TITAH: Journal of Law
2026, 1 (1), 63-84

Protecting Biometric Data in Digital Transactions: Assessing the Adequacy of Indonesia's Personal Data Protection Regime

Ayu Mega Harahap[1]; Juwita Hana Situmorang[2]; Dimas Ilyas Situmorang[3]

[1]Department of Civil Law, Faculty of Law, Universitas Pancasila, Jakarta, Indonesia
[2]Department of Criminal Law, Faculty of Law, Universitas Pancasila, Jakarta, Indonesia
[3]Department of Legal Studies, Faculty of Law, Universitas Pancasila, Jakarta, Indonesia

Article History

Received: 2026-03-14
Revised: 2026-03-21
Accepted: 2026-03-26
Published: 2026-04-08

Keywords:

Biometric Data; Digital Transactions; Personal Data Protection; Privacy by Design; Data Subject Rights.

DOI:

10.xxxx/titah.volx.issx.artx

Corresponding author:

Ayu Mega Harahap
ayu.harahap@univpancasila.ac.id

Other author email(s):

juwita.situmorang@univpancasila.ac.id
dimas.situmorang@univpancasila.ac.id

Paper type:

Research article

Published by PT Penerbit Velora Indonesia

Abstract

Purpose – This study assesses the adequacy of Indonesia's personal data protection regime for biometric data used in digital transactions, focusing on consent, transparency, retention, deletion, security, accountability, and data subject rights.

Methodology – A qualitative socio-legal design involved 24 participants from user, legal-compliance, cybersecurity-biometric, academic, legal-practice, and civil-society groups. The study also reviewed 14 documents from eight digital service providers and applied thematic analysis using rights-based and privacy-by-design frameworks.

Findings – Indonesia's Personal Data Protection Law provides a significant normative foundation, but operational protection remains uneven. Consent was often formal rather than substantively informed, disclosure of retention and third-party processing was limited, and data subject rights were difficult to exercise. Organizations showed stronger cybersecurity maturity than privacy-by-design implementation, while institutional supervision and biometric-specific guidance remained underdeveloped.

Implications – Regulators and digital service providers should strengthen biometric-specific consent, transparency, retention and deletion standards, privacy impact assessments, processor accountability, and accessible rights mechanisms.

Originality – The study assesses biometric protection through the combined interaction of law, institutions, technological design, and user experience.

Cite this article:

Harahap, A. M., Situmorang, J. H., & Situmorang, D. I. (2026). Protecting biometric data in digital transactions: Assessing the adequacy of Indonesia's personal data protection regime. TITAH: Journal of Law, x(x), xx–xx. DOI to be assigned.https://doi.org/10.xxxx/titah.volx.issx.artx

Introduction

The rapid expansion of digital transactions has transformed the way individuals establish identity, access financial services, authorize payments, and interact with digital platforms. Biometric authentication has become increasingly attractive because facial images, fingerprints, iris patterns, voice characteristics, and behavioral traits can provide fast and relatively reliable identity verification. Unlike passwords or identification numbers, however, biometric characteristics remain closely attached to the individual and cannot easily be replaced after compromise. Günay (2023) explains that biometric data require heightened legal protection because they constitute a sensitive category of personal information with distinctive implications for individual rights. The problem extends beyond the confidentiality of information. Mordini (2023) argues that biometric privacy also concerns bodily and psychological integrity because recognition technologies can affect the boundary between individuals and systems that continuously identify them. These characteristics explain why contemporary biometric protection increasingly combines legal safeguards with technical privacy controls. Arman et al. (2024) show that privacy-preserving biometric systems

P ISSN xxxx-xxxx | E ISSN xxxx-xxxx

must reconcile security, recognition performance, and confidentiality across the processing lifecycle. Melzi et al. (2024) similarly demonstrate that biometric privacy requires technical measures capable of reducing linkability, reconstructability, and unauthorized disclosure. Privacy protection must therefore begin before biometric information becomes permanently integrated into a digital identity infrastructure. Hasan et al. (2023) further identify the need for privacy protection at the stage where facial information is captured, rather than relying exclusively on protection after biometric templates have already been generated.

The global proliferation of biometric technologies has also created concerns about consent, surveillance, discrimination, accountability, and the proportionality of data processing. Facial recognition illustrates this tension because it allows individuals to be identified without requiring physical contact and, under certain configurations, without active participation by the person being identified. DP et al. (2023) find that the benefits of facial recognition for security coexist with substantial legal and ethical risks involving personal data protection. Wang et al. (2024) similarly argue that governance frameworks for facial recognition must place privacy and ethical accountability at the center of technological deployment. The regulatory challenge becomes more complex where a general data protection framework exists but lacks rules tailored to biometric identification. Kavoliūnaitė-Ragauskienė (2024) demonstrates that even within the European Union, questions remain regarding whether existing privacy and data protection rules can adequately respond to increasingly sophisticated facial recognition applications. A systematic examination of public facial recognition also identifies privacy, consent, and bias as recurring areas of concern that require stronger institutional safeguards (Beya et al., 2024). These developments indicate that the presence of legislation does not itself guarantee substantive protection. Qandeel (2024) therefore emphasizes that facial recognition governance must be connected to fundamental rights and the rule of law so that technological efficiency does not weaken individual autonomy.

Indonesia faces these challenges while simultaneously accelerating financial inclusion, digital banking, fintech services, electronic commerce, and platform-based transactions. Electronic Know Your Customer procedures increasingly use facial recognition and biometric scanning to establish the identity of customers without requiring face-to-face verification. Fitriyanti et al. (2024) identify biometric verification as an important component of Indonesian e-KYC systems and connect its development with the expansion of the digital economy. The Personal Data Protection Law, Law No. 27 of 2022, has consequently become central to the governance of data-intensive financial services. Zuwanda et al. (2024) show that fintech companies must address consent, security, breach notification, and organizational compliance as part of the new regulatory environment. These obligations are particularly relevant because weaknesses in identity verification and data governance can expose consumers to impersonation and unauthorized transactions. Gunawan (2024) identifies personal data leakage as a significant problem in online lending and highlights stronger authentication as one element of preventive protection. At the same time, biometric authentication creates a new concentration of sensitive information that itself requires protection. Onesi-Ozigagun et al. (2024) observe that AI-driven biometric systems can strengthen fintech security but also introduce privacy and regulatory concerns that must be managed alongside technological benefits. Technical developments show that privacy-enhancing authentication can reduce these risks without abandoning biometrics altogether. Guo et al. (2024), for example, demonstrate that biometric verification can be designed to authenticate users while reducing disclosure of biometric templates.

Indonesia's PDP Law represents an important regulatory milestone because biometric information falls within the category of specific personal data and is therefore entitled to stronger safeguards. Yet the effectiveness of this protection depends on how general principles are translated into technological and organizational procedures. Sembiring et al. (2024) argue that privacy by design is particularly relevant to biometric data because safeguards should operate from registration through subsequent processing rather than being introduced only after a violation

occurs. Regulatory specificity remains another issue. Girsang (2024) concludes that Indonesia still requires clearer rules specifically addressing facial recognition technology because general personal data provisions do not resolve all risks associated with automated biometric identification. Comparative experience reinforces this concern. Natamiharja and Setiawan (2024) find that although Indonesia and France share a commitment to personal data protection, Indonesia remains less mature in regulatory implementation and enforcement. At the domestic level, gaps between legal standards and the realization of privacy rights continue to appear. Judijanto et al. (2024) identify limitations involving legal clarity, enforcement arrangements, technological developments, and public awareness. Institutional challenges also influence the practical effectiveness of the PDP framework. Razi et al. (2024) find that delayed institutional development, technological infrastructure, and coordination can weaken the implementation of statutory protections even after comprehensive legislation has been enacted.

Problems become more visible when biometric technologies are examined from the perspective of users and specific digital applications. A study of biometric self-service technology among older users in Indonesia shows that actual interaction with biometric systems is shaped by facilitating conditions and users' ability to operate the technology (Kumalasari et al., 2024). Trust and perceived risk also influence how individuals respond to biometric authentication. Kusyanti et al. (2024) find that trust, attitude, and perceived risk affect users' willingness to use fingerprint-based authentication. Indonesian research using the Technology Acceptance Model similarly indicates that concerns about how biometric data are stored, accessed, and used can influence technology acceptance (Gusnan & Utomo, 2024). These concerns are no longer theoretical because biometric information has become embedded in commercial platforms. Putri (2025) identifies problems involving explicit consent, transparency, and mechanisms for exercising data subject rights in the use of facial recognition by the FotoYu application. The Worldcoin case extends the problem to iris scanning. Alfaaiz (2025) finds that Indonesia formally classifies iris-based biometric information as protected specific personal data, but limitations remain regarding technical regulation and active institutional supervision. These empirical and case-specific developments indicate that meaningful protection requires more than a privacy notice or formal declaration of consent.

Recent scholarship also reveals a wider enforcement problem within Indonesia's evolving data protection regime. Budiman (2023) argues that the early implementation of the PDP Law faces challenges involving institutional readiness, public awareness, and enforcement capacity. Major cybersecurity incidents have reinforced concerns regarding whether formal rights can be effectively protected against large-scale technological threats. Yusliwidaka et al. (2024) connect Indonesia's personal data protection challenges with weaknesses in cybersecurity infrastructure, institutional coordination, and state responsibility. The legal framework also operates within a digital ecosystem in which private entities routinely collect and exchange data. Syailendra et al. (2024) find that the PDP Law creates significant opportunities for stronger protection but continues to face implementation obstacles that require regulatory and institutional responses. Individual behavior represents another layer of the problem because people may recognize privacy risks while continuing to disclose personal information. Darnela and Rusdiana (2025) identify this privacy paradox in Indonesia and demonstrate that regulatory effectiveness is partly connected to legal awareness and digital literacy. Cross-border processing further complicates accountability in digital services. Rahman and Mulyani (2025) show that Indonesia's post-PDP framework must balance data protection obligations with increasingly complex cross-border data flows. Taken together, existing research has provided strong normative, comparative, technological, and behavioral insights, but it has not sufficiently explained how biometric data protection is understood and operationalized as a process within everyday digital transactions.

This gap is important because regulatory adequacy cannot be evaluated only by comparing statutory provisions with foreign legislation. It must also be assessed through the experiences of

data subjects, compliance professionals, technology providers, and other actors who implement or encounter biometric verification in practice. Comparative research indicates that Indonesia still faces weaknesses in procedural detail, institutional readiness, and enforceability when measured against more mature regimes (Taufiq & Kenyo, 2025). Questions also remain about privacy by design, data portability, supervisory independence, and cross-border governance (Karnedi & Alam, 2025). The development of Indonesia's digital identity system further demonstrates that privacy protection intersects with identity fraud prevention, public trust, legal certainty, and institutional responsibility (Priyantiwi & Hufron, 2025). Against this background, this study aims to assess qualitatively the adequacy of Indonesia's personal data protection regime in safeguarding biometric data used in digital transactions. It focuses on consent, transparency, purpose limitation, data minimization, storage and retention, deletion, security, third-party access, accountability, breach response, and remedies. The study contributes theoretically by integrating a rights-based conception of privacy with privacy by design and socio-legal analysis. Practically, it seeks to provide evidence for regulators, financial institutions, fintech companies, technology providers, and digital platforms when developing biometric governance that protects users throughout the data-processing lifecycle.

Literature Review

Biometric Data and the Changing Meaning of Digital Identity

Biometric authentication differs fundamentally from conventional identity verification because it transforms physical or behavioral characteristics into information that can be processed computationally. Fingerprints, facial characteristics, iris patterns, voices, and behavioral signals may function as evidence that a person is who they claim to be. This capability provides convenience but also creates distinctive security risks. Bezas and Filippidou (2023) explain that biometric characteristics are persistent and unique, making attacks against biometric systems particularly consequential when the underlying identifiers cannot simply be replaced. Their analysis of facial anti-spoofing techniques demonstrates that biometric security must account for presentation attacks and attempts to imitate legitimate users.

Modern biometric authentication also creates a broader attack surface as artificial intelligence improves the ability to generate convincing artificial identities. Salko et al. (2024) show that deepfakes can threaten face authentication systems and create risks to financial security and protected digital services. The problem illustrates why biometric authentication should not be treated as inherently secure simply because it relies on biological characteristics. Sriman et al. (2024) identify spoofing, multimodal integration, privacy, and fraudulent activity as persistent challenges across biometric authentication techniques. Security and privacy therefore remain interdependent. A biometric system that increases authentication accuracy while exposing templates or enabling unrestricted secondary processing cannot be classified as adequately protective.

Privacy-Preserving Biometric Authentication

Technical research increasingly seeks to reduce the exposure of biometric information during authentication. One major approach involves cryptographic methods that enable comparison or verification while preventing disclosure of raw biometric information. Yang et al. (2023) show that homomorphic encryption has become an important privacy-preserving mechanism because computations can be conducted without exposing the underlying biometric data in plain form. Such solutions are relevant to legal concepts such as data minimization because a controller should avoid exposing more information than is necessary to complete an authentication task.

Privacy-preserving technology, however, cannot replace governance. Technical protection does not determine whether data collection is lawful, whether users have received meaningful information, or whether the purpose of processing is proportionate. Vásquez Cerna et al. (2023) identify evolving vulnerabilities in biometric authentication and emphasize the need to combine

technological safeguards with ethical and regulatory controls. This distinction is important for the present study. Regulatory adequacy requires both legal legitimacy and technically credible implementation.

Consent, Autonomy, and Purpose Limitation

Consent holds an important but complex role in biometric processing. Digital service providers can present biometric authentication as a voluntary security feature while, in practice, making it difficult to obtain the service without completing facial or fingerprint verification. A formal act of clicking an agreement does not necessarily demonstrate meaningful autonomy when the user lacks information about storage, retention, sharing, or alternative authentication mechanisms. This problem becomes especially significant when data controllers reuse biometric information for purposes that were not apparent when it was initially collected.

Purpose limitation therefore provides a critical safeguard. Biometric information collected to authenticate one transaction should not automatically become available for unrelated profiling, marketing, surveillance, or machine learning. The principle also requires controllers to define the purpose before collecting information rather than develop new purposes after accumulating large biometric databases. Data minimization supports this requirement by limiting collection to information objectively needed for verification.

A rights-based interpretation strengthens these principles because biometric privacy concerns individual autonomy as well as information security. Data subjects should be able to understand why biometric verification is required, who controls the information, whether third parties receive access, how long the information remains stored, and what mechanism exists for deletion or complaint. In this sense, transparency functions as a prerequisite for meaningful consent rather than an independent administrative formality.

Privacy by Design and Biometric System Architecture

Privacy by design provides an important conceptual framework for connecting legal principles with technological practice. Under this approach, privacy protection begins during system planning rather than after deployment. A biometric system should therefore incorporate minimization, access control, secure templates, separation of datasets, retention limits, deletion procedures, logging, and incident response from the beginning of its lifecycle.

The value of privacy by design lies in its preventive orientation. Once raw biometric information has been extensively replicated across interconnected platforms, remedies become more difficult. The risk is higher than with replaceable credentials because a person's face or fingerprint cannot be reset in the same way as a password. System architecture therefore influences the substantive realization of the right to privacy.

Privacy by design also requires organizational responsibility. A technologically secure system may still violate privacy if employees receive unnecessary access, vendors process biometric information without adequate restrictions, or organizations retain information indefinitely. Effective privacy design consequently involves legal, technical, and organizational measures that operate together.

Regulatory Adequacy under Indonesia's PDP Regime

Indonesia's PDP Law creates an important legal foundation by recognizing data subject rights and imposing duties on controllers and processors. Its relevance to biometric data arises from the classification of biometric information as specific personal data. This classification reflects the greater risks associated with processing information capable of establishing or authenticating identity.

Substantive adequacy nevertheless depends on regulatory detail. A general obligation to protect personal data does not necessarily answer operational questions involving biometric

templates, raw facial photographs, liveness detection data, third-party identity verification providers, automated matching, or model-training datasets. The distinction becomes particularly important as biometric services increasingly rely on complex chains of controllers, processors, cloud infrastructure, and specialized technology vendors.

Institutional adequacy represents another dimension. Data subjects require an identifiable institution that can investigate complaints, assess controller practices, coordinate breach responses, and impose sanctions. Weak institutional capacity can convert statutory rights into rights that are difficult to enforce. The effectiveness of biometric regulation therefore depends on the interaction between substantive rules, institutional authority, technological competence, and procedural accessibility.

Procedural adequacy concerns whether individuals can actually exercise the rights granted by legislation. A right to obtain information has limited practical value when privacy notices are highly technical. A right to deletion becomes ineffective when users cannot identify where biometric templates are stored. A right to object becomes weak when authentication cannot be completed through a reasonable alternative method. This study therefore treats regulatory adequacy as an operational concept rather than a simple assessment of whether relevant statutory provisions exist.

Research Gap and Analytical Framework

Existing literature can be divided into four main streams. The first examines the technical security and privacy of biometric systems. The second evaluates ethical and human rights consequences of facial recognition. The third analyzes Indonesia's PDP Law through normative and comparative legal research. The fourth examines technology acceptance, trust, and perceived risk among biometric users. Each stream contributes an important dimension, but they rarely examine these dimensions together.

The Indonesian literature is particularly strong in doctrinal analysis. It identifies the status of biometric information, controller obligations, weaknesses in facial recognition regulation, enforcement limitations, and differences from foreign data protection regimes. Research has also begun to address specific technologies such as e-KYC, facial recognition applications, iris scanning, and digital identity systems. Nevertheless, most studies evaluate legal provisions or individual cases rather than investigating how multiple actors translate those legal requirements into everyday data-processing practices.

Empirical technology studies provide another useful perspective but usually focus on adoption and acceptance. These studies explain whether people consider biometrics convenient, risky, trustworthy, or easy to use. They offer less evidence about whether users understand their statutory rights, how organizations operationalize retention and deletion, or how consent works when biometric verification becomes effectively necessary to access a service.

This study addresses that gap by using regulatory adequacy as its central analytical concept. Regulatory adequacy is assessed across four dimensions: substantive protection, institutional capacity, procedural effectiveness, and technological implementation. A rights-based approach is used to evaluate autonomy, transparency, control, proportionality, and access to remedies. Privacy by design is used to determine whether organizations translate these principles into system architecture and data-management practices. The socio-legal perspective connects both frameworks with the experiences of users and institutional actors. This integrated framework enables the study to investigate the difference between protection in law and protection in practice.

Research Methods

Research Design

This study adopts a qualitative socio-legal research design. The approach combines legal analysis with an empirical examination of how biometric data protection operates within digital

transactions. A purely doctrinal approach would establish what the PDP Law requires but would provide limited evidence about how organizations understand those requirements, how technology systems implement them, and how users experience biometric verification. The socio-legal design addresses this limitation by treating regulation as both a body of legal norms and a set of practices produced through interactions among law, institutions, technologies, and individuals.

The research focuses on biometric processing associated with digital transactions in Indonesia. Relevant practices include facial recognition in e-KYC, fingerprint-based authentication, biometric account access, identity verification, and other biometric mechanisms used by financial institutions, fintech providers, and digital platforms. The unit of analysis is not the accuracy of a biometric algorithm. Instead, the study examines the process through which biometric information is collected, processed, stored, shared, protected, and deleted.

Participants and Sampling Strategy

The study uses purposive sampling to identify participants with direct experience or specialized knowledge concerning biometric data and digital transactions. The final sample comprised 24 participants: 10 users of biometric-enabled digital services, five legal or compliance professionals, four cybersecurity and biometric technology professionals, and five academics, legal practitioners, or civil society representatives working on privacy and digital rights. Maximum variation was applied within the purposive strategy so that the study did not rely on one institutional perspective. User participants varied in their experience with digital financial services and frequency of biometric authentication, while professional participants represented legal compliance, information security, technological implementation, and privacy governance functions.

Snowball recruitment supplemented purposive recruitment where relevant specialists were difficult to identify. Participant recruitment continued until interviews no longer generated substantial new meanings relevant to the analytical categories. Saturation was evaluated at the level of themes rather than through a predetermined numerical threshold. This strategy was appropriate because the purpose of the study was analytical depth and variation of experience rather than statistical representation of Indonesia's entire population.

Data Collection

Primary data were collected through semi-structured in-depth interviews. This format provided consistency across the main topics while allowing participants to explain their experiences in their own terms. Interviews with data subjects explored how biometric verification was introduced, what information they received, whether alternatives were available, how they understood consent, whether they knew where their data would be stored, and whether they understood their rights after providing biometric information.

Interviews with organizational participants examined the translation of legal requirements into internal procedures. Topics included the identification of a lawful basis for processing, informed consent, purpose specification, data minimization, privacy impact assessment, retention periods, deletion procedures, access control, encryption, vendor management, cross-border processing, incident response, and communication with data subjects. Technology professionals were also asked how legal principles affected system architecture and whether technical limitations created difficulties in implementing data subject rights.

The interview guide used open-ended questions and follow-up probes. Interviews were conducted face-to-face or through secure online communication depending on participants' geographical location and availability. Each interview lasted approximately 45 to 75 minutes. With participant permission, interviews were audio-recorded and transcribed verbatim. Field notes recorded contextual information, non-sensitive observations, and preliminary analytical reflections.

Document Analysis

Interview evidence was supplemented by qualitative document analysis. The documentary corpus comprised 14 documents from eight digital service providers, including privacy notices, biometric consent statements, terms of service, and publicly available information concerning e-KYC and identity-verification procedures. Legal documents included Law No. 27 of 2022 on Personal Data Protection and relevant regulations concerning electronic systems, financial technology, digital identity, and electronic transactions. Public documentation concerning selected biometric cases was also reviewed where it provided evidence relevant to facial recognition, iris scanning, e-KYC, or biometric authentication.

Document analysis served two purposes. First, it established the normative standards against which participants' accounts could be interpreted. Second, it allowed the researcher to compare what organizations publicly communicated with how relevant actors described actual implementation. Documents were selected according to relevance rather than quantity. They were included when they contained information directly connected with the collection, processing, protection, or governance of biometric or identity-related data in digital transactions, while documents that mentioned privacy only in general terms without relevance to the analytical framework were excluded.

Data Analysis

The research applied reflexive thematic analysis using a combination of inductive and deductive coding. Analysis began with repeated reading of interview transcripts and documents. Initial codes captured statements concerning consent, transparency, user understanding, voluntariness, necessity, purpose limitation, minimization, storage, retention, deletion, security, access, third-party processing, accountability, data breaches, supervision, and remedies.

Inductive coding allowed themes to emerge from participant accounts even when they did not fit predetermined legal categories. This step was important because users and practitioners could understand biometric risks differently from the terminology used in statutes. Deductive coding then connected these emerging meanings with the rights-based framework, privacy-by-design principles, and the obligations established under Indonesia's PDP regime. Codes were progressively grouped into higher-level themes, including the limits of meaningful biometric consent, fragmented control over the biometric lifecycle, the imbalance between security and privacy maturity, institutional implementation gaps, and the practical accessibility of data subject rights.

The final analytical stage compared the themes with four dimensions of regulatory adequacy. Substantive adequacy considered the clarity and scope of rights and obligations. Institutional adequacy considered supervision, coordination, and enforcement capacity. Procedural adequacy considered whether data subjects could effectively exercise their rights. Technological adequacy considered whether legal safeguards were embedded into biometric system design. This analytical structure allowed the study to determine where formal legal protection corresponded with practice and where implementation gaps persisted.

Trustworthiness

The study used several procedures to strengthen qualitative trustworthiness. Source triangulation compared accounts from users, legal and compliance personnel, technical professionals, academics, and civil society actors. Method triangulation compared interview evidence with legal and organizational documents. Contradictory evidence was retained and examined rather than removed because differences among stakeholders could reveal important institutional or technological tensions.

An audit trail documented sampling decisions, interview development, coding changes, theme formation, and interpretation. Reflexive notes recorded how the researcher's legal assumptions could influence interpretation. The analysis also paid particular attention to negative cases. When

a participant reported effective privacy practices that differed from the dominant pattern, that evidence was examined to identify the conditions that produced stronger protection. This approach prevented the analysis from treating regulatory weakness as a predetermined conclusion and supported a balanced assessment of the PDP regime.

Ethical Considerations

Participation was voluntary and based on informed consent. Participants received clear information concerning the study's purpose, interview procedures, recording, confidentiality, data storage, and their ability to discontinue participation. The research collected only information required to answer the research questions. No biometric sample was collected during the study, and participants were not asked to provide fingerprints, facial templates, iris information, account credentials, passwords, or confidential security configurations.

Personal identifiers were removed from transcripts, and pseudonymous participant codes were used during analysis and reporting. Interview recordings and transcripts were stored in access-restricted digital storage. Quotations were reviewed to prevent indirect identification of participants whose positions or institutional responsibilities could make them recognizable. Organizationally sensitive information was reported only at the level necessary to explain the research findings. These procedures ensured that a study concerning personal data protection did not itself reproduce unnecessary data-processing risks.

Results and Discussion

The analysis involved 24 participants divided into four stakeholder groups: 10 users of digital services that employed biometric verification, five legal or compliance professionals, four cybersecurity and biometric technology professionals, and five academics, legal practitioners, or civil society representatives working on privacy and digital rights. The empirical material was complemented by documentary analysis of 14 documents from eight digital service providers, consisting of privacy notices, biometric consent statements, terms of service, and publicly available information concerning e-KYC and identity verification procedures. The thematic analysis identified six closely connected findings concerning the substantive quality of consent, transparency and information asymmetry, fragmented control over the biometric data lifecycle, the stronger development of security measures compared with privacy controls, institutional implementation gaps, and difficulties in exercising data subject rights. These themes indicate that the adequacy of biometric data protection cannot be evaluated solely from the existence of statutory provisions. It must also be examined through the way organizations interpret those provisions, the way biometric systems are technically designed, and the extent to which users can understand and exercise the rights formally granted to them.

Biometric Consent Remains Formally Available but Substantively Uneven

The findings indicate a clear difference between the formal existence of biometric consent and the substantive quality of that consent. Eight of the 10 user participants described biometric verification as effectively mandatory because they could not complete account registration, identity verification, or certain digital transactions without submitting facial or fingerprint data. Only two participants recalled being offered an alternative verification mechanism. Most users consequently understood biometric verification as a routine technical requirement attached to the service rather than as a separate decision involving the processing of highly sensitive personal data. This distinction is important because a user may technically click an agreement while having little practical freedom to reject biometric processing if rejection prevents access to the service. The interview findings therefore suggest that voluntariness becomes difficult to establish when biometric identification is embedded into essential account-opening, transaction, or security procedures without a reasonable alternative.

The interviews further revealed that formal acceptance was not accompanied by an equally strong understanding of the processing involved. Seven of the 10 users remembered clicking an agreement or accepting terms before biometric verification, but only three users could explain whether their biometric information would be stored after the verification process had been completed. None of the participants could clearly distinguish between an ordinary facial photograph, a biometric template, liveness-detection information, and the technical result of a biometric match. This finding shows that consent mechanisms may fulfil a procedural function without ensuring that users understand what type of information is being processed, for what purpose it will be used, how long it will be retained, or whether it will be transferred to another processor. Putri (2025) identifies comparable concerns regarding explicit consent and transparency in facial recognition-based digital services in Indonesia, while the present findings demonstrate that the issue extends beyond the existence or absence of consent and involves the substantive quality of the user's understanding.

A notable gap also emerged between the way organizations assessed consent and the way users experienced it. Four of the five compliance participants considered their organizations' consent procedures legally adequate because users received privacy information before continuing with biometric verification. In contrast, eight user participants admitted that they focused primarily on completing registration, recovering account access, or authorizing a transaction and did not read the privacy information in detail. This divergence suggests that organizations tend to evaluate consent through documented procedures, while users experience consent within a practical context shaped by urgency, convenience, and the desire to complete the service process. Darnela and Rusdiana (2025) describe a similar privacy paradox in Indonesia, where individuals may understand that disclosure creates privacy risks but continue to provide data because immediate benefits outweigh perceived long-term consequences. In biometric transactions, this tension becomes more serious because compromised biometric identifiers cannot be replaced as easily as passwords or account credentials.

The findings therefore suggest that Indonesia's PDP regime provides a sufficient formal basis for requiring consent but does not yet ensure that such consent is consistently meaningful in biometric transactions. A more protective approach would require biometric consent to be separated from general terms and conditions and presented through concise, contextual information immediately before biometric capture. Users should be told what biometric information will be collected, why it is necessary, whether it will be retained, whether third parties will process it, and what consequences follow if the user refuses. This approach would move consent from a procedural formality toward a substantive mechanism for protecting autonomy and would better align organizational compliance with the actual experience of data subjects.

Transparency Is Weakened by Information Asymmetry

The second major finding concerns the information gap between digital service providers and the individuals whose biometric data are processed. Seven of the 10 user participants understood the immediate purpose of biometric verification, usually as a mechanism for identity confirmation, account security, or fraud prevention. However, only three participants could explain what happened to their biometric information after verification had been successfully completed. Most users were uncertain whether facial images were deleted immediately, retained by the service provider, transformed into biometric templates, stored for future authentication, or transmitted to external technology providers. This uncertainty indicates that transparency is often concentrated on explaining why biometric verification is needed at the point of use, while considerably less information is communicated concerning the subsequent lifecycle of the data.

Document analysis reinforced this pattern. Of the 14 documents reviewed, 11 provided a general explanation of the purposes for collecting personal data, but only six explicitly identified biometric information as a distinct category of processed data. Only three documents stated a

reasonably clear retention period for biometric or identity-verification data, and only four documents clearly disclosed that third-party technology or verification providers could participate in processing. These results show that digital service providers generally communicate broad privacy principles more effectively than the specific mechanisms governing biometric processing. The distinction matters because biometric data carry greater risks than many ordinary account details, yet users often receive less concrete information about storage periods, processor involvement, deletion procedures, and technical transformation of those data.

The problem becomes particularly important in e-KYC environments, where a single verification transaction may involve several interconnected systems. Fitriyanti et al. (2024) emphasize that personal data protection has become central to Indonesian e-KYC because remote identity verification depends on intensive digital processing and data exchange. The present findings show that users often see only the visible part of that process, such as taking a selfie or completing a liveness test, while remaining unaware of the underlying processing chain. Interviews with compliance and technical personnel confirmed that six of the eight digital services represented in the document sample relied on at least one external provider for identity verification, cloud infrastructure, fraud detection, or biometric processing. Nevertheless, the involvement of these external actors was not always presented clearly in the documents available to users.

The absence of specific retention information also weakens transparency because users cannot evaluate whether continued storage remains proportionate to the original purpose of collection. Statements that data will be retained 'for as long as necessary' give organizations substantial discretion while providing users with limited certainty about when their information will actually be deleted. Arman et al. (2024) argue that biometric privacy must be protected across the entire processing lifecycle, and the present findings support this position by showing that transparency cannot stop at the moment of collection. Effective transparency should explain the immediate purpose, storage model, expected retention period, processor involvement, and the user's available rights in a layered and accessible format. Such an approach would reduce information asymmetry and enable users to evaluate biometric processing based on more than the visible authentication interface.

Control Becomes Fragmented Across the Biometric Data Lifecycle

The third theme concerns the fragmentation of control once biometric information enters digital processing systems. Interviews with compliance and technology participants revealed a common sequence that included identity-document submission, facial image capture, liveness detection, biometric comparison, generation of a verification result, storage of identity-verification records, and retention of selected information for fraud-prevention or compliance purposes. This sequence demonstrates that biometric processing is rarely a single act of capturing and comparing a face. Instead, it consists of multiple technical operations that may generate different types of information and may involve several organizational actors. Such complexity increases the importance of clearly allocating responsibility for each stage of collection, transformation, storage, access, retention, and deletion.

Among the nine compliance and technology participants, seven reported that at least one stage of biometric processing depended on an external vendor or cloud-based service. This arrangement means that a digital service provider may remain legally responsible for data protection even when important processing functions are technically performed by another organization. The involvement of external processors creates additional difficulties because biometric information or related verification records can be distributed across infrastructures controlled by several entities. Responsibility therefore needs to be maintained not only through contracts but also through technical auditability, access controls, processor monitoring, and clear procedures for responding to user requests. Without such mechanisms, a controller may be unable to determine quickly where

a particular biometric record exists or whether all copies have been removed after a deletion request.

The interviews revealed that deletion was one of the clearest examples of this fragmentation. Only three of the nine organizational participants stated that their organizations had a clearly documented procedure for tracing biometric information across primary systems, vendor environments, and backup storage after a deletion request. Four participants understood deletion primarily as removing data from an active customer-facing system, while two acknowledged that backup copies could remain until routine retention periods expired. These different interpretations demonstrate that deletion does not always carry the same legal and technical meaning. A user may reasonably believe that data have disappeared after requesting deletion, while copies could continue to exist in backup repositories, security logs, fraud-prevention databases, or processor-controlled environments for a specified period.

Retention practices were similarly inconsistent. Five organizational participants stated that retention periods were primarily determined by internal compliance or fraud-prevention policies, while only three described a process in which retention was regularly reassessed against necessity and purpose limitation. One participant acknowledged that technical dependence on third-party systems could affect the speed at which particular records were removed. Sembiring et al. (2024) argue that privacy safeguards must be incorporated across the biometric lifecycle, and this finding illustrates why such an approach is necessary. A legal right to deletion becomes difficult to exercise when a system was not designed from the beginning to locate, separate, and remove biometric data efficiently.

The findings therefore reveal that Indonesia's current regulatory framework provides general principles for accountability, purpose limitation, and data subject rights but leaves substantial operational variation in how controllers implement them. Melzi et al. (2024) emphasize that privacy-enhancing biometric systems should reduce unnecessary exposure and linkability, which is especially relevant where information passes through several processors. More detailed implementation standards are needed to clarify what constitutes effective deletion, how long particular biometric records may be retained, what controllers must document when third parties are involved, and how users can be assured that requests have been fulfilled throughout the entire processing chain.

Technical Safeguards Are Developing Faster Than User-Facing Privacy Controls

The fourth theme shows that organizations generally demonstrate stronger maturity in cybersecurity controls than in privacy-oriented system design. All nine compliance and technology participants identified at least one technical safeguard used to protect identity-verification systems. Eight participants reported encryption during storage or transmission, seven mentioned role-based or restricted access controls, six referred to liveness detection or anti-spoofing mechanisms, and five described additional authentication measures for employees or administrators accessing sensitive systems. These findings indicate that organizations are aware of the security threats associated with biometric systems and have adopted measures intended to prevent unauthorized access, impersonation, and fraudulent verification.

This emphasis is justified because biometric authentication systems face increasingly sophisticated attacks. Vásquez Cerna et al. (2023) identify presentation attacks, reconstruction risks, and other vulnerabilities that require continuous improvement of technical safeguards. Salko et al. (2024) further demonstrate that deepfake technologies create new challenges for facial authentication because synthetic facial content can be designed to imitate legitimate users. Liveness detection, anti-spoofing measures, encryption, and restricted system access therefore represent important elements of biometric security, especially in financial and high-risk digital transactions where successful impersonation can lead directly to financial loss or identity abuse.

However, the interviews revealed that privacy engineering received considerably less attention than conventional security. Only four of the nine organizational participants could identify specific privacy-by-design measures beyond standard information-security controls. Three mentioned minimization of stored biometric information, two described separation between raw facial images and verification records, and only two referred to privacy impact assessment as a routine element of system development. This imbalance suggests that many organizations interpret biometric protection primarily through a cybersecurity lens. While such controls reduce the risk of unauthorized access, they do not automatically address excessive collection, prolonged retention, insufficient transparency, weak consent, or unnecessary secondary use.

The distinction between privacy and security therefore becomes central to evaluating regulatory adequacy. Security focuses on maintaining confidentiality, integrity, and availability, while privacy also concerns necessity, proportionality, purpose limitation, user autonomy, and the ability to control personal information. A biometric database can be encrypted and technically resistant to intrusion while still violating privacy principles if the organization retains information longer than necessary or processes it for purposes that users did not reasonably understand. Guo et al. (2024) demonstrate that privacy-preserving biometric authentication can reduce exposure without sacrificing verification functionality, while Yang et al. (2023) show that privacy-preserving computation can support authentication without requiring unnecessary disclosure of sensitive information.

The findings therefore support the development of a risk-based model that combines cybersecurity and privacy engineering rather than treating them as separate or competing objectives. Biometric systems used in financial and digital transactions should apply encryption, template protection, anti-spoofing, restricted access, data minimization, defined retention periods, processor controls, and privacy impact assessments as interconnected safeguards. This approach would shift organizational practice from protecting biometric data primarily against external attack toward protecting individuals against the full range of risks created by collection, retention, reuse, and institutional misuse.

Regulatory Protection Is Stronger on Paper Than in Institutional Practice

The fifth theme concerns the difference between the normative development of Indonesia's personal data protection regime and the maturity of its implementation. All 10 professional participants drawn from legal, academic, and civil society backgrounds regarded Law No. 27 of 2022 as a major improvement compared with the previously fragmented framework governing personal data. They particularly recognized the importance of data subject rights, controller accountability, breach obligations, and the classification of biometric information as specific personal data. However, eight of the 10 participants considered implementation and enforcement to be less developed than the substantive framework contained in the law, suggesting that Indonesia has moved faster in establishing legal principles than in building consistent institutional mechanisms for applying them.

The most frequently identified problems involved detailed implementation guidance, supervisory capacity, coordination between sectoral regulators, and clear technical standards for high-risk data processing. Seven professional participants specifically stated that biometric technologies require more detailed operational guidance because general principles such as security, minimization, transparency, and accountability allow organizations considerable room for interpretation. This creates the possibility that two organizations can both claim compliance while applying substantially different standards for biometric retention, deletion, third-party processing, and privacy impact assessment. Natamiharja and Setiawan (2024) similarly find that Indonesia's data protection framework remains at an earlier stage of institutional development than more mature European systems.

Participants also emphasized that effective biometric supervision requires technical as well as legal expertise. Six professional participants argued that document-based compliance review would be insufficient for investigating complex biometric systems because privacy risks may be embedded in technical architecture, algorithms, vendor relationships, access configurations, or retention mechanisms that are not visible from privacy policies alone. Yusliwidaka et al. (2024) identify institutional coordination and cybersecurity infrastructure as significant challenges in Indonesian personal data governance, while the findings of this study indicate that those challenges become even more important when regulators must assess automated biometric recognition and high-risk identity technologies.

An important distinction emerged between normative adequacy and operational adequacy. Nine of the 10 professional participants considered the PDP Law generally sufficient to establish basic principles, rights, and responsibilities, yet only three considered the current implementation environment mature enough to produce consistent protection across digital services. Taufiq and Kenyo (2025) identify similar gaps concerning institutional readiness and enforceability when comparing Indonesia's regime with the GDPR. This means that the central challenge is not the complete absence of legal regulation but the translation of broad statutory principles into uniform technical, procedural, and supervisory standards.

The findings therefore characterize the Indonesian situation as an implementation gap rather than a legal vacuum. The law provides a strong normative starting point, but institutional effectiveness depends on regulatory clarity, specialized technical competence, effective complaint mechanisms, coordination among authorities, and consistent enforcement. Without these supporting mechanisms, organizations may interpret compliance differently, and users may receive unequal levels of protection depending on the platform or service involved. Strengthening implementation is therefore as important as refining substantive rules because effective biometric governance depends on the ability of institutions to supervise technological practice rather than simply recognize privacy rights in legislation.

Data Subject Rights Are Difficult to Exercise After Biometric Collection

The sixth theme concerns the practical accessibility of data subject rights once biometric information has entered a digital system. Among the 10 user participants, only two knew how to submit a specific request to access or delete personal data through the services they used. Four participants knew in general terms that privacy rights existed but could not identify the procedure or communication channel through which they could exercise those rights. The remaining four had never considered requesting access to or deletion of biometric information. These findings indicate that legal rights have not yet become familiar or easily usable mechanisms for most users, particularly when the information involved is biometric rather than ordinary account data.

The documentary evidence confirmed this problem. Nine of the 14 reviewed documents mentioned at least one data subject right, but only five provided a clear procedural channel for requesting access, correction, objection, or deletion. Three documents directed users to a general customer-service function without explaining how requests involving biometric information would be distinguished from ordinary account inquiries. This creates practical uncertainty because users may not know whether a facial template can be accessed or deleted separately from the customer account, whether verification logs remain after deletion, or whether exercising a privacy right will affect future access to the service.

Users also demonstrated limited understanding of the distinction between ordinary personal information and biometric data. Eight of the 10 participants knew how to update information such as email addresses or telephone numbers, while only two believed they could separately access or request deletion of biometric information. Putri (2025) identifies similar concerns regarding the exercise of rights in facial recognition-based services, and the present study extends that finding to the wider context of digital transactions. The difficulty does not arise only because users lack legal

knowledge. It also reflects the technical invisibility of biometric processing because users often do not know whether the system retains a photograph, template, verification token, or another form of derived information.

This issue has broader implications for digital identity governance. Priyantiwi and Hufron (2025) emphasize that personal data protection within digital identity systems is connected to privacy, fraud prevention, trust, and legal certainty. For these rights to be meaningful, organizations need to translate them into procedures that users can understand without specialized legal or technical knowledge. A deletion mechanism, for example, should explain what information will be removed, whether temporary copies remain in backups, how long the process will take, and whether alternative authentication methods are available after deletion.

The findings therefore indicate that regulatory effectiveness should be measured not only by whether rights appear in legislation or privacy policies but also by whether ordinary users can exercise them without excessive difficulty. Digital service providers should establish biometric-specific pathways for access, objection, withdrawal of consent, and deletion, accompanied by clear explanations of the effects of each request. Making these procedures visible and understandable would strengthen user control and help transform abstract statutory rights into practical protections within everyday digital transactions.

Overall Assessment of Regulatory Adequacy

Taken together, the findings show that Indonesia's personal data protection regime provides a stronger normative foundation than operational protection for biometric data used in digital transactions. The PDP Law establishes important principles, recognizes the sensitivity of biometric information, and places obligations on controllers and processors. However, these protections are implemented unevenly at the level of consent, transparency, lifecycle management, technical system design, supervision, and user remedies. The evidence therefore suggests that the central weakness is not the absence of a regulatory foundation but the incomplete translation of that foundation into consistent organizational and technological practice.

From the perspective of substantive adequacy, the regime can be regarded as moderately strong because participants generally recognized that the PDP Law establishes sufficient legal principles concerning lawful processing, security, accountability, and data subject rights. Nevertheless, eight professional participants considered biometric-specific implementation guidance inadequate, particularly in relation to retention periods, deletion standards, third-party processors, biometric templates, and high-risk automated identification. This indicates that broad statutory provisions are capable of supporting biometric protection but require more detailed standards to ensure uniform implementation across different sectors and technologies.

From the perspective of procedural adequacy, the findings reveal more substantial weaknesses. Eight of the 10 users experienced biometric verification as effectively mandatory, only three understood what happened to biometric information after verification, and only two knew a specific procedure for exercising access or deletion rights. These findings demonstrate that formal rights and consent mechanisms do not necessarily produce informed participation or effective control. Procedural adequacy therefore depends on accessible explanations, reasonable alternatives where possible, clear request mechanisms, and practical guidance concerning what users can do after their biometric information has been collected.

From the perspective of technological adequacy, security controls were comparatively stronger than privacy-oriented controls. Eight of the nine organizational participants reported encryption, while six identified anti-spoofing or liveness-detection mechanisms. In contrast, only four could identify specific privacy-by-design practices beyond conventional security measures. The findings therefore suggest that biometric systems are becoming technologically more secure against unauthorized access and impersonation, but organizations have not yet incorporated

privacy principles with the same consistency. Protection remains predominantly security-oriented rather than fully privacy-oriented.

From the perspective of institutional adequacy, participants consistently identified an implementation gap. Eight of the 10 professional participants considered enforcement and implementation less mature than the substantive framework, while only three believed the current institutional environment was capable of guaranteeing consistent protection. Razi et al. (2024) identify similar implementation challenges within Indonesia's broader PDP regime. The overall assessment is therefore that Indonesia has established the basic legal architecture needed to protect biometric information, but procedural, institutional, and technological implementation remains uneven. The regime can consequently be characterized as normatively established but operationally incomplete.

Practical Implications

The findings have several practical implications for digital service providers, technology companies, and regulators. First, biometric consent should be separated from general privacy statements and presented in a contextual format immediately before collection. Users need concise information explaining what type of biometric information will be captured, why it is needed, whether it will be retained, whether another organization will process it, and what alternatives exist. This approach would reduce the gap between formal consent and meaningful understanding and would make biometric processing more transparent at the point where the privacy decision is actually made.

Second, organizations should establish clearer biometric retention and deletion policies. The documentary analysis showed that only three of the 14 reviewed documents communicated reasonably clear retention periods, while organizational interviews revealed different interpretations of deletion. Controllers should therefore define retention periods according to necessity and legal purpose rather than operational convenience and should create technical workflows capable of tracing data across active databases, processors, logs, and backup environments. Users should also receive clear confirmation regarding the scope and completion of a deletion request.

Third, privacy impact assessment should become a routine requirement for high-risk biometric processing. The interviews revealed considerably stronger use of conventional security controls than privacy-by-design measures. A structured privacy impact assessment should examine whether biometric processing is necessary, whether less intrusive alternatives exist, what data will be retained, how processors are controlled, how bias or security risks will be managed, and whether data subject rights can be technically supported. Integrating these questions before system deployment would reduce the need for corrective measures after privacy problems have already emerged.

Fourth, regulators should develop more specific technical and procedural guidance for biometric data. General obligations under the PDP Law remain important, but high-risk processing requires more detailed interpretation concerning raw facial images, derived biometric templates, liveness information, processor responsibilities, retention, deletion, template protection, encryption, and incident response. Such guidance would reduce inconsistency among controllers and give supervisory authorities clearer standards for evaluating compliance.

Finally, service providers should establish accessible pathways for exercising biometric-specific rights. Users should not be required to infer how general privacy rights apply to technically complex biometric systems. Clear procedures should explain how access, objection, correction where applicable, consent withdrawal, and deletion operate in practice, how long requests will take, and whether exercising those rights affects future use of the service. These measures would strengthen accountability while also improving public trust in digital identity technologies.

Overall Discussion

The findings extend existing Indonesian scholarship by showing that the main challenge in biometric data protection lies in the relationship between formal law and operational practice. Previous studies have identified normative shortcomings, technological vulnerabilities, institutional limitations, and patterns of technology acceptance, but these dimensions are often examined separately. The present analysis demonstrates that they are interconnected. Weak consent can be reinforced by opaque technology, fragmented processing can make deletion difficult, strong cybersecurity can coexist with weak privacy governance, and legal rights can remain ineffective when institutions or users lack practical mechanisms to enforce them.

The strongest pattern concerns the difference between formal compliance and substantive experience. Most organizational participants regarded existing consent procedures as legally defensible because information was provided before biometric verification, yet most users experienced the process primarily as a required technical step. This gap demonstrates that compliance cannot be assessed solely through the existence of documentation. It must also consider whether users understand the processing, whether they can make meaningful choices, and whether organizational procedures support the actual exercise of rights.

A second important pattern is the difference between security maturity and privacy maturity. Organizations showed strong awareness of encryption, access control, liveness detection, and fraud prevention, but fewer participants could identify systematic privacy-by-design practices involving minimization, lifecycle transparency, retention controls, and privacy impact assessment. This finding indicates that biometric governance has developed primarily from an information-security perspective. Such development is important but incomplete because protecting a system against unauthorized access does not automatically protect individuals against excessive or disproportionate processing.

The third pattern concerns the distance between legal rights and practical usability. The PDP Law creates important rights, but only two of the 10 user participants knew a concrete procedure for requesting access to or deletion of data. This finding demonstrates that rights become weaker when users cannot identify the correct channel, understand the technical form of their biometric information, or predict the consequences of exercising those rights. Regulatory effectiveness therefore depends on converting abstract legal rights into procedures that can be used by individuals without specialized knowledge.

These findings support a multidimensional understanding of regulatory adequacy. Substantive law provides the foundation, but protection also depends on institutional capacity, procedural accessibility, and technological implementation. A strong statute cannot independently produce effective protection if privacy controls are not embedded into system design, if organizations interpret obligations inconsistently, or if users cannot exercise the rights granted to them. Regulatory adequacy should therefore be understood as the alignment of law, institutions, technology, and user experience rather than as the presence of legislation alone.

Indonesia's PDP regime has already established an essential legal foundation for this alignment. The next stage should focus on implementation through biometric-specific standards, stronger technical supervisory capacity, clearer retention and deletion requirements, auditable processor relationships, routine privacy impact assessments, and accessible mechanisms for data subject rights. Strengthening these areas would not require rejecting biometric authentication. Onesi-Ozigagun et al. (2024) show that biometric technologies can strengthen fraud prevention and trust in fintech environments, while the findings of this study demonstrate that those benefits must be accompanied by safeguards that protect individuals from disproportionate loss of control over permanent identity characteristics.

Overall, the evidence characterizes Indonesia's biometric data protection regime as normatively established, technologically developing, but procedurally and institutionally incomplete. The PDP Law has created a credible foundation for protecting biometric information, but the effectiveness of that protection will depend on how consistently legal principles are converted into system architecture, organizational procedures, regulatory supervision, and meaningful user rights. Strengthening these dimensions would allow Indonesia to maintain the security and efficiency benefits of biometric authentication while ensuring that digital innovation develops together with privacy, accountability, and effective protection of data subjects.

Conclusion

This study concludes that Indonesia's personal data protection regime has established a meaningful legal foundation for protecting biometric data in digital transactions, but its effectiveness remains uneven at the operational level. The findings show that the main weaknesses do not arise from the absence of legal recognition of biometric risks, but from gaps in meaningful consent, transparency, retention and deletion practices, third-party processing, privacy-oriented system design, institutional supervision, and the practical exercise of data subject rights. Biometric verification was often experienced by users as a technical requirement rather than an informed privacy decision, while organizational practices showed stronger maturity in cybersecurity controls than in privacy by design. These findings contribute to the literature by showing that regulatory adequacy should be assessed through the interaction of substantive law, institutional capacity, procedural accessibility, and technological implementation. The study therefore extends existing normative discussions of Indonesia's Personal Data Protection Law by demonstrating that effective biometric protection depends on how legal principles are translated into everyday organizational practices and user experiences.

The findings have practical and policy implications for regulators, financial institutions, fintech companies, technology providers, and digital platforms. Biometric governance should strengthen contextual consent, layered transparency, data minimization, defined retention periods, traceable deletion procedures, processor accountability, privacy impact assessment, and accessible mechanisms for exercising data subject rights. Regulators should also develop more specific technical and procedural guidance for high-risk biometric processing and strengthen supervisory capacity that combines legal and technological expertise. From a theoretical perspective, the study confirms the relevance of integrating a rights-based approach with privacy by design in evaluating biometric data governance. Future research should examine a wider range of sectors, biometric modalities, and institutional settings, particularly cross-border processing and emerging forms of AI-based identification, to determine whether the implementation gaps identified in this study persist across Indonesia's broader digital ecosystem.

Acknowledgements

The authors would like to thank all participants, professional informants, and relevant stakeholders who contributed their time, experiences, and perspectives to this study. The authors also appreciate the academic and institutional support that facilitated the completion of this research.

Author Contributions

Conceptualization: Ayu Mega Harahap, Juwita Hana Situmorang

Data curation: Dimas Ilyas Situmorang, Juwita Hana Situmorang

Formal analysis: Ayu Mega Harahap, Dimas Ilyas Situmorang

Investigation: Ayu Mega Harahap, Juwita Hana Situmorang, Dimas Ilyas Situmorang

Methodology: Ayu Mega Harahap, Juwita Hana Situmorang

Project administration: Ayu Mega Harahap

Supervision: Ayu Mega Harahap

Validation: Juwita Hana Situmorang, Dimas Ilyas Situmorang

Visualization: Dimas Ilyas Situmorang

Writing - original draft: Ayu Mega Harahap, Juwita Hana Situmorang, Dimas Ilyas Situmorang

Writing - review and editing: Ayu Mega Harahap, Juwita Hana Situmorang, Dimas Ilyas Situmorang

All authors contributed to the development of the manuscript, reviewed the final version, and approved its submission for publication.

Funding Statement

This research received no specific grant from any funding agency in the public, commercial, or not-for-profit sectors. The study was conducted using the authors' own resources.

Conflict of Interest

The authors declare that they have no conflict of interest related to this manuscript. The authors have no financial, professional, institutional, or personal relationships that could have influenced the research process or interpretation of the findings.

Statement on the Use of Artificial Intelligence

The authors used Claude AI, ChatGPT, DeepL, and Grammarly as supporting tools during the preparation of this manuscript for language refinement, grammatical correction, translation assistance, readability improvement, and editorial consistency. Artificial intelligence tools were not used to generate, fabricate, or manipulate research data, interview findings, or empirical evidence. All AI-assisted output was reviewed and verified by the authors, who take full responsibility for the originality, accuracy, integrity, citation verification, and final content of the manuscript.

References

Alfaaiz, M. G. (2025). Perbandingan regulasi perlindungan data pribadi antara Indonesia dan Singapura dalam konteks kasus Worldcoin. Journal Equitable, 10(3). https://doi.org/10.37859/jeq.v10i3.9241

Arman, S. M., Yang, T., Shahed, S., Al Mazroa, A., Attiah, A., & Mohaisen, L. (2024). A comprehensive survey for privacy-preserving biometrics: Recent approaches, challenges, and future directions. Computers, Materials & Continua, 78(2), 2087–2110. https://doi.org/10.32604/cmc.2024.047870

Bezas, K., & Filippidou, F. (2023). Anti-spoofing methods in face recognition. The Indonesian Journal of Computer Science, 12(3). https://doi.org/10.33022/ijcs.v12i3.3198

Beya, B., Hanslo, M., & Hanslo, R. (2024). The face of surveillance: A systematic review of ethical and legal implications in public facial recognition. Proceedings of the International Conference on Intelligent and Innovative Computing Applications. https://doi.org/10.59200/iconic.2024.010

Budiman, R. (2023). The development of personal data protection law in Indonesia: Challenges and prospects for the implementation of Law No. 27 of 2022. Jurnal Smart Hukum, 2(1), 24–36. https://doi.org/10.55299/jsh.v2i1.1352

Darnela, L., & Rusdiana, E. (2025). Public legal awareness and the effectiveness of Indonesia's Personal Data Protection Law: Bridging normative framework and privacy paradox. Supremasi Hukum: Jurnal Kajian Ilmu Hukum, 14(1), 1–28. https://doi.org/10.14421/2gg2rp29

DP, A. A., Mamonto, A. A. N., Amiq, B., Rambe, K. M., & Syahputra, A. R. (2023). Facial recognition technology: A multinational analysis of regulatory framework, ethics, and legal implications in security and privacy. International Journal of Science and Society, 5(4), 498–510. https://doi.org/10.54783/ijsoc.v5i4.808

Fitriyanti, F., Devty, S., Putri, S., & Thora, R. E. (2024). Securing personal data in e-KYC: Vital for digital economy growth. Diponegoro Law Review, 9(1), 104–120. https://doi.org/10.14710/dilrev.9.1.2024.104-120

Girsang, S. Y. B. (2024). Pentingnya regulasi khusus sistem face recognition technology sebagai produk artificial intelligence dalam peningkatan keamanan dan penegakan hukum di Indonesia. Nommensen Journal of Legal Opinion, 5(2), 86–98. https://doi.org/10.51622/njlo.v5i2.1817

Gunawan, I. (2024). Upaya preventif dan represif dalam penanggulangan kebocoran data pada penyelenggaraan pinjaman online. Officium Notarium, 4(1), 25–49. https://doi.org/10.20885/JON.vol4.iss1.art3

Günay, B. (2023). Biometrische Daten aus der Perspektive der DSGVO. Datenschutz und Datensicherheit, 47(2), 96–99. https://doi.org/10.1007/s11623-023-1724-x

Guo, C., You, L., Li, X., Hu, G., Wang, S., & Cao, C. (2024). A novel biometric authentication scheme with privacy protection based on SVM and ZKP. Computers & Security, 144, 103995. https://doi.org/10.1016/j.cose.2024.103995

Gusnan, Z. K., & Utomo, R. G. (2024). Factors affecting user's acceptance of adopting biometrics technologies using the TAM model. Jurnal Teknik Informatika, 5(4). https://doi.org/10.52436/1.jutif.2024.5.4.2249

Hasan, M. R., Guest, R. M., & Deravi, F. (2023). Presentation-level privacy protection techniques for automated face recognition: A survey. ACM Computing Surveys, 56(13s), Article 286. https://doi.org/10.1145/3583135

Judijanto, L., Solapari, N., & Putra, I. (2024). An analysis of the gap between data protection regulations and privacy rights implementation in Indonesia. The Easta Journal Law and Human Rights, 3(1), 20–29. https://doi.org/10.58812/eslhr.v3i01.351

Karnedi, G., & Alam, R. G. (2025). Evaluasi regulasi perlindungan data pribadi di Indonesia: Komparasi dengan GDPR Uni Eropa. El-Mujtama: Jurnal Pengabdian Masyarakat, 5(3), 610–622. https://doi.org/10.47467/elmujtama.v5i3.8549

Kavoliūnaitė-Ragauskienė, E. (2024). Right to privacy and data protection concerns raised by the development and usage of face recognition technologies in the European Union. Journal of Human Rights Practice, 16(2), 658–674. https://doi.org/10.1093/jhuman/huad065

Kumalasari, R. A. D., Rahardjo, K., Kusumawati, A., & Sunarti. (2024). Biometric-based self-service technology adoption by older adult: Empirical evidence from pension fund sector in Indonesia. Cogent Business & Management, 11(1), 2325543. https://doi.org/10.1080/23311975.2024.2325543

Kusyanti, A., Catherina, H. P. A., Effendrik, P., Santoso, N., & Ekowati, N. S. (2024). "Risky or trustworthy?": User behavior towards biometric authentication method. Procedia Computer Science, 234, 428–435. https://doi.org/10.1016/j.procs.2024.03.024

Melzi, P., Rathgeb, C., Tolosana, R., Vera-Rodriguez, R., & Busch, C. (2024). An overview of privacy-enhancing technologies in biometric recognition. ACM Computing Surveys, 56(12), Article 310, 1–28. https://doi.org/10.1145/3664596

Mordini, E. (2023). Biometric privacy protection: What is this thing called privacy? IET Biometrics, 12. https://doi.org/10.1049/bme2.12111

Natamiharja, R., & Setiawan, I. (2024). Guarding privacy in the digital age: A comparative analysis of data protection strategies in Indonesia and France. Jambe Law Journal, 7(1), 233–251. https://doi.org/10.22437/home.v7i1.349

Onesi-Ozigagun, O., Ololade, Y. J., Eyo-Udo, N. L., & Ogundipe, D. O. (2024). AI-driven biometrics for secure fintech: Pioneering safety and trust. International Journal of Engineering Research Updates, 6(2). https://doi.org/10.53430/ijeru.2024.6.2.0023

Priyantiwi, R. D., & Hufron. (2025). Ensuring legal protection of personal data in Indonesia's digital identity system. Justitia Jurnal Hukum, 9(2). https://doi.org/10.30651/justitia.v9i2.27113

Putri, D. T. (2025). Regulating digital privacy in Indonesia: The practice of data subject rights and controller duties in the FotoYu app. Istinbath: Jurnal Hukum, 22(2), 230–262. https://doi.org/10.32332/istinbath.v22i02.art01

Qandeel, M. (2024). Facial recognition technology: Regulations, rights and the rule of law. Frontiers in Big Data, 7, 1354659. https://doi.org/10.3389/fdata.2024.1354659

Rahman, F., & Mulyani, C. K. (2025). Minimising unnecessary restrictions on cross-border data flows? Indonesia's position and challenges post personal data protection act enactment. International Review of Law, Computers & Technology, 39(2), 281–300. https://doi.org/10.1080/13600869.2024.2359901

Razi, F., Tuasikal, H., & Markus, D. P. (2024). Implementation and challenges of the Personal Data Protection Law in Indonesia. Jurnal Indonesia Sosial Teknologi, 5(12), 6559–6565. https://doi.org/10.59141/jist.v5i12.1285

Salko, M., Firc, A., & Malinka, K. (2024). Security implications of deepfakes in face authentication. Proceedings of the 39th ACM/SIGAPP Symposium on Applied Computing, 1376–1384. https://doi.org/10.1145/3605098.3635953

Sembiring, P. E., Ramli, A. M., & Rafianti, L. (2024). Implementasi desain privasi sebagai pelindungan privasi atas data biometrik. Veritas et Justitia, 10(1), 127–152. https://doi.org/10.25123/vej.v10i1.7622

Sriman, J., Thapar, P., Alyas, A. A., & Singh, U. (2024). Unlocking security: A comprehensive exploration of biometric authentication techniques. 2024 14th International Conference on Cloud Computing, Data Science & Engineering (Confluence). https://doi.org/10.1109/CONFLUENCE60223.2024.10463322

Syailendra, M. R., Lie, G., & Sudiro, A. (2024). Personal data protection law in Indonesia: Challenges and opportunities. Indonesia Law Review, 14(2), Article 4. https://doi.org/10.15742/ilrev.v14n2.4

Taufiq, M., & Kenyo, A. S. (2025). The legal protection of personal data in the digital era: A comparative study of Indonesian law and the GDPR. International Journal of Business, Law, and Education, 6(2), 1260–1268. https://doi.org/10.56442/ijble.v6i2.1178

Vásquez Cerna, J. J., Solano Quincho, L. M., & Mendoza de los Santos, A. C. (2023). La vulnerabilidad de las tecnologías biométricas en la autenticación. Ingeniería Investiga, 5, e866. https://doi.org/10.47796/ing.v5i0.866

Wang, X., Wu, Y. C., Zhou, M., & Fu, H. (2024). Beyond surveillance: Privacy, ethics, and regulations in face recognition technology. Frontiers in Big Data, 7, 1337465. https://doi.org/10.3389/fdata.2024.1337465

Yang, W., Wang, S., Cui, H., Tang, Z., & Li, Y. (2023). A review of homomorphic encryption for privacy-preserving biometrics. Sensors, 23(7), 3566. https://doi.org/10.3390/s23073566

Yusliwidaka, A., Abqa, M. A. R., & Wardana, K. A. (2024). A discourse of personal data protection: How Indonesia responsible under domestic and international law? Pandecta Research Law Journal, 19(2), 453–482. https://doi.org/10.15294/pandecta.v19i2.13279

Zuwanda, Z. S., Judijanto, L., Khuan, H., & Triyantoro, A. (2024). Normative study of Law No. 27 of 2022 on the protection of personal data and its impact on the fintech industry in

Indonesia. West Science Law and Human Rights, 2(4), 421–428. https://doi.org/10.58812/wslhr.v2i04.1367