustus 2025 Belanja di China dan Jepang Bisa Pakai QRIS*. Detik Jatim.

Reis, O., Eneh, N. E., Ehimuan, B., Anyanwu, A., Olorunsogo, T., & Abrahams, T. O. (2024). Privacy Law Challenges in the Digital Age: A Global Review of Legislation and Enforcement. *International Journal of Applied Research in Social Sciences*, *6*(1), 73–88. https://doi.org/10.51594/ijarss.v6i1.733

Romadiah, A., Zulfa, Z., & Puannandini, D. A. (2025). Efektivitas Penerapan UU Perlindungan Data Pribadi dalam Transaksi E-Commerce: Tinjauan Terhadap Keamanan Konsumen. *SYARIAH: Jurnal Ilmu Hukum*, *2*(2), 205–210. https://doi.org/10.62017/syariah.v2i2.3818

Ruslan, S. (2023). Challenges and Opportunities for Legal Practice and the Legal Profession in the Cyber Age. *International Journal of Law and Policy*, *1*(4), 1–10. https://doi.org/10.59022/ijlp.59

Shukla, G., & Puranik, M. (2025). A Study on Security and Privacy in E-Banking. *International Journal For Multidisciplinary Research*, *7*(1), 1–8. https://doi.org/10.36948/ijfmr.2025.v07i01.35701

Situmeang, A., Park, J., Sudirman, L., Silviani, N. Z., & Agustini, S. (2025). Evaluating Data Breach Notification Protocols. *Lentera Hukum*, *12*(1), 42–61. https://doi.org/10.19184/ejlh.v12i1.47621

Situmeang, A., Weley, N. C., & Disemadi, H. S. (2025). Kepastian Pertanggungjawaban Hukum Pidana Korporasi atas Penyalahgunaan Data Pribadi di Indonesia. *Proceedings Series on Social Sciences & Humanities*, *23*, 8–15. https://doi.org/10.30595/pssh.v23i.1544

Sudarso, S., & Yusuf, H. (2024). Landasan Filosofis Hukum

Transaksi Bank Digital di Indonesia. *Journal of Comprehensive Science*, *3*(6), 1061–1071. https://doi.org/10.59188/jcs.v3i6.744

Sulfaunsilah, S., Hokamah, W., Sari, S. F., & Astuti, R. P. (2025). Peran Aktif Bank Indonesia Dalam Menjaga Stabilitas Sistem Keuangan Melalui Sistem Pembayaran. *Menulis: Jurnal Penelitian Nusantara*, *1*(5), 214–220. https://doi.org/10.59435/menulis.v1i5.255

Tan, D. (2021). Metode Penelitian Hukum: Mengupas dan Mengulas Metodologi dalam Menyelenggarakan Penelitian Hukum. *NUSANTARA: Jurnal Ilmu Pengetahuan Sosial*, *8*(5), 2463–2478. https://jurnal.um-tapsel.ac.id/index.php/nusantara/article/view/5601

Union, P. O. of the E., Graux, H., Gryffroy, P., Gad-Nowak, M., & Boghaert, L. (2024). *The role of artificial intelligence in processing and generating new data – An exploration of legal and policy challenges in open data ecosystems*. Publications Office of the European Union. https://doi.org/doi/10.2830/412108

Wewege, L., Lee, J., & Thomsett, M. C. (2020). Disruptions and Digital Banking Trends. *Journal of Applied Finance & Banking*, *10*(6), 15–56.

Windasari, N. A., Kusumawati, N., Larasati, N., & Amelia, R. P. (2022). Digital-only banking experience: Insights from gen Y and gen Z. *Journal of Innovation & Knowledge*, *7*(2), 100170. https://doi.org/https://doi.org/10.1016/j.jik.2022.100170

Wong, R. Y., & Mulligan, D. K. (2019). Bringing Design to the Privacy Table. *Proceedings of the 2019 CHI Conference on Human Factors in Computing Systems*, 1–17. https://doi.org/10.1145/3290605.3300492

Zainal, A. (2023). Role of Artificial Intelligence and Big Data Technologies in Enhancing Anomaly Detection and Fraud

Prevention in Digital Banking Systems. *International Journal of Advanced Cybersecurity Systems, Technologies, and Applications*, *7*(12), 1–10.