Jurnal Hukum Siber
dan Regulasi Teknologi

SAH PUBLISHER

Vol. 1, No. 1, January 2026

# The Use of Biometrics in Public Services and the Risk of Privacy Violations

**Abid Nurhuda[1], Nuri Safitri[2]***

[1]Universitas PTIQ Jakarta
[2]STAI Darussalam Lampung

Email: abidnurhuda123@gmail.com[1], nurisafitri052@gmail.com[2]

**Abstract.** The use of biometric technology in public services in Indonesia has expanded significantly in line with the digitalization of government administration and the need for accurate identification systems. The processing of biometric data such as fingerprints, facial features, and iris scans offers benefits in improving efficiency and preventing identity misuse; however, it simultaneously poses serious risks to the protection of citizens' privacy. The main issues examined concern the legal basis for the use of biometrics in public services, the potential privacy violations that may arise, and the adequacy of the existing legal safeguards. This study adopts a normative juridical approach by examining Indonesian laws and regulations, particularly Law Number 27 of 2022 on Personal Data Protection, as well as regulations governing the provision of public services and electronic systems. The findings indicate that biometric data are classified as specific personal data that require a higher level of protection. Although a legal framework is already in place, the implementation of privacy protection in public service practices still faces challenges, including the risk of data breaches, limitations in oversight mechanisms, and weak fulfillment of data subject rights. Therefore, it is necessary to strengthen technical regulations, enhance state accountability mechanisms, and consistently apply privacy protection principles to ensure that the use of biometrics in public services does not compromise citizens' right to privacy.

**Keywords**: Biometrics, Public Services, Privacy, Personal Data Protection, Indonesian Regulation

## INTRODUCTION

The development of biometric technology has driven significant changes in the delivery of public services in Indonesia. The use of biometrics aims to

Received Dec 2025 / Revised Jan 2026 / Accepted Jan 2026
*Corresponding author.
Email addresses: nurisafitri052@gmail.com (Safitri)
DOI: XX.XXXXX/jhsrt.xxxx.XXXXX

improve the accuracy of identification, service efficiency, and the security of state administrative systems[1]. Various public services, ranging from population administration to access to social services, now rely on biometric technology as part of the digital transformation of the government sector[2].

Biometrics function as instruments of identification and authentication based on an individual's physical and biological characteristics[3]. Unlike conventional forms of identification, biometric data are unique and inherently attached to an individual, making them difficult to falsify[4]. In public services, the use of biometrics seeks to ensure that services are provided to the correct subject while preventing identity misuse and duplication of citizens' data[5].

Various types of biometric data are used in state administrative systems, including fingerprints, facial images, iris scans, and voice data[6]. Fingerprint and facial data are the most commonly applied in population administration, while iris and voice biometrics are increasingly being developed for advanced authentication systems[7]. The use of diverse biometric data illustrates the growing dependence of public services on body-based identification technologies[8].

The digitalization of public services in Indonesia has encouraged the integration of biometric technology into various electronic government systems[9]. Population administration programs, healthcare services, social security schemes, and immigration services increasingly rely on digital systems to enhance service speed and accuracy[10]. In this context, biometrics are viewed

[1] Owusu-Oware, E., & Effah, J. (2024). Biometric system for protecting information and improving service delivery: The case of a developing country's social security and pension organisation. Information Development, 40(1), 61-74.
[2] Scott, M., Acton, T., & Hughes, M. (2005). An assessment of biometric identities as a standard for e-government services. International Journal of Services and Standards, 1(3), 271-286.
[3] Jain, A., Hong, L., & Pankanti, S. (2000). Biometric identification. Communications of the ACM, 43(2), 90-98.
[4] Jain, A. K., Deb, D., & Engelsma, J. J. (2021). Biometrics: Trust, but verify. IEEE Transactions on Biometrics, Behavior, and Identity Science, 4(3), 303-323.
[5] Owusu-Oware, E., & Effah, J. (2024). Biometric system for protecting information and improving service delivery: The case of a developing country's social security and pension organisation. Information Development, 40(1), 61-74.
[6] Kadhim, S. M., Paw, J. K. S., Tak, Y. C., & Ameen, S. (2024). Deep Learning Models for Biometric Recognition based on Face, Finger vein, Fingerprint, and Iris: A Survey. Journal of Smart Internet of Tdings, 2024(1), 117-157.
[7] Jain, L. C., Halici, U., Hayashi, I., Lee, S. B., & Tsutsui, S. (Eds.). (2022). Intelligent biometric techniques in fingerprint and face recognition. Routledge.
[8] Maeko, E., & Van Der Haar, D. (2024, August). Human-Centric Considerations in Deploying Biometric Modalities: A Multi-Modal Approach for Public Services Application. In 2024 International Conference on Artificial Intelligence, Big Data, Computing and Data Communication Systems (icABCD) (pp. 1-10). IEEE.
[9] FAKRULLOH, Z. A., & SH, M. (2025). NYARIS SEWINDU: Pembaruan dan Transformasi Kebijakan Administrasi Kependudukan di Indonesia. PT. RajaGrafindo Persada.
[10] Al-Muttaqin, F. A., & Nugroho, A. R. (2025). Effectiveness of digital-based public service innovation: Case study of population services in Indonesia's local government. JAKPP: Jurnal Analisis Kebijakan Dan Pelayanan Publik, 11, 1-16.

as a technical solution to address issues of duplicate identities and data inconsistencies, while also supporting effective governance[11].

The use of biometrics in public services provides benefits in the form of increased efficiency, accuracy, and service security. Identity verification processes become faster and less prone to errors compared to manual methods[12]. In addition, biometrics help the government prevent identity fraud and the misuse of public services[13]. These advantages position biometric technology as an important instrument in bureaucratic reform and the improvement of service quality for the public.

Despite its benefits, the use of biometrics also poses various risks, particularly in relation to the protection of citizens' privacy. Biometric data are sensitive and permanent in nature, meaning that data breaches or misuse may result in long-term consequences[14]. Risks of excessive surveillance, use beyond the original purpose, and weak data security systems are issues that require serious attention in the implementation of biometric-based public services[15].

The use of biometric technology in public services is closely linked to the right to privacy as a fundamental human right[16]. Biometric data represent the most personal form of an individual's biological identity, thus requiring stricter safeguards in their processing[17]. If not clearly regulated, the use of biometrics may infringe upon citizens' privacy boundaries, particularly when data are collected and processed without adequate transparency and control[18].

Biometric data are considered sensitive due to their unique, permanent, and irreplaceable characteristics in the event of a data breach. Unlike passwords or identity cards, biometric data are attached to an individual for life. These characteristics place biometric data within a category of personal data that requires special legal protection. Poor management of biometric data can pose serious risks to individual security and freedom.

---

[11] Balamurugan, M. (2024). Biometric Authentication: A Double-Edged Sword for Security. International Journal of Science and Research (IJSR), 13(9), 170-173.
[12] Perwej, Y. (2023). An empirical investigation of human identity verification methods. International Journal of Scientific Research in Science, Engineering and Technology, 10(1), Pages-16.
[13] Nair, A., & Eskici, B. (2022). Digital public services: the development of biometric authentication in India. In Introduction to Development Engineering: A Framework with Applications from the Field (pp. 533-561). Cham: Springer International Publishing.
[14] Jose, D. (2024). Exploring the sensitivity of Biometric Data: A Comparative Analysis of Theoretical and Human Perspectives.
[15] Bedewy, S. F. (2024). The impact of data security and privacy concerns on the implementation of integrated. Smart Cities: Foundations and Perspectives, 59.
[16] Allahrakha, N. (2023). Balancing cyber-security and privacy: legal and ethical considerations in the digital age. Legal Issues in the digital Age, (2), 78-121.
[17] Kind, A. (2023). Biometrics and the metaphysics of personal identity. IET Biometrics, 12(3), 176-182.
[18] Kumar, T., Bhushan, S., Sharma, P., & Garg, V. (2024). Examining the vulnerabilities of biometric systems: Privacy and security perspectives. In Leveraging Computer Vision to Biometric Applications (pp. 34-67). Chapman and Hall/CRC.

In Indonesia, biometrics have been widely used in various public services, such as population administration through the electronic identity card (e-KTP), immigration services, and the distribution of social assistance[19]. These practices demonstrate the central role of biometrics in the state administrative system. However, such widespread implementation has not always been accompanied by sufficient public awareness of personal data rights and the available mechanisms for privacy protection.

The use of biometrics in public services faces complex regulatory challenges. Biometric regulation remains fragmented across various sectoral laws and regulations and has not yet been fully integrated[20]. This condition may lead to policy inconsistencies among institutions and varying data security standards. These challenges highlight the need for a more systematic and consistent legal framework governing the processing of biometric data.

As the provider of public services, the state bears the primary responsibility for ensuring the security and protection of citizens' biometric data[21]. The state acts not only as a user of technology but also as a personal data controller. This responsibility requires the state to ensure that all biometric processing is conducted lawfully, transparently, and accountably, and does not exceed legally justified public service purposes.

The massive use of biometrics in public services underscores the urgency of legal studies focusing on privacy protection. Technological developments that outpace regulatory frameworks may create gaps that enable violations of citizens' rights. Therefore, juridical analysis is necessary to assess the conformity of biometric practices with personal data protection principles and human rights standards.

Based on the foregoing discussion, the issues examined in this study include the legal basis for the use of biometrics in public services in Indonesia, the types of privacy risks arising from the processing of biometric data, and the extent to which the existing legal framework is capable of providing effective protection for citizens' privacy rights in the implementation of biometric-based public services.

---

[19] Perdana, D., Sukrisna, E., & Satria, M. H. (2022, November). Study of Biometric Data for Citizenship Administrative Services in Indonesia By Using ISO ISO/IEC 39794. In 2022 International Conference on Advanced Creative Networks and Intelligent Systems (ICACNIS) (pp. 1-8). IEEE.

[20] Borrelli, M., Musch, S., Ventura MBE, L., Ocak Basev, H., Day, E., Brock, B., ... & Oschlag-Michael, N. (2025). Overseeing Biometric Identification.

[21] Utegen, D., & Rakhmetov, B. Z. (2023). Facial recognition technology and ensuring security of biometric data: Comparative analysis of legal regulation models. Journal of Digital Technologies and Law, 1(3).

## RESEARCH METHODOLOGY

A normative juridical approach is employed to examine the use of biometric technology in public services and the associated risks of privacy violations[22]. This approach emphasizes the analysis of legal norms governing personal data protection, the provision of public services, and the processing of biometric data. Through this approach, the study focuses on assessing the conformity of biometric practices with legal principles and human rights standards.

The sources of analysis include relevant Indonesian laws and regulations, particularly Law Number 27 of 2022 on Personal Data Protection, regulations on population administration, and rules governing the operation of electronic systems[23]. The study is also supported by secondary literature in the form of legal textbooks, academic journals, and scholarly opinions addressing biometrics, privacy, and technology law.

The analytical technique is conducted in a prescriptive and systematic manner. Prescriptive analysis is used to formulate normative assessments of biometric use in accordance with privacy protection principles. Systematic analysis is carried out by examining the interrelationship among legal norms in order to evaluate regulatory consistency and identify the need for strengthened regulation in the delivery of biometric-based public services.

## RESULTS AND DISCUSSION

### A. Legal Basis for the Use of Biometrics in Public Services in Indonesia

Law Number 27 of 2022 on Personal Data Protection classifies biometric data as a category of specific personal data. Biometric data are understood as data generated from the processing of an individual's physical, physiological, or behavioral characteristics that enable unique identification. The designation of biometrics as specific personal data indicates a higher level of protection due to the potential risks posed to privacy rights and data subject security.

The use of biometrics in population administration in Indonesia has been widely implemented, particularly through the electronic identity card (e-KTP) system. Fingerprint data and facial images are used to ensure the uniqueness of residents' identities and to prevent duplicate identities. This practice provides a legal basis for the state to utilize biometrics in the interest of orderly administration, while simultaneously placing the state in a strategic position in managing citizens' biometric data.

---

[22] Negara, T. A. S. (2023). Normative legal research in Indonesia: Its originis and approaches. Audito Comparative Law Journal (ACLJ), 4(1), 1-9.

[23]Sudarwanto, A. S., & Kharisma, D. B. B. (2022). Comparative study of personal data protection regulations in Indonesia, Hong Kong and Malaysia. Journal of Financial Crime, 29(4), 1443-1457.

In addition to population administration, biometrics are also used in various electronic public service systems, such as immigration services, social security programs, and healthcare services. The utilization of biometrics in electronic systems aims to enhance security and accuracy in user authentication. Such use is subject to regulations governing the operation of electronic systems, which require system operators to ensure data security, system reliability, and the protection of personal data subject rights.

Within the context of public services, the state acts as the controller of biometric data because it determines the purposes and means of processing citizens' data. This position entails significant legal responsibilities, including the obligation to ensure lawful data processing, limitation to legitimate public service purposes, and the implementation of adequate safeguards. The state is also required to ensure that the use of biometrics does not exceed its authority and continues to respect citizens' privacy rights.

**B. Risks of Privacy Violations in the Use of Biometrics**

The use of biometrics in public services entails a high risk of data breaches and misuse. Biometric data are stored in centralized databases and processed through electronic systems, making them vulnerable to cyberattacks or unauthorized access. In the event of a breach, the consequences are severe because biometric data cannot be replaced. This risk necessitates stricter technical and organizational safeguards compared to ordinary personal data.

In public service practices, biometric data processing is often imposed as an administrative requirement without providing alternative options for citizens. This situation raises concerns regarding valid consent, as citizens are not in an equal position to freely give consent. The use of biometrics without a clear consent basis may conflict with personal data protection principles, particularly the principles of lawfulness and purpose limitation.

The massive deployment of biometrics has the potential to encourage excessive surveillance of citizens. The integration of biometric data across public services enables extensive tracking of individual activities. Without clear legal limits, such use may go beyond legitimate public service objectives and lead to disproportionate social control. This condition raises concerns about the potential abuse of state authority in the digital sphere.

Privacy risks are further exacerbated by limited oversight and complaint mechanisms available to data subjects. Citizens are often unaware of how their biometric data are processed, stored, or shared. Moreover, complaint and redress mechanisms for biometric data violations are not yet fully effective. These limitations weaken citizens' positions in protecting their privacy rights against the use of biometrics in public services.

**C. Legal Protection of Citizens' Biometric Data**

Legal protection of biometric data is grounded in personal data protection principles, such as lawfulness of processing, purpose limitation, data minimization, security, and accountability. These principles require that biometric processing be conducted lawfully, restricted to clearly defined public service purposes, and accompanied by adequate technical and organizational safeguards. The application of these principles serves as a normative basis for preventing violations of citizens' privacy rights.

As data subjects, citizens possess certain rights in relation to biometric data processing, including the right to information, the right of access, the right to rectification, and the right to erasure in accordance with the law. These rights aim to provide individuals with control over their biometric data. However, in the context of public services, the fulfillment of data subject rights often faces limitations due to state administrative interests, thereby necessitating clear and transparent mechanisms.

The protection of biometric data is also reflected in the affirmation of the responsibilities of public service providers as data controllers. Service providers are obligated to ensure data security, prevent unauthorized access, and bear responsibility for losses arising from data breaches. Provisions on administrative, civil, and criminal sanctions function as enforcement instruments to ensure that biometric data management is carried out prudently and responsibly.

Although a legal framework for the protection of biometric data is already in place, a gap remains between legal norms and public service practices. The implementation of data protection principles is often suboptimal due to limited institutional capacity, oversight, and privacy literacy. This gap indicates the need to strengthen legal implementation so that biometric data protection does not remain merely normative, but is realized in actual practice.

**D. Directions for Strengthening Biometric Regulation in Public Services**

Strengthening biometric regulation requires technical rules that establish detailed standards for the security and governance of biometric data processing. These standards include encryption, access control, periodic audits, and data breach incident management. Uniform technical regulations are essential to reduce disparities in practices among institutions and to ensure consistent protection of biometric data across all public services.

In addition to technical standards, oversight and accountability mechanisms must be reinforced to ensure compliance by public service providers. Effective internal and external supervision, including compliance reporting and the handling of data subject complaints, is essential. State accountability as a data controller requires transparency in biometric processing

policies and the imposition of firm sanctions for violations in order to prevent abuses of authority.

An ideal model for the use of biometrics places privacy protection as a primary principle. Biometric processing should be proportional, purpose-based, and provide non-biometric alternatives where possible. The principles of privacy by design and privacy by default should be integrated from the system design stage of public services, ensuring that the use of biometrics supports service efficiency without compromising citizens' privacy rights.

## CONCLUSION AND RECOMMENDATIONS

The use of biometric technology in public services in Indonesia has a clear legal basis and provides significant benefits in improving the accuracy and efficiency of service delivery. However, the sensitive and permanent nature of biometric data poses a high risk of privacy violations if not managed with due care. Although the existing legal framework recognizes the importance of protecting biometric data, its implementation in public service practices still faces various challenges. The legal implications of biometric use require the state to perform a dual role responsibly, both as a provider of public services and as a controller of personal data. Risks of data breaches, excessive surveillance, and limited fulfillment of data subject rights highlight the need to balance state administrative interests with the protection of citizens' privacy rights. Without strong oversight and accountability mechanisms, the use of biometrics may undermine public trust in government services. As a normative recommendation, it is necessary to strengthen technical regulations governing security standards and the governance of biometric data in public services. Policymakers and service providers should enhance transparency, oversight mechanisms, and access to remedies for data subjects. In addition, integrating privacy protection principles from the system design stage is a crucial step to ensure that the use of biometrics aligns with the protection of human rights and legal certainty.

## REFERENCES


[1] Owusu-Oware, E., & Effah, J. (2024). Biometric system for protecting information and improving service delivery: The case of a developing country's social security and pension organisation. Information Development, 40(1), 61-74.

[2] Scott, M., Acton, T., & Hughes, M. (2005). An assessment of biometric identities as a standard for e-government services. International Journal of Services and Standards, 1(3), 271-286..

[3] Jain, A., Hong, L., & Pankanti, S. (2000). Biometric identification. Communications of the ACM, 43(2), 90-98.

[4] Jain, A. K., Deb, D., & Engelsma, J. J. (2021). Biometrics: Trust, but verify. IEEE Transactions on Biometrics, Behavior, and Identity Science, 4(3), 303-323.
[5] Owusu-Oware, E., & Effah, J. (2024). Biometric system for protecting information and improving service delivery: The case of a developing country's social security and pension organisation. Information Development, 40(1), 61-74.
[6] Kadhim, S. M., Paw, J. K. S., Tak, Y. C., & Ameen, S. (2024). Deep Learning Models for Biometric Recognition based on Face, Finger vein, Fingerprint, and Iris: A Survey. Journal of Smart Internet of Tdings, 2024(1), 117-157.
[7] Jain, L. C., Halici, U., Hayashi, I., Lee, S. B., & Tsutsui, S. (Eds.). (2022). Intelligent biometric techniques in fingerprint and face recognition. Routledge.
[8] Maeko, E., & Van Der Haar, D. (2024, August). Human-Centric Considerations in Deploying Biometric Modalities: A Multi-Modal Approach for Public Services Application. In 2024 International Conference on Artificial Intelligence, Big Data, Computing and Data Communication Systems (icABCD) (pp. 1-10). IEEE.
[9] FAKRULLOH, Z. A., & SH, M. (2025). NYARIS SEWINDU: Pembaruan dan Transformasi Kebijakan Administrasi Kependudukan di Indonesia. PT. RajaGrafindo Persada.
[10] Al-Muttaqin, F. A., & Nugroho, A. R. (2025). Effectiveness of digital-based public service innovation: Case study of population services in Indonesia's local government. JAKPP: Jurnal Analisis Kebijakan Dan Pelayanan Publik, 11, 1-16.
[11] Balamurugan, M. (2024). Biometric Authentication: A Double-Edged Sword for Security. International Journal of Science and Research (IJSR), 13(9), 170-173.
[12] Perwej, Y. (2023). An empirical investigation of human identity verification methods. International Journal of Scientific Research in Science, Engineering and Technology, 10(1), Pages-16.
[13] Nair, A., & Eskici, B. (2022). Digital public services: the development of biometric authentication in India. In Introduction to Development Engineering: A Framework with Applications from the Field (pp. 533-561). Cham: Springer International Publishing.
[14] Jose, D. (2024). Exploring the sensitivity of Biometric Data: A Comparative Analysis of Theoretical and Human Perspectives.
[15] Bedewy, S. F. (2024). The impact of data security and privacy concerns on the implementation of integrated. Smart Cities: Foundations and Perspectives, 59.

[16] Allahrakha, N. (2023). Balancing cyber-security and privacy: legal and ethical considerations in the digital age. Legal Issues in the digital Age, (2), 78-121.
[17] Kind, A. (2023). Biometrics and the metaphysics of personal identity. IET Biometrics, 12(3), 176-182.
[18] Kumar, T., Bhushan, S., Sharma, P., & Garg, V. (2024). Examining the vulnerabilities of biometric systems: Privacy and security perspectives. In Leveraging Computer Vision to Biometric Applications (pp. 34-67). Chapman and Hall/CRC.
[19]Perdana, D., Sukrisna, E., & Satria, M. H. (2022, November). Study of Biometric Data for Citizenship Administrative Services in Indonesia By Using ISO ISO/IEC 39794. In 2022 International Conference on Advanced Creative Networks and Intelligent Systems (ICACNIS) (pp. 1-8). IEEE.
[20] Borrelli, M., Musch, S., Ventura MBE, L., Ocak Basev, H., Day, E., Brock, B., ... & Oschlag-Michael, N. (2025). Overseeing Biometric Identification.
[21] Utegen, D., & Rakhmetov, B. Z. (2023). Facial recognition technology and ensuring security of biometric data: Comparative analysis of legal regulation models. Journal of Digital Technologies and Law, 1(3).
[22] Negara, T. A. S. (2023). Normative legal research in Indonesia: Its originis and approaches. Audito Comparative Law Journal (ACLJ), 4(1), 1-9.
[23] Sudarwanto, A. S., & Kharisma, D. B. B. (2022). Comparative study of personal data protection regulations in Indonesia, Hong Kong and Malaysia. Journal of Financial Crime, 29(4), 1443-1457.