International Journal of Social Science, Educational, Economics, Agriculture Research and Technology (IJSET) | ISSN (e) : 2827-766X
Volumes 4 No. 8 (2025)

LEGAL ANALYSIS OF THE EFFECTIVENESS OF AUTOGATE USE AND PERSONAL DATA PROTECTION AT IMMIGRATION CHECKPOINTS (RESEARCH STUDY AT THE CLASS I SPECIAL IMMIGRATION OFFICE IN BATAM)

Bayu Saputra[1*], Bachtiar Simatupang,[2] and Ramlan [3]
[1, 2, 3] Master of Law Program, Universitas Batam
e-mail : 74124035@univbatam.ac.id
***Corresponding Author : Bayu Saputra**

Received	: 25 July 2025	Published	: 08 September 2025
Revised	: 13 August 2025	DOI	: https://doi.org/10.54443/ijset.v4i8.1136
Accepted	: 29 August 2025	Link Publish	: https://www.ijset.org/index.php/ijset/index

Abstract

The development of digital technology in immigration services has driven the modernization of inspection systems through the use of autogates, an automated system that processes biometric data to verify the identity of travelers. However, the use of this technology raises legal issues related to the protection of personal data, especially in the context of compliance with Law Number 27 of 2022 concerning Personal Data Protection (PDP Law).This study aims to analyze the legal regulations and assess the effectiveness of personal data protection implementation in the autogate system at the Class I Special Immigration Office TPI Batam.The research method used is a normative juridical and empirical juridical approach, with data collection techniques through literature review, interviews, and field observations. A sociological approach to law is employed to assess the awareness and compliance of officers and users regarding the right to privacy in the practice of using the autogate. The results of the study show that, normatively, the legal regulations for personal data protection are already adequate, but they have not yet been specifically implemented in the governance of autogate usage at immigration checkpoints. At the implementation level, various technical, legal, and sociological obstacles were found, such as limited understanding of the Personal Data Protection Law by officials, the absence of specific SOPs, and low public awareness of their rights as data subjects. Recommendations include the need to formulate technical regulations that integrate the principles of the Personal Data Protection Law into the operations of the autogate system, regular training for immigration officers on personal data protection, and public education to increase legal awareness regarding the use of technology-based immigration services.

Keywords: ***Autogate, Personal Data Protection, Immigration.***

1. Introduction

The integration of technology into immigration processes has become a necessity in the digital era. Autogate systems, which use biometric and electronic data to verify travelers' identities, are increasingly adopted worldwide to improve efficiency and security at border checkpoints. In Batam, a major international gateway for Indonesia, the Class I Special TPI Immigration Office has implemented autogate systems to streamline the flow of travelers while maintaining strict immigration control. However, this advancement raises significant juridical questions regarding its effectiveness and the protection of travelers' personal data. Legal compliance and technological capability must align to ensure that such systems do not infringe privacy rights or expose sensitive data to misuse.[1] The Indonesian legal framework recognizes the importance of safeguarding personal data, as reflected in the Constitution, the Electronic Information and Transactions Law, and other sectoral regulations. Yet, data breaches and misuse remain a concern. The operation of autogate systems involves the collection and processing of sensitive biometric information, making them targets for cyber threats.[2] The challenge lies not only in technical security but also in ensuring institutional readiness, legal clarity, and enforcement mechanisms that can prevent, detect, and respond to misuse. The research

therefore seeks to analyze how effectively the autogate system functions in Batam, particularly in balancing operational efficiency with legal protections for personal data. This study applies a juridical-empirical method, combining analysis of statutory provisions, institutional policies, and field data collected through interviews and observation. The goal is to evaluate whether the autogate system complies with existing laws and whether its implementation aligns with principles of personal data protection [3]. In doing so, it provides insights into how immigration authorities can strengthen legal certainty and trust in technology-enabled border management.

2. Literature Review

2.1. Autogate Systems and Legal Basis

Autogate systems are technological innovations designed to automate immigration clearance using biometric identifiers such as facial recognition, fingerprints, or iris scans. These systems reduce the need for manual checks, minimize human error, and speed up border crossing processes, particularly in high-traffic areas such as airports and ferry terminals. The primary legal basis for the implementation of autogate systems in Indonesia can be found in Law No. 6 of 2011 on Immigration, which authorizes immigration officers to conduct examinations and verifications using electronic tools [3]. This law acknowledges that technology can enhance border security and efficiency. Furthermore, ministerial regulations and technical guidelines from the Directorate General of Immigration reinforce the operationalization of electronic systems, though they often emphasize manual procedures and lack detailed technical specifications [4]. Globally, autogate systems are used by countries such as Singapore, Malaysia, and Australia, which have developed robust operational frameworks combining law, technology, and human resource readiness [5].

These countries demonstrate that a successful autogate system depends not only on infrastructure but also on supporting legal and policy frameworks. In Indonesia, the shift toward automation is relatively recent and still evolving. Many provisions in current regulations are written with traditional immigration checks in mind. As a result, there is a gap between legal mandates and practical implementation, often causing inconsistencies at points of entry In addition, the use of autogate systems raises important legal questions about liability, privacy, and operational accountability. For example, who is responsible if the system fails to detect fraudulent documents, or if biometric data is misused, These issues require clear legal standards and institutional guidelines. Academic works emphasize that technology should complement, not replace, human oversight, as officers remain essential for handling exceptional or high-risk cases . Thus, the literature suggests that while the legal foundation for autogate systems exists, the supporting regulations must evolve to ensure clarity, uniformity, and legal certainty, particularly in terms of standards, accountability, and integration with broader border management policies [6].

2.2 Data Protection in Immigration Context

The collection and processing of personal data is central to the operation of autogate systems. Every time a traveler uses an autogate, sensitive biometric information such as facial scans, fingerprints, and travel history is captured, stored, and matched with existing databases to verify identity and prevent unauthorized entry. This process is highly data-intensive and requires strict compliance with privacy and security regulations. The Indonesian Constitution recognizes the right to privacy as an integral part of human rights, positioning it as a fundamental protection for all citizens and residents [7]. This constitutional safeguard is operationalized through laws such as the Electronic Information and Transactions Law (ITE Law), which regulates the use and protection of electronic information and emphasizes the responsibilities of institutions managing personal data . The recently enacted Personal Data Protection Law (Law No. 27 of 2022) strengthens this framework by introducing clear definitions of personal and sensitive data, outlining the principles of data minimization, requiring lawful and transparent processing, and imposing administrative and criminal penalties for breaches [8].

However, translating these principles into operational practice within the immigration sector poses unique challenges. Immigration offices are often high-pressure environments where large volumes of personal and biometric data must be processed rapidly to maintain efficiency and security. These processes involve real-time coordination with other government agencies, law enforcement bodies, and, at times, international databases to detect irregularities and manage cross-border risks. Literature on data governance notes that biometric data is inherently more sensitive than other types of personal data because it is immutable—if compromised, it cannot be reissued like a passport or an ID card. The risk of unauthorized access, cyberattacks, data breaches, or even internal misuse becomes particularly significant in high-traffic areas such as Batam, where operational demands are high and resources can be strained [9]

Research also highlights the critical importance of public trust. Citizens' and travelers' willingness to provide biometric data depends on their confidence that the authorities can safeguard this information. Breaches or misuse not only affect individuals but can also damage institutional credibility and even national security. International best practices emphasize measures such as strict access controls, multi-layered encryption, periodic privacy impact assessments, staff vetting, and independent oversight mechanisms to ensure transparency and accountability [10]. Indonesia's immigration offices, including those in Batam, have begun implementing some of these measures. For instance, there are moves to upgrade servers, restrict access to authorized personnel, and develop internal audit mechanisms. Nevertheless, gaps remain: not all immigration staff are adequately trained in data protection principles, incident response protocols are sometimes unclear, and integration between biometric systems and other national databases may create vulnerabilities if not fully secured [11]. The literature suggests that protecting biometric and personal data in immigration is not merely a matter of regulatory compliance but also a prerequisite for operational success. Policies must be converted into clear, actionable procedures, supported by ongoing technical upgrades and robust cybersecurity strategies. Furthermore, the human element—training, accountability, and ethical standards—is as critical as the technology itself. Without consistent investment in staff capacity and technical safeguards, the benefits of automation could be overshadowed by privacy risks and legal liabilities. This indicates that strong and continuous alignment between law, technology, and practice is essential to maintain both efficiency and public confidence in the immigration system.

2.3 Challenges in Enforcement

Despite the presence of clear legal mandates and the adoption of modern technology, enforcement remains one of the most critical barriers to fully realizing the potential of autogate systems and personal data protection in Batam's immigration context. The findings from the study, supported by previous literature, highlight multiple layers of challenges that are both structural and cultural. Structural and capacity-related issues are at the forefront. The number of inspectors and technical personnel assigned to Batam's immigration office is insufficient compared to the volume of travelers it manages daily. As a key international gateway connecting Indonesia to Singapore and Malaysia, Batam experiences heavy traffic, especially during holidays and business seasons. The small pool of trained officers must monitor equipment, troubleshoot technical issues, verify travelers manually when biometrics fail, and ensure compliance with data protection protocols. This heavy workload often results in fatigue, errors, and uneven enforcement . Additionally, budget limitations restrict the ability to recruit and train more staff, invest in up-to-date hardware, or conduct frequent audits and system upgrades.

Training and skill disparities also undermine enforcement. Not all officers receive standardized or comprehensive training on biometric technologies or cybersecurity. In some cases, technical updates are rolled out without sufficient user education, leading to reliance on outdated practices or overdependence on manual verification when issues arise. This affects the consistency of enforcement and weakens trust in the system's reliability. Similarly, inter-agency cooperation remains limited. Immigration operations intersect with port authorities, cybersecurity teams, law enforcement, and sometimes international bodies, but communication and data-sharing protocols are often fragmented. Without cohesive policies, agencies work in silos, slowing responses to technical or security incidents.

Institutional culture and readiness also pose challenges. Although autogate systems are designed to simplify processes and reduce human error, some officers remain hesitant to trust fully automated systems. Cultural resistance to change, fear of technological obsolescence, and concerns about accountability when something goes wrong all contribute to cautious adoption. Moreover, data protection responsibilities add another layer of complexity. Handling sensitive biometric data requires a high degree of diligence, and some officers are not fully confident in applying retention policies, breach reporting, or privacy safeguards [12]. This gap reflects the need for not only technical training but also the development of an organizational culture that prioritizes transparency, accountability, and trust. External threats exacerbate enforcement difficulties. Cybercrime targeting biometric and immigration systems is a growing global concern. Hackers and organized crime networks actively look for vulnerabilities in border systems, and biometric data because it is unique and permanent has high value if compromised [13]. Enforcement strategies therefore cannot be static; they must evolve to meet changing threats. Continuous monitoring, real-time threat detection, regular penetration testing, and cooperation with national cybersecurity agencies are essential. Yet, resource and expertise constraints mean these strategies are often only partially implemented. Dynamic and adaptive strategies are required. Scholars and practitioners agree that building strong enforcement capacity requires more than technology and legal rules. It demands organizational commitment, continuous professional development, adequate funding, clear accountability systems, and integration with broader national and international security frameworks

[14]. For Batam, as a busy maritime and air transit hub, these elements are critical. Enhancing enforcement could involve partnerships with neighboring countries for best practice exchange, investment in public education to build traveler trust in biometric processes, and consistent audits to identify weak points. In summary, enforcement in Batam faces a combination of resource, cultural, and external threat challenges. Strengthening this pillar will require a long-term approach: investing in people and systems, fostering a culture of accountability, and ensuring policies remain responsive to evolving technological and criminal landscapes.

3. Methodology

This study adopts a juridical-empirical research approach, combining normative legal analysis with field data. Normative analysis reviews primary and secondary legal sources, including Law No. 6 of 2011 on Immigration, Ministerial Regulations, the Personal Data Protection Law, and related technical guidelines. Empirical research involves observations at Batam's Class I Special TPI Immigration Office and interviews with officers, IT staff, and users of the autogate system .The data collection process was designed to capture both legal and operational perspectives. Observations focused on the implementation of autogates, including biometric capture, database integration, user flow, and officer roles. Interviews explored challenges such as system downtime, privacy concerns, and enforcement gaps. Supporting data included incident reports, inspection records, and technical documentation. Data were analyzed qualitatively to identify patterns and evaluate the extent to which the current framework supports effective and secure operations. The juridical component examined preventive and repressive measures, referencing Hadjon's theory of legal protection. Preventive measures relate to policies, training, and system safeguards; repressive measures refer to sanctions and enforcement after violations . The integration of these methods ensures a comprehensive view of the system's effectiveness, bridging law and practice.[15]

4. Results and Discussion

4.1 Implementation of Autogate at Batam Immigration Office

The deployment of the autogate system at the Class I Special TPI Immigration Office in Batam is a major step toward automating border control. This system uses biometric authentication, including fingerprint and facial recognition technology, to accelerate immigration clearance for travelers. The purpose is to improve service efficiency, reduce congestion, and strengthen security, particularly in Batam, a hub for cross-border travel between Indonesia, Singapore, and Malaysia. The introduction of this system aligns with the legal mandate in Law No. 6 of 2011, which encourages the modernization of immigration services and technology adoption . Operationally, the autogate has reduced average processing times, with travelers spending less than half the time compared to manual clearance. Observations show that during peak hours, the system can process significantly more travelers without causing major bottlenecks. This outcome reflects the system's potential to enhance service quality and reduce workload for officers. However, limitations were identified. Some travelers face difficulties due to low-quality biometric data, such as worn fingerprints, low-resolution photos, or technical failures in facial recognition. When mismatches occur, manual intervention is required, often leading to queues. Smaller entry points or secondary gates face more technical interruptions due to limited infrastructure. Additionally, there are concerns regarding system downtime and the need for backup procedures, which indicate a dependence on reliable power and network connectivity. The legal framework supports autogate use, but operational guidelines are still being refined. Questions of accountability arise when systems fail, particularly in cases where errors could lead to missed detections or inconvenience to travelers . This highlights the need for more detailed procedures, including liability allocation and emergency response measures.

4.2 Data Protection Practices and Gaps

The autogate system's reliance on biometric data brings the issue of personal data protection to the forefront. Indonesian law, particularly the Electronic Information and Transactions Law and the 2022 Personal Data Protection Law, establishes clear obligations for handling sensitive data . Batam's immigration office has introduced measures such as encryption, secure servers, and limited access to sensitive information. Officers receive training to ensure compliance, and internal audits are occasionally performed to maintain accountability . Despite these efforts, several gaps remain. Not all officers fully understand retention periods or breach response protocols, and there is no unified incident management framework. Data sharing between agencies sometimes occurs without standardized safeguards, raising the risk of unauthorized access or misuse . Moreover, the integration of biometric systems with other databases is still developing, which could create vulnerabilities if not properly secured.

Trust is essential for travelers to willingly provide biometric data. Any perception of weak data protection can reduce confidence and deter usage. Literature and best practices show that strong policies, transparent communication, privacy impact assessments, and independent oversight are critical to maintaining trust . Currently, some of these elements are still in their early stages in Batam. The study also found that while officers are aware of data sensitivity, technical limitations and budget constraints can reduce effectiveness. For example, regular cybersecurity training and updates are not yet standard practice. The risk of cyber threats, including hacking attempts, makes it essential to continuously improve security infrastructure .

4.3 Challenges in Enforcement

Enforcement remains one of the most significant obstacles to maximizing the potential benefits of the autogate system in Batam. Although the system has proven capable of improving operational efficiency and reducing waiting times, its success heavily depends on consistent oversight and strong institutional support. One of the foremost issues is the limited number of technical staff and inspectors compared to the growing volume of travelers. Batam is a major gateway for both domestic and international passengers, with thousands of people passing through immigration checkpoints daily. However, the number of trained personnel available to monitor, maintain, and troubleshoot the autogate system is insufficient. This mismatch between demand and resources makes it challenging to ensure that all equipment is functioning optimally and that any technical problems are resolved quickly.

Another pressing concern is weak coordination among relevant agencies. Immigration offices must work closely with cybersecurity units, port authorities, and sometimes law enforcement or customs officials. However, the study found that inter-agency communication is often fragmented, leading to delays in response when technical or security issues arise. Without an integrated system of information sharing and joint protocols, each agency tends to operate in silos. This lack of synergy can compromise the integrity of the system and create vulnerabilities .Cultural and behavioral factors also play an important role. Many immigration officers are accustomed to manual inspection methods and may feel more confident relying on traditional practices, especially when technical errors occur. This mindset can reduce the system's effectiveness, as officers sometimes bypass the autogate system to handle travelers manually. Furthermore, the training programs provided are not always standardized or updated. Officers may not receive timely information about new technical upgrades, cybersecurity threats, or legal changes, which affects their ability to respond effectively to evolving challenges .

Another barrier to enforcement is user-related issues. Travelers themselves contribute to inconsistencies. Some passengers hesitate to use biometric verification due to concerns about privacy, fear of data misuse, or simple unfamiliarity with the technology. Others may struggle with the system's interface, leading to repeated failures in verification. These issues highlight the importance of public education campaigns and intuitive design to improve user experience and acceptance. Finally, external threats add a critical layer of complexity. As immigration systems become more technology-driven, they become attractive targets for cybercriminals. Hackers could exploit weaknesses in the network to gain unauthorized access to biometric databases, potentially leading to identity theft, fraud, or other criminal activities. In the absence of strong cybersecurity measures, such as encryption, firewalls, and real-time monitoring, the risk of breach increases. Cyberattacks could not only compromise personal data but also undermine public trust in the immigration system and national security . To address these enforcement challenges, the study emphasizes the need for a multi-dimensional strategy. This includes increasing staffing levels, investing in continuous training, improving cross-agency collaboration, developing clear contingency protocols, and strengthening cybersecurity infrastructure. Without these steps, the autogate system's benefits will remain limited, and its vulnerabilities could overshadow its advantages.

4.4 Impact and Recommendations for Improvement

The study's findings show that the autogate system at Batam's Class I Special TPI Immigration Office has brought noticeable improvements to immigration services, particularly in reducing waiting times and increasing the accuracy of identity verification . By automating the clearance process using biometric data, the system has eased officer workloads and provided travelers with faster service, which is crucial given Batam's position as a high-traffic international gateway. These improvements align with the government's broader digitalization and service modernization agenda under Law No. 6 of 2011 . However, despite these positive outcomes, the research highlights significant challenges that, if left unaddressed, could undermine the system's long-term success. One key issue is enforcement. While the legal framework exists, operational guidelines remain broad and often leave room for interpretation, resulting in inconsistent practices across checkpoints . For example, smaller entry points may lack the

technical capacity or trained staff to handle system errors, forcing officers to revert to manual checks. This inconsistency could affect service reliability and diminish the perceived value of the system . Another concern is data protection. The autogate system processes sensitive biometric information such as fingerprints and facial images, making it a potential target for cyber threats. Although measures such as encryption and access controls are in place, interviews revealed gaps in officers' understanding of data retention policies and breach management protocols . Without clear and consistent data protection measures, the risk of unauthorized access or misuse of personal information could undermine public trust and violate privacy laws, including the 2022 Personal Data Protection Law

From a technical standpoint, the system's infrastructure needs strengthening. Hardware and software updates are not always implemented uniformly, and downtime or system malfunctions can disrupt operations, especially during peak hours . These technical limitations are often linked to budget constraints and the availability of skilled IT personnel. Moreover, inter-agency coordination is still developing; cybersecurity agencies, port authorities, and immigration offices need clearer protocols for collaboration, particularly when responding to security incidents . Benchmarking against ASEAN neighbors provides valuable lessons. Singapore's autogates operate within a tightly regulated environment, supported by strong data protection laws, regular audits, and seamless integration with national ID systems. Malaysia, too, has focused on interoperability and training, ensuring officers can handle technical issues effectively . Both countries recognize that technology alone is not enough; legal clarity, institutional readiness, and public awareness are equally important.

To strengthen Batam's system, a multi-pronged approach is needed. First, legal and operational guidelines should be updated to include clear liability provisions, standardized technical protocols, and stronger data governance . Second, investment in infrastructure is crucial, not only for hardware but also for cybersecurity tools and continuous monitoring systems . Third, capacity building must be prioritized: officers and IT staff require regular training on both technical skills and privacy protection to ensure consistent enforcement . Finally, building public trust is essential. Transparent communication about how biometric data is collected, stored, and protected can increase traveler confidence. Public education campaigns, user-friendly interfaces, and feedback mechanisms can also enhance user experience . Batam, with its high traveler volume and strategic position, can serve as a pilot site for best practices, creating a scalable model for other immigration offices nationwide.

5. Comparison

The study's findings can be better understood when compared to practices in other countries. Singapore, Malaysia, and Australia have implemented autogate systems earlier and more extensively than Indonesia. In Singapore, autogates are integrated with the national identity system and operate across all major entry points. The country emphasizes precision, speed, and security, with frequent audits and real-time monitoring. Malaysia also uses autogate technology at airports and border checkpoints, integrating it with immigration databases and enforcement systems. Compared to these benchmarks, Indonesia's implementation in Batam shows promise but remains in an early stage. While Law No. 6 of 2011 provides a clear legal mandate for technology use, specific operational standards and data security measures are still evolving. This contrasts with Singapore, where the Personal Data Protection Act clearly governs biometric data use, and Malaysia, where detailed operational manuals ensure consistency.

Another key difference is resource allocation. Singapore and Malaysia invest heavily in training, cybersecurity, and infrastructure, recognizing that technological systems require ongoing updates and staff expertise. In Batam, the lack of technical personnel and budget constraints hampers system performance and enforcement . Similarly, inter-agency cooperation is more robust in Singapore, where immigration, cybersecurity, and law enforcement agencies work in integrated frameworks. Batam's immigration office still operates with relatively limited cross-agency coordination . Despite these gaps, Batam can leverage its position as a high-traffic entry point to pilot improvements. Lessons from other jurisdictions highlight the need for clear liability rules, regular audits, and public education on data protection. The comparison suggests that Indonesia's framework is conceptually sound but needs more investment and cultural readiness to meet international standards .

6. Conclusions and Suggestion

Based on the discussion in the previous chapter, the following conclusions can be drawn:

a. The autogate system in Batam has improved immigration efficiency by reducing waiting times and minimizing manual errors. However, the system still faces operational challenges, including technical interruptions and biometric mismatches.

b. Legal frameworks exist but lack detailed technical standards and liability provisions for data misuse or system failures. Data protection measures have been introduced but are not yet uniformly applied
c. Enforcement remains inconsistent due to limited resources, inadequate training, and weak inter-agency coordination. Public awareness and trust in the system are still developing

From these conclusions, the author can offer several recommendations, namely:

a. Strengthen Legal and Technical Frameworks Update regulations to include clear provisions on data security, system liability, and technical standards for biometric systems.
b. Enhance Cybersecurity and Data Protection Invest in encryption technologies, strict access control, and regular audits. Establish incident response plans and independent oversight to ensure compliance.
c. Capacity Building Provide continuous training for officers and technical staff. Encourage a culture of accountability and readiness to adapt to technological changes.
d. Public Engagement and Transparency Increase traveler awareness about autogate use and data protection policies. Clear communication builds trust and encourages voluntary compliance.
e. Improve Inter-Agency and International Collaboration Collaborate with cybersecurity agencies, law enforcement, and international partners to share knowledge, develop standards, and enhance system resilience.
f. Pilot and Scale-Up Programs Use Batam as a model for testing advanced systems and gradually extend successful practices to other immigration checkpoints.
g. Continuous Evaluation and Audits Conduct regular operational reviews to identify weaknesses and measure performance against international best practices

Author Contributions: A short paragraph specifying their individual contributions must be provided for research articles with several authors **(mandatory for more than 1 author)**. The following statements should be used "Conceptualization: X.X. and Y.Y.; Methodology: X.X.; Software: X.X.; Validation: X.X., Y.Y. and Z.Z.; Formal analysis: X.X.; Investigation: X.X.; Resources: X.X.; Data curation: X.X.; Writing—original draft preparation: X.X.; Writing—review and editing: X.X.; Visualization: X.X.; Supervision: X.X.; Project administration: X.X.; Funding acquisition: Y.Y."

Funding: Please add: "This research received no external funding" or "This research was funded by NAME OF FUNDER, grant number XXX". Check carefully that the details given are accurate and use the standard spelling of funding agency names. Any errors may affect your future funding **(mandatory).**

Data Availability Statement: We encourage all authors of articles published in FAITH journals to share their research data. This section provides details regarding where data supporting reported results can be found, including links to publicly archived datasets analyzed or generated during the study. Where no new data were created or data unavailable due to privacy or ethical restrictions, a statement is still required.

Acknowledgments: In this section, you can acknowledge any support given that is not covered by the author contribution or funding sections. This may include administrative and technical support or donations in kind (e.g., materials used for experiments). Additionally, A statement of AI tools usage transparency has been included in the Acknowledgement section, if applicable.

Conflicts of Interest: Declare conflicts of interest or state **(mandatory)**, "The authors declare no conflict of interest." Authors must identify and declare any personal circumstances or interests that may be perceived as inappropriately influencing the representation or interpretation of reported research results. Any role of the funders in the study's design; in the collection, analysis, or interpretation of data; in the writing of the manuscript; or in the decision to publish the results must be declared in this section. If there is no role, please state, "The funders had no role in the design of the study; in the collection, analyses, or interprettation of data; in the writing of the manuscript; or in the decision to publish the results".

REFERENCES

1] Republik Indonesia, Undang-Undang Nomor 6 Tahun 2011 tentang Keimigrasian, Lembaran Negara Republik Indonesia Tahun 2011 Nomor 52, hlm. 15–20.
[2] Kementerian Hukum dan HAM RI, Peraturan Menteri Hukum dan HAM Nomor 8 Tahun 2014 tentang Paspor dan Dokumen Perjalanan, Jakarta: Ditjen Imigrasi, 2014, hlm. 7–12.
[3] Republik Indonesia, Undang-Undang Nomor 24 Tahun 2013 tentang Administrasi Kependudukan, Lembaran Negara Republik Indonesia Tahun 2013 Nomor 232, hlm. 30–36.
[4] Republik Indonesia, Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi, Lembaran Negara Republik Indonesia Tahun 2022 Nomor 180, hlm. 25–33.
[5] Republik Indonesia, Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (ITE), Lembaran Negara Republik Indonesia Tahun 2008 Nomor 58, hlm. 10–18.
[6] International Air Transport Association (IATA), Biometric Technology in Border Control, Montreal: IATA Publications, 2021, pp. 42–47.
[7] International Organization for Migration (IOM), Facilitating Cross-Border Mobility through Technology, Geneva: IOM Publications, 2022, pp. 53–61.
[8] Hadjon, Philipus M., Perlindungan Hukum bagi Rakyat di Indonesia, Surabaya: Bina Ilmu, 1987, hlm. 78–85.
[9] United Nations Office on Drugs and Crime (UNODC), Handbook on Identity-Related Crime, Vienna: UNODC, 2021, pp. 96–102.
[10] Immigration and Checkpoints Authority of Singapore, Automated Border Control: Security and Efficiency, Singapore, 2020, pp. 13–19.
[11] Data Protection Commission (Ireland), Guidelines on Biometric Data Handling, Dublin: Data Protection Commission, 2021, pp. 24–29.
[12] Cybersecurity and Infrastructure Security Agency (CISA), Biometric Data Security Framework, U.S. Department of Homeland Security, 2022, pp. 35–42.
[13] Direktorat Jenderal Imigrasi RI, Laporan Tahunan Direktorat Jenderal Imigrasi 2022, Jakarta: Ditjen Imigrasi, 2023, hlm. 55–62.
[14] Kementerian Komunikasi dan Informatika RI (Kominfo), Pedoman Perlindungan Data Pribadi, Jakarta: Kominfo, 2022, hlm. 21–27.
[15] Organisation for Economic Co-operation and Development (OECD), Privacy and Biometrics: Best Practice for Data Protection, Paris: OECD Publishing, 2021, pp. 73–79.