

ISSN 2797-8508 (Print)
ISSN 2807-8330 (Online)

VOL. 5 NO. 1, JAN-JUNE (2025)

Saran Perujukan

How to cite:

Rahmayani, Chanidia., (2025). Consent or Coercion? A Comparative Legal Analysis of Biometric Data Practices in Digital Banking Systems *Ikatan Penulis Mahasiswa Hukum Indonesia Law Journal*, 5 (1) 103-116. <https://doi.org/10.15294/ipmhi.v5i1.28731>


© 2022 Authors. This work is licensed under a [Attribution-NonCommercial-ShareAlike 4.0 International \(CC BY-NC-SA 4.0\)](https://creativecommons.org/licenses/by-nc-sa/4.0/). All writings published in this journal are personal views of the authors and do not represent the views of this journal and the author's affiliated institutions. This title has been indexed by [Google Scholar](https://scholar.google.com/)



Consent or Coercion? A Comparative Legal Analysis of Biometric Data Practices in Digital Banking Systems

Chanidia Ari Rahmayani.¹ 

¹ Faculty of Law, Universitas Negeri Semarang

 Correspondent email: chanidia@mail.unnes.ac.id

Abstract *The digital revolution in the financial sector has accelerated the adoption of biometric technology as a method of authentication, offering greater security and efficiency than traditional password- or PIN-based systems. Biometric technology relies on unique physical or behavioral characteristics—such as fingerprints, facial patterns, and voice recognition—making it highly resistant to forgery. However, the use of biometric data presents a significant paradox: while it enhances security, it also poses serious risks to personal privacy. Because biometric data is immutable, any compromise can result in permanent and irreversible consequences. Indonesia has responded to these challenges through the enactment of Law No. 27 of 2022 on Personal Data Protection (PDP Law), which classifies biometric data as specific personal data that requires explicit, written, and revocable consent. Despite the existence of this legal framework, implementation remains difficult due to the absence of sector-specific regulations and limited regulatory oversight. In comparison, the European Union’s General Data Protection Regulation (GDPR) sets a high standard for biometric data protection, emphasizing explicit consent, data minimization, and strict enforcement mechanisms. The United States follows a sectoral approach, with state-level regulations such as Illinois’ Biometric Information Privacy Act (BIPA) imposing*

stringent requirements and significant legal liabilities. A key concern in the banking sector is whether the consent obtained from consumers truly meets legal standards, particularly given the imbalance of power between financial institutions and users. This study employs a normative juridical and comparative legal approach to analyze the regulatory frameworks of Indonesia, the European Union, and the United States. It identifies best practices and offers recommendations for improving the protection of biometric data in the banking sector.

Keywords *Personal Data Privacy, Biometric, Technology Law*

A. Introduction

The digital revolution in the financial sector has been marked by the massive adoption of biometric technology as an authentication method, which is considered more secure and efficient than traditional systems based on passwords or PINs. In the context of Indonesian banking, the adoption of biometric technology has experienced exponential growth, with major banks such as Bank Central Asia (BCA), Bank Negara Indonesia (BNI), and Bank Rakyat Indonesia (BRI) integrating biometric systems into their mobile banking services¹. Visa Survey conducted in 2022 as cited in Francisco Liébana-Cabanillas et al, *Biometric M-Payment system: A multi-analytical approach to determining use intention*, revealed that 86% of consumers are interested in using biometrics to authenticate their identity for making payments. The majority, 70%, agree that biometrics are easier to use, whereas 46% believe that biometric systems are more secure than passwords or PINs².

Biometric technology in banking leverages individual's unique characteristics such as fingerprints, facial patterns, retinal scans, and voice patterns for identification and authentication purposes. The strength of this technology its uniqueness and resistance to forgery, offering a higher level of security compared to conventional methods³. However, the implementation of biometric technology in the banking sector presents a fundamental paradox between security and privacy. The "privacy paradox" highlights the contradiction in how users interact with technology: they freely distribute personal information and images while simultaneously worrying more about privacy and security issues⁴. Behind the

¹ Otoritas Jasa Keuangan, "Supporting Financial Inclusion for MSMEs through FinTech" (Jakarta, 2020).

² Francisco Liébana-Cabanillas et al., "Biometric M-Payment Systems: A Multi-Analytical Approach to Determining Use Intention," *Information & Management* 61, no. 2 (March 2024): 103907, <https://doi.org/10.1016/j.im.2023.103907>; Otoritas Jasa Keuangan, "Supporting Financial Inclusion for MSMEs through FinTech."

³ Waheeduddin Khadri Syed et al., "Biometric Authentication Systems in Banking: A Technical Evaluation of Security Measures," in *2024 IEEE 3rd World Conference on Applied Intelligence and Computing (AIC)* (IEEE, 2024), 1331–36, <https://doi.org/10.1109/AIC61668.2024.10731026>.

⁴ Monika Taddicken, "The 'Privacy Paradox' in the Social Web: The Impact of Privacy Concerns, Individual Characteristics, and the Perceived Social Relevance on Different Forms of Self-Disclosure*," *Journal of*

sophistication of this technology there is significant legal complexity concerning the protection of personal data, particularly in the context of the validity of the consent given by data subjects⁵. Biometric data possess unique, immutable characteristics that cannot be changed over an individual's lifetime⁶. Consequently, if such data are leaked or misused, the resulting impact is permanent and irreversible. Unlike passwords, which can be changed, compromised fingerprints or iris patterns cannot be “reset” or updated⁷.

Indonesia has responded to this challenge through the enactment of Law No. 27 of 2022 on Personal Data Protection (PDP Law), which explicitly classifies biometric data as specific personal data requiring heightened protection. This legislation marks a significant milestone in the evolution of data privacy law in Indonesia⁸. However, its implementation within the banking sector continues to face numerous technical and practical challenges. The Financial Services Authority (Otoritas Jasa Keuangan, OJK), as the financial sector regulator, has demonstrated a commitment to integrating biometric technology into banking systems, even proposing access to biometric data held by the Directorate General of Population and Civil Registration to support the development of digital banking services⁹.

At the global level, biometric regulations vary significantly across jurisdictions, reflecting differing approaches to balancing technological innovation with privacy protection. The European Union, through the General Data Protection Regulation (GDPR), has established a gold standard for biometric data protection, emphasizing the principles of explicit consent and data subject rights¹⁰. According to GDPR article 9, biometric data holds a special status as a form of “special category data” or sensitive data that requires extra protection. Its permanent and irreplaceable nature fundamentally distinguishes it from conventional personal data, such as passwords, which can be changed in the event of a breach. When biometric data is leaked or

Computer-Mediated Communication 19, no. 2 (January 1, 2014): 248–73, <https://doi.org/10.1111/jcc4.12052>.

⁵ Akhmad Afridho Wira P, Fitria Esfandiari, and Wasis Wasis, “Juridical Analysis of Legal Protection of Personal Data in Terms of Legal Certainty,” *Indonesia Law Reform Journal* 3, no. 1 (March 31, 2023): 96–108, <https://doi.org/10.22219/ilrej.v3i1.23840>.

⁶ Dario Salice and Jennifer Salice, *Foundations and Opportunities of Biometrics* (Berkeley, CA: Apress, 2024), <https://doi.org/10.1007/979-8-8688-0509-7>.

⁷ Anthony Paul, “Biometric Data Security: Balancing Convenience with Privacy,” May 11, 2024.

⁸ Patricia Edina Sembiring, Ahmad M. Ramli, and Laina Rafianti, “IMPLEMENTASI DESAIN PRIVASI SEBAGAI PELINDUNGAN PRIVASI ATAS DATA BIOMETRIK,” *Veritas et Justitia* 10, no. 1 (June 29, 2024): 127–52, <https://doi.org/10.25123/vej.v10i1.7622>.

⁹ Aziz, “OJK Minta Ditjen Dukcapil Buka Data Biometrik Untuk Perbankan,” *Pasar Dana*, <https://pasardana.id/news/2018/10/20/ojk-minta-ditjen-dukcapil-buka-data-biometrik-untuk-perbankan/>, 2018.

¹⁰ Iqbal Prasetya, “Biometric Security vs. Privacy Rights: A Comparative Study of Global Privacy Laws in the Biometric Era,” *SSRN Electronic Journal*, 2025, <https://doi.org/10.2139/ssrn.5013459>.

misused, the consequences are irreversible and can permanently threaten an individual's privacy¹¹.

The United States adopts a more fragmented approach, with state-level regulations such as the Illinois Biometric Information Privacy Act (BIPA) offering stringent protections¹².

A fundamental question arises: does the consent provided in biometric banking practices truly meet the legal standards of data protection? This issue is further complicated by the inherent power imbalance in the relationship between financial institutions and consumers, where access to banking services often constitutes an essential, unavoidable need.

This study aims to conduct a comparative analysis of three key jurisdictions in biometric data protection: Indonesia with its Law No. 27 of 2022 on Personal Data Protection (PDP Law), the European Union with the General Data Protection Regulation (GDPR), and the United States with its sectoral regulatory model. Through this comparative approach, the study seeks to identify the strengths and weaknesses of each legal system and provide recommendations for improving biometric data protection mechanisms within the banking sector.

B. Method

This research conducted as normative juridical approach combined with a descriptive-comparative analytical method to examine the regulatory framework governing the storage of biometric data in banking services. The normative juridical approach is deemed appropriate as the research focuses on the analysis of legal norms, statutory provisions, and their implementation within the context of biometric data protection in the banking sector. This methodological framework enables the researcher to critically examine the applicable legal provisions, identify normative gaps, and propose reformative recommendations grounded in prevailing legal principles.

The legal materials utilized in this research comprise primary and secondary sources. Primary legal materials include statutory instruments such as Law No. 27 of 2022 on Personal Data Protection and Law No. 1 of 2024 on Electronic Information and Transactions. In addition, the study analyzes international regulatory frameworks, including the European Union's General Data Protection Regulation (GDPR), the Illinois Biometric Information Privacy Act (BIPA) of the United States.

¹¹ Meng Wang et al., "Identifying Personal Physiological Data Risks to the Internet of Everything: The Case of Facial Data Breach Risks," *Humanities and Social Sciences Communications* 10, no. 1 (May 8, 2023): 216, <https://doi.org/10.1057/s41599-023-01673-3>.

¹² Carmen Sobczak, "BIPA and Article III Standing: Are Notice and Consent More Than 'Bare Procedural' Rights?," *Berkeley Technology Law Journal* 35, no. 4 (2020).

The secondary legal materials from national and international legal journals, legal monographs, research reports from academic institutions, and publications by international organizations. Particular emphasis is placed on scholarly literature addressing the application of biometric technologies in the financial sector, the protection of personal data, and comparative regulatory analysis.

Data collection was conducted through doctrinal legal research, primarily involving literature review across academic journal databases, legal repositories, and official publications issued by governmental and international regulatory. The analysis also incorporates a review of policy documents from the Financial Services Authority (Otoritas Jasa Keuangan, OJK), Bank Indonesia, and financial regulators from comparator jurisdictions. The analytical process was undertaken using a combination of content analysis and comparative legal analysis. Content analysis was employed to identify and classify legal provisions pertinent to biometric data protection, while comparative analysis served to evaluate the regulatory approaches of different jurisdictions and to identify best practices that could be adopted within the Indonesian legal framework.

C. Result and Discussion

1. Biometric and Data Privacy Regulations

Europe Union

The General Data Protection Regulation (GDPR) establishes legal framework for the processing of biometric data, categorizing it as a “special category of personal data,”¹³ which is generally prohibited unless specific legal exemptions apply. Article 9 of the GDPR explicitly provides that the processing of biometric data for the purpose of uniquely identifying an individual is permissible only with the data subject’s *explicit consent* or on the basis of substantial public interest.¹⁴

The GDPR sets a high threshold for consent, requiring it to be clear, specific, and unambiguous. In the context of the banking sector, this means that financial institutions cannot rely on general or bundled forms of consent; instead, they must obtain consent that is expressly granted for each specific purpose involving biometric data processing.

Furthermore, the GDPR enforces the principles of data minimization and purpose limitation, which restrict the collection and use of biometric data to what is strictly necessary and for clearly defined, legitimate purposes. Financial institutions are thus obliged to assess whether the processing of biometric data is truly necessary and proportionate to the intended objectives.

¹³ Anneliese Roos, “An Evaluation of Selected ‘Content Principles,’” *The Comparative and International Law Journal of Southern Africa* 53, no. 3 (2020): 1–37, <https://www.jstor.org/stable/27327972>.

¹⁴ Edward S Dove and Jiahong Chen, “What Does It Mean for a Data Subject to Make Their Personal Data ‘Manifestly Public’? An Analysis of GDPR Article 9(2)(e),” *International Data Privacy Law* 11, no. 2 (August 6, 2021): 107–24, <https://doi.org/10.1093/idpl/ipab005>.

The GDPR also guarantees a comprehensive set of rights for data subjects, including the right of access, rectification, erasure (the "right to be forgotten"), restriction of processing, data portability, and the right to object. However, the application of these rights in the context of biometric data presents significant technical challenges, particularly with regard to erasure, since biometric identifiers are often embedded in complex security systems.

Compliance with the GDPR is backed by strong enforcement measures, including administrative fines of up to €20 million or 4% of the global annual turnover, whichever is higher. These stringent penalties serve as a powerful incentive for financial institutions to adhere strictly to GDPR requirements.

Indonesia

Indonesia's Personal Data Protection Law (PDP Law), enacted through Law No. 27 of 2022, recognizes biometric data as a form of "specific personal data" requiring heightened protection. Biometric data under the PDP Law refers to information related to an individual's physical, physiological, or behavioural characteristics that can be used for unique identification, including facial recognition and fingerprint data.

The law requires that consent be explicit, written, and revocable. Article 20(2)(a) mandates that personal data may only be processed with the valid and explicit consent of the data subject for one or more specific purposes as communicated by the data controller.

The PDP Law incorporates internationally recognized principles of data processing, including limitations on purpose, legality, and transparency. Article 34 requires data controllers to conduct a Data Protection Impact Assessment (DPIA) for processing activities deemed to pose a high risk, such as the handling of biometric data.

Nevertheless, several challenges have emerged in the implementation of the PDP Law. First, the absence of sector-specific implementing regulations, particularly for the financial services industry, has led to legal uncertainty. Secondly, the regulatory oversight mechanism remains weak, as the dedicated data protection authority mandated by the law is not yet fully operational.

Studies show that many banks in Indonesia have not fully complied with Articles 20 and 21 of the PDP Law. These institutions often fail to obtain explicit consent from their customers and do not provide the detailed information required by law, such as the legal basis for processing, the purpose, types of data collected, retention periods, and the rights of the data subjects.

Compared to the GDPR, the PDP Law has relatively limited enforcement mechanisms. The maximum administrative fine is only 2% of annual revenue significantly lower than that imposed by the GDPR. Furthermore, oversight

currently relies on the Ministry of Communication and Digital (KOMDIGI) which has limited capacity and authority.

United States

The United States adopts a sector-specific approach to data protection and does not have a comprehensive federal privacy law equivalent to the GDPR. Biometric data is primarily regulated at the state level, with the Illinois Biometric Information Privacy Act (BIPA) being the most comprehensive and widely referenced legislation.

BIPA imposes strict requirements on the collection, use, and storage of biometric information. It requires organizations to provide prior notice and obtain written consent before collecting biometric data, prohibits the sale of such data, and mandates the implementation of reasonable security measures for its storage and protection.¹⁵

The jurisprudential evolution of BIPA has significantly amplified its regulatory impact through expansive judicial interpretations that have established stringent liability standards for corporate defendants. The case of *Facebook vs. class action plaintiffs* became a landmark case in the enforcement of BIPA. Facebook ultimately agreed to pay a \$650 million settlement over allegations that it violated BIPA through its face-tagging feature, which collected and processed facial recognition data without explicit written consent. This case highlights the significant potential financial exposure for companies that breach biometric data protection regulations¹⁶.

JPMorgan Chase also faced a class action lawsuit over its use of Gatekeeper technology developed by Microsoft subsidiary Nuance Communications for voice authentication without obtaining explicit consent from customers¹⁷. This case illustrates how financial institutions in the U.S. may face liability for using biometric technology in fraud prevention and customer authentication.

The "notice and choice" approach, which dominates in the U.S., is considered insufficient by many scholars and legal practitioners. This model assumes that consumers can make informed decisions based on provided privacy notices, but in reality, most consumers do not read or understand the complex and lengthy privacy policies. This evolution reflects the ongoing challenge faced by policymakers in balancing technological innovation with privacy protection, and Illinois's

¹⁵ Youna Jung and Ethan D. Virgil, "Analysis of Legislative Framework Governing Biometric Data," *Procedia Computer Science* 241 (2024): 48–55, <https://doi.org/10.1016/j.procs.2024.08.009>.

¹⁶ Tony Bitziosis, "Facebook Returns with Increased Settlement in BIPA Case," Facebook Returns with Increased Settlement in BIPA Case, July 23, 2020, <http://idtechwire.com/facebook-returns-increased-settlement-bipa-case-072301/>.

¹⁷ Corrado Rizzi, "Chase Bank Does Not Secure Consent Before Capturing, Examining Calif. Callers' Voiceprints, Class Action Says," *ClassAction.Org*, September 30, 2022.

experience will likely continue to inform the development of biometric regulation at both federal and state levels across the United States¹⁸.

2. Consent and Coercion in Data Protection Law

Definition and Concept of Consent in Data Protection Law

The concept of consent constitutes one of the fundamental pillars of modern personal data protection law¹⁹. Under the General Data Protection Regulation (GDPR), consent is defined as "any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her"²⁰. This definition highlights four key elements: freely given, specific, informed, and unambiguous.

Indonesia's Personal Data Protection Law (PDP Law) adopts a similar approach, defining consent as "a written or recorded statement provided consciously and clearly by the Personal Data Subject to allow the processing of their personal data". Although the terminology differs, the substance of this definition aligns with the international standards set by the GDPR.

In the privacy law literature, consent is conceptualized as a mechanism that enables data subjects to exercise the primary purpose of data protection law: informational self-determination. This concept grants individuals control over how their personal data is collected, processed, and used by others.

Power Imbalance Theory in Financial Institution–Consumer Relations

The theory of power imbalance provides an understanding the dynamics between financial institutions and consumers in the context of biometric consent²¹. This imbalance manifests in several dimensions: first, asymmetric information, where financial institutions possess significantly greater technical and legal knowledge than the average consumer; second, economic dependence, in which consumers rely on banking services to fulfill essential financial needs; and third, a disparity in bargaining power that places consumers in a take-it-or-leave-it position²².

Within the banking sector, such power imbalances may lead to situations where the consent provided by consumers does not meet the "freely given" standard required

¹⁸ Emma Graham, "Burdened by Bipa: Balancing Consumer Protection and the Economic Concerns of Businesses," *University of Illinois Law Review* 2022, no. 2 (2022): 929–61.

¹⁹ Manasvi Aiyer and Beni Chugh, "Designing a Consent Artefact for Digital Financial Services to Cater to Constrained Users," 2021.

²⁰ Ben Wolford, "What Are the GDPR Consent Requirement?," GDPR EU, <https://gdpr.eu/gdpr-consent-requirements/>, n.d.

²¹ Neil Richards and Woodrow Hartzog, "The Pathologies of Digital Consent," *Washington University Law Review*, Available at: https://openscholarship.wustl.edu/law_lawreview/Vol96/Iss6/11_96_no_06 (2019).

²² *Ibid.*

by data protection regulations²³. The urgency to access banking services often exerts pressure on consumers to consent to the use of biometric data, thereby compromising the voluntariness of their consent.

Coerced Consent and Privacy Fatigue

Coerced consent refers to situations in which individuals provide consent not as an expression of free will, but due to a lack of practical alternatives²⁴. In the context of digital services, including biometric banking, coerced consent arises when access to essential services is conditioned upon acceptance of data collection and processing practices that users may otherwise reject²⁵.

Privacy fatigue refers to a condition where individuals feel worn out by the constant exposure to consent requests, leading them to approve data collection or processing without fully considering the implications. This tendency is made worse by the complicated and technical language often found in privacy policies and terms of service, which can be difficult for most users to understand. As people encounter numerous consent prompts throughout their daily online activities, they may develop a habit of automatically accepting them, often without reading or fully grasping what they are agreeing to²⁶.

In the context of biometric banking, privacy fatigue may result in consent that fails to meet the standard of "informed consent" because data subjects do not fully grasp the long-term risks and consequences associated with sharing their biometric data²⁷. This poses a significant concern, given the irreversible nature of compromised biometric identifiers.

An assessment of the validity of consent in biometric banking authentication must consider the structural power imbalance inherent in the relationship between financial institutions and consumers. In practice, the consent provided by customers often fails to meet the criteria of being "freely given" due to several factors: first, the essential nature of banking services, which means that refusing to consent can result in exclusion from the financial system; second, the lack of meaningful alternatives that would allow consumers to access comparable services without submitting biometric data; and third, significant information asymmetry between institutions

²³ Ibid.

²⁴ Tom Dougherty, "Coerced Consent with an Unknown Future*," *Philosophy and Phenomenological Research* 103, no. 2 (September 17, 2021): 441–61, <https://doi.org/10.1111/phpr.12718>.

²⁵ Leon Trakman, Robert Walters, and Bruno Zeller, "Digital Consent and Data Protection Law – Europe and Asia-Pacific Experience," *Information & Communications Technology Law* 29, no. 2 (May 3, 2020): 218–49, <https://doi.org/10.1080/13600834.2020.1726021>.

²⁶ Xuemin Yang, Hong Mei, and Yueping Zheng, "Understanding the Antecedents of Privacy Fatigue in Facial Recognition-Based m-Gov Services: An Empirical Study from China," *Government Information Quarterly* 40, no. 3 (June 2023): 101827, <https://doi.org/10.1016/j.giq.2023.101827>.

²⁷ Xiaodong Ding and Hao Huang, "For Whom Is Privacy Policy Written? A New Understanding of Privacy Policies," *Computer Law & Security Review* 55 (November 2024): 106072, <https://doi.org/10.1016/j.clsr.2024.106072>.

and consumers regarding the risks and consequences of biometric data processing²⁸.

The principle of proportionality requires that biometric data processing must be proportionate to the legitimate aims being pursued. In the banking context, the use of biometric data for fraud prevention and customer authentication can be considered legitimate; however, the scope and duration of processing must be limited to what is strictly necessary.

The fairness principle also requires consideration of the reasonable expectations of consumers and the potential adverse effects of processing. The use of biometric data for purposes beyond the original consent such as customer profiling or marketing may violate the fairness principle, even if technically covered by broad consent language.

D. Conclusion

A comparative analysis of the GDPR, PDP Law, and BIPA reveals that, although biometric technology in the banking sector offers significant benefits, particularly in terms of security and convenience its current implementation continues to face serious challenges in ensuring the validity of consent in accordance with modern data protection standards.

Across all the three law, the fundamental issue of consent validity in the context of essential services remains unresolved. Current consent models, which rely heavily on individual choice, often fail to account for structural power imbalances and the lack of meaningful alternatives that characterize consumer-bank relationships.

The intersection of consent fatigue, power imbalance, and biometric data in digital banking creates complex regulatory challenges requiring innovative solutions. Comparative analysis shows no single perfect approach, with each jurisdiction facing trade-offs between innovation, security, and privacy protection.

The EU's rights-based approach offers the strongest protection but faces implementation hurdles that may hinder financial innovation. The U.S.'s market-based approach provides flexibility but inconsistent protections that may disadvantage vulnerable consumers. Indonesia's developing framework presents opportunities to learn from international experiences while crafting context-appropriate solutions.

Future research should focus on developing empirical measures for consent burden assessment, evaluating regulatory effectiveness, and designing technology-enabled solutions for meaningful consent in biometric banking. Integrating

²⁸ Manasvi Aiyer and Beni Chugh, "Designing a Consent Artefact for Digital Financial Services to Cater to Constrained Users," 2021.

behavioral economics insights into regulatory design can help create more effective frameworks accounting for cognitive limitations in consent decision-making.

Ultimately, addressing biometric consent challenges requires reconceptualizing from an individual responsibility model to a shared responsibility framework recognizing structural inequalities and institutional power in financial ecosystems. Only through such a comprehensive approach can the benefits of biometric technology in banking be enjoyed while protecting fundamental rights and human dignity.

E. Reference

- Aiyer, Manasvi, and Beni Chugh. "Designing a Consent Artefact for Digital Financial Services to Cater to Constrained Users," 2021.
- . "Designing a Consent Artefact for Digital Financial Services to Cater to Constrained Users," 2021.
- Aziz. "OJK Minta Ditjen Dukcapil Buka Data Biometrik Untuk Perbankan." *Pasar Dana*, <https://pasardana.id/news/2018/10/20/ojk-minta-ditjen-dukcapil-buka-data-biometrik-untuk-perbankan/>, 2018.
- Bitziosis, Tony. "Facebook Returns with Increased Settlement in BIPA Case." *Facebook Returns with Increased Settlement in BIPA Case*, July 23, 2020. <http://idtechwire.com/facebook-returns-increased-settlement-bipa-case-072301/>.
- Ding, Xiaodong, and Hao Huang. "For Whom Is Privacy Policy Written? A New Understanding of Privacy Policies." *Computer Law & Security Review* 55 (November 2024): 106072. <https://doi.org/10.1016/j.clsr.2024.106072>.
- Dougherty, Tom. "Coerced Consent with an Unknown Future*." *Philosophy and Phenomenological Research* 103, no. 2 (September 17, 2021): 441–61. <https://doi.org/10.1111/phpr.12718>.
- Dove, Edward S, and Jiahong Chen. "What Does It Mean for a Data Subject to Make Their Personal Data 'Manifestly Public'? An Analysis of GDPR Article 9(2)(e)." *International Data Privacy Law* 11, no. 2 (August 6, 2021): 107–24. <https://doi.org/10.1093/idpl/ipab005>.
- Graham, Emma. "Burdened by Bipa: Balancing Consumer Protection and the Economic Concerns of Businesses." *University of Illinois Law Review* 2022, no. 2 (2022): 929–61.
- Jung, Youna, and Ethan D. Virgil. "Analysis of Legislative Framework Governing Biometric Data." *Procedia Computer Science* 241 (2024): 48–55. <https://doi.org/10.1016/j.procs.2024.08.009>.
- Liébana-Cabanillas, Francisco, Zoran Kalinic, Francisco Muñoz-Leiva, and Elena Higuera-Castillo. "Biometric M-Payment Systems: A Multi-Analytical Approach to Determining Use Intention." *Information & Management* 61, no. 2 (March 2024): 103907. <https://doi.org/10.1016/j.im.2023.103907>.
- Otoritas Jasa Keuangan. "Supporting Financial Inclusion for MSMEs through FinTech." Jakarta, 2020.

- P, Akhmad Afridho Wira, Fitria Esfandiari, and Wasis Wasis. "Juridical Analysis of Legal Protection of Personal Data in Terms of Legal Certainty." *Indonesia Law Reform Journal* 3, no. 1 (March 31, 2023): 96–108. <https://doi.org/10.22219/ilrej.v3i1.23840>.
- Paul, Anthony. "Biometric Data Security: Balancing Convenience with Privacy," May 11, 2024.
- Prasetya, Iqbal. "Biometric Security vs. Privacy Rights: A Comparative Study of Global Privacy Laws in the Biometric Era." *SSRN Electronic Journal*, 2025. <https://doi.org/10.2139/ssrn.5013459>.
- Richards, Neil, and Woodrow Hartzog. "The Pathologies of Digital Consent." *Washington University Law Review*, Available at: https://Openscholarship.Wustl.Edu/Law_lawreview/Vol96/Iss6/1196, no. 06 (2019).
- Rizzi, Corrado. "Chase Bank Does Not Secure Consent Before Capturing, Examining Calif. Callers' Voiceprints, Class Action Says." *ClassAction.Org*, September 30, 2022.
- Roos, Anneliese. "An Evaluation of Selected Content Principles?" *The Comparative and International Law Journal of Southern Africa* 53, no. 3 (2020): 1–37. <https://www.jstor.org/stable/27327972>.
- Salice, Dario, and Jennifer Salice. *Foundations and Opportunities of Biometrics*. Berkeley, CA: Apress, 2024. <https://doi.org/10.1007/979-8-8688-0509-7>.
- Sembiring, Patricia Edina, Ahmad M. Ramli, and Laina Rafianti. "IMPLEMENTASI DESAIN PRIVASI SEBAGAI PELINDUNGAN PRIVASI ATAS DATA BIOMETRIK." *Veritas et Justitia* 10, no. 1 (June 29, 2024): 127–52. <https://doi.org/10.25123/vej.v10i1.7622>.
- Sobczak, Carmen. "BIPA and Article III Standing: Are Notice and Consent More Than 'Bare Procedural' Rights?" *Berkeley Technology Law Journal* 35, no. 4 (2020).
- Syed, Waheeduddin Khadri, Abubakar Mohammed, Janamolla Kavitha Reddy, and S. Dhanasekaran. "Biometric Authentication Systems in Banking: A Technical Evaluation of Security Measures." In *2024 IEEE 3rd World Conference on Applied Intelligence and Computing (AIC)*, 1331–36. IEEE, 2024. <https://doi.org/10.1109/AIC61668.2024.10731026>.
- Taddicken, Monika. "The 'Privacy Paradox' in the Social Web: The Impact of Privacy Concerns, Individual Characteristics, and the Perceived Social Relevance on Different Forms of Self-Disclosure*." *Journal of Computer-Mediated Communication* 19, no. 2 (January 1, 2014): 248–73. <https://doi.org/10.1111/jcc4.12052>.
- Taddicken, Monika. "The 'Privacy Paradox' in the Social Web: The Impact of Privacy Concerns, Individual Characteristics, and the Perceived Social Relevance on Different Forms of Self-Disclosure*," *Journal of Computer-Mediated Communication* 19, no. 2 (January 1, 2014): 248–73
- Trakman, Leon, Robert Walters, and Bruno Zeller. "Digital Consent and Data Protection Law – Europe and Asia-Pacific Experience." *Information & Communications Technology Law* 29, no. 2 (May 3, 2020): 218–49. <https://doi.org/10.1080/13600834.2020.1726021>.
- Wang, Meng, Yalin Qin, Jiaojiao Liu, and Weidong Li. "Identifying Personal Physiological Data Risks to the Internet of Everything: The Case of Facial Data Breach Risks." *Humanities and*

Social Sciences Communications 10, no. 1 (May 8, 2023): 216.
<https://doi.org/10.1057/s41599-023-01673-3>.

Wolford, Ben. "What Are the GDPR Consent Requirement?" GDPR EU, <https://gdpr.eu/gdpr-consent-requirements/>, n.d.

Yang, Xuemin, Hong Mei, and Yueping Zheng. "Understanding the Antecedents of Privacy Fatigue in Facial Recognition-Based m-Gov Services: An Empirical Study from China." *Government Information Quarterly* 40, no. 3 (June 2023): 101827.
<https://doi.org/10.1016/j.giq.2023.101827>.

Biography

A lecturer at the Faculty of Law Universitas Negeri Semarang with a research focus on International Law and Technology Law.

< This page is intentionally left blank >