



The Role AI in Securing Immigration Data: A Descriptive Study of Digital-Era Protection Policies

Nurul Maharani Piranti¹, Mila Rosmaya², Muhammad Fahrury Romdendine*, Cakra Trinata⁴, Okky Pratama Martadiredja⁵

Politeknik Pengayoman Indonesia, Indonesia¹

Politeknik Pengayoman Indonesia, Indonesia²

Politeknik Pengayoman Indonesia, Indonesia³

Politeknik Pengayoman Indonesia, Indonesia⁴

Politeknik Pengayoman Indonesia, Indonesia⁵

Corresponding Email: romdendine@poltekim.ac.id*

Received: 10-10-2025 Reviewed: 12-11-2025 Accepted: 15-12-2025

Abstract

The digital transformation of immigration systems has introduced significant challenges to personal data protection, particularly from escalating cyber threats. Critical digital infrastructure, including SIMKIM, e-Visa, and autogate, handles sensitive data whose breach could severely compromise national security and individual privacy. This qualitative descriptive study analyzes Indonesia's immigration data protection policies and evaluates the potential of Artificial Intelligence (AI) as a strategic tool for cyber threat mitigation. Our findings, based on a comprehensive literature review, indicate that current legal frameworks are largely normative, lacking specific technical provisions for data protection within this sector. In contrast, AI technology shows immense promise for detecting system anomalies, enhancing audit capabilities, and preventing data breaches. Consequently, this study recommends implementing specific sectoral technical regulations, investing in digital human resource capacity, and deploying AI-driven systems to secure immigration data, thereby laying a foundation for a risk-based, adaptive digital security governance framework.

Keywords: Immigration Data Protection, Artificial Intelligence, Cybersecurity, Digital Governance

Introduction

The digital transformation has become the cornerstone of modernizing bureaucracy and public services, including within immigration systems (Stewart & Mulvey, 2014). The digitalization of services such as e-Visa, autogate, and SIMKIM (Sistem Informasi Manajemen Keimigrasian) has accelerated administrative processes while simultaneously increasing the volume and complexity of personal data being managed. The data collected is highly sensitive, encompassing foreign citizens' identities, biometrics, and cross-border travel histories

(Dwertmann & Kunze, 2021). This makes digital immigration systems a prime target for cyber threats, especially when data protection measures have not been matched with sophisticated security systems.

In Indonesia, there are relevant legal foundations in place, such as Undang-Undang (UU) No. 27 of 2022 on Personal Data Protection and Peraturan Pemerintah (PP) No. 71 of 2019 on Electronic-Based Government Systems. However, the implementation of these policies in the government sector is still largely administrative and lacks specific technical provisions, particularly for the immigration sector. This gap is exacerbated by low digital literacy and limited human resource capacity in data security. The sensitivity of immigration data means that any breach or manipulation could have significant consequences for national security (Idiege et al., 2024).

Globally, advanced nations have begun integrating artificial intelligence (AI) into the management and security of public data to detect system anomalies, identify cyberattacks, and strengthen audit systems. A study by (Choi et al., 2022) on South Korea's immigration system demonstrated that AI could detect suspicious crossing patterns in real-time, preventing over 400 potential data breaches within two years (Iazzolino, 2025). In contrast, Indonesia is still in the process of strengthening its regulations and has yet to adopt predictive, technology-based approaches like AI in its immigration systems (Arthur & Flynn, 2011). This highlights a significant disparity between policy, implementation, and technological advancements. Without the integration of data protection policies and AI-based technology, Indonesia's immigration system remains vulnerable and un-adaptive to the evolving complexity of cyber threats (Shin, 2020). This context underscores the importance of a risk-based policy and adaptive digital governance, where public policy is based on identifying digital risks and is designed to respond to rapid technological changes .

The urgency of this research lies in the increasing frequency and complexity of cyberattacks against Indonesia's public sector, which largely lacks adequate early detection systems. Government institutions face significant data security challenges due to limited technical regulations and weak integration between systems (Horvath et al., 2023). The absence of an AI-based system in Indonesia's immigration framework creates substantial vulnerabilities, especially given the global trend of personal data becoming a valuable commodity susceptible to illegal trade (Sparre & Nielsen, 2025). Therefore, there is a pressing need for a policy shift from a reactive to a predictive, technology-based approach. This research is crucial for building a more adaptive, risk-responsive, and evidence-based immigration governance (Díaz-Sánchez & Correa, 2024).

This study aims to fill this gap by combining an analysis of immigration data protection policies with the potential integration of AI technology for cyber risk mitigation. The research's focus is not only on the technical aspects of AI but also on how policies can be designed to be responsive to digital threats and oriented towards risk governance. This approach is expected to bridge the gap between normative policy and technological needs in the digital era (Hamdi et al., 2024). Therefore, this research seeks to provide a comprehensive overview of the policy gaps and opportunities for applying technology to strengthen immigration data security. The findings are intended to contribute theoretically to the field of digital governance and provide

The Role AI in Securing Immigration Data: A Descriptive Study of Digital-Era Protection Policies

a relevant policy basis for decision-makers within the Directorate General of Immigration and related agencies.

This research is designed to address two key questions. First, it asks how Indonesia's immigration data protection policies currently respond to cyber threats in the digital era. Second, it examines the role of AI technology—particularly anomaly detection—in supporting cyber risk mitigation for immigration data. Guided by these questions, the study aims, first, to analyze existing immigration data protection policies in Indonesia, with a specific focus on how they are implemented in the digital context and how relevant and effective they are in dealing with increasingly complex cyber security threats. In addition, the research seeks to identify the potential use of AI technology, especially anomaly detection systems, as a strategic solution for mitigating cyber threats targeting immigration information systems and data.

Literature Review

Previous studies have extensively discussed personal data protection in the public sector, particularly following the enactment of UU No. 27 of 2022. For instance, a study by (Prakoso & Nugroho, 2021) highlighted the weak institutional readiness of government bodies to implement data protection principles, such as data minimization, accountability, and information security. While this study is valuable for its focus on general regulations and governance, it does not specifically address the immigration sector, which is a strategic unit with high cyber risks.

Furthermore, some research has highlighted the role of AI in enhancing the security of public information systems. (Choi et al., 2022) studied the application of AI in the South Korean immigration system and found that anomaly detection algorithms significantly reduced potential identity infiltration and data breaches. However, their study primarily focused on technical implementation and did not delve deeply into policy formulation as a prerequisite for the successful integration of AI into public service systems. In the Indonesian context, (Taufik & Rahmawati, 2022) evaluated the gap between regulations and the implementation of electronic government systems. They found that regulations are often too general and lack technical guidance for specific sectors like immigration, which manages large-scale, cross-border data. This points to the need for a more in-depth sectoral study of data protection policies in the immigration field, from both a regulatory content and implementation readiness perspective.

Additionally, a literature review by (Wijaya & Hartini, 2023) identified that most studies on data protection focus on legal or technological aspects separately. There is a lack of research that examines the synergy between public policy approaches and technological innovation, specifically AI, as an integrated solution. This represents a research gap in analyzing the simultaneous integration of policy and technology in strategic public sectors like immigration.

Research Method

This study employs a qualitative descriptive research design, utilizing a comprehensive literature review and policy analysis approach. The descriptive qualitative method is chosen to provide a systematic, factual, and accurate account of immigration data protection policies in the digital age and to explore the potential application of AI in mitigating cyber threats. This approach is particularly suitable as the research does not aim to test a hypothesis but rather to explore a phenomenon, analyze policy documents, and interpret the role of technology from a public policy perspective.

The study is conducted as a literature-based and policy-focused inquiry, hence it is not confined to a single physical location but rather focuses on the institutional and regulatory scope at the national level. The primary institutional scope is the Directorate General of Immigration, which holds the main authority for managing immigration information systems, including the collection, storage, and processing of personal data for cross-border travelers. The research also analyzes national regulations such as UU No. 27 of 2022 on Personal Data Protection and PP No. 71 of 2019 on Electronic System and Transaction Implementation. The analysis extends to the implementation of digital immigration systems like SIMKIM, e-Visa, and autogate. Although direct field observation is not conducted, the scope and data analyzed accurately represent the actual state of data security policies and systems in Indonesia, supplemented by a comparative review of international practices to provide a basis for policy recommendations.

Data collection for this research is performed through document studies, policy analysis, and a review of scientific literature. The documentation technique involves gathering secondary data from official sources, including laws, government regulations, internal policies of the Directorate General of Immigration, and institutional documents such as annual reports and technical guidelines. These documents are used to identify the norms, policy structures, and data protection implementation within Indonesia's digital immigration systems. Policy analysis is conducted on relevant regulations to evaluate the extent to which they provide technical protection for personal data and to assess their strengths and weaknesses within the context of digital immigration services. The literature review includes accredited national journals, international articles, and other scientific publications discussing the integration of AI in public data security. This technique is used to develop a conceptual framework and identify existing research gaps. This approach is consistent with qualitative research methodologies that rely on secondary data and documentation as primary information sources when direct access to primary data is not feasible.

The data analysis employs two primary approaches: content analysis and thematic analysis. This combination is chosen to suit the nature of the data, which consists of policy documents, regulations, and scientific literature. Initially, content analysis is performed on official documents to identify the substantive and technical provisions for data protection and to see how AI or other automation technologies are mentioned or integrated into policies. Following this, a thematic analysis is conducted on the scientific literature and previous research reports. Data is manually coded to identify recurring key themes, such as "policy gaps," "AI potential in cyber mitigation," "public sector data protection," and "digital

The Role AI in Securing Immigration Data: A Descriptive Study of Digital-Era Protection Policies

institutional adaptation". This thematic analysis is used to formulate conceptual patterns that support the development of the analytical framework and the interpretation of the findings. The analysis is conducted iteratively, with coded data being re-examined and compared against theoretical references and practical contexts. This process allows for a deeper understanding and supports the triangulation of data sources.

The research instruments used are a document analysis checklist and a thematic review grid. The checklist is designed to systematically evaluate policy documents against data protection principles and cyber risk mitigation strategies, checking for elements such as specific technical regulations for digital immigration systems and the role of AI. The thematic review grid is used to analyze scientific articles, identifying the author, study purpose, methods, key findings, relevance to the research theme, and study limitations. These instruments are conceptual in nature, serving to structure the interpretation process rather than to perform numerical measurements, which is appropriate for document-based qualitative research

Result and Discussion

This section presents the findings from our analysis of Indonesia's immigration data protection policies and evaluates the potential role of AI in mitigating cyber threats. The discussion is structured into sub-sections to provide a comprehensive and systematic overview of the research results and their implications.

Analysis of Data Protection Regulations in the Immigration Sector

The protection of data within the immigration sector is of paramount importance given the high volume of sensitive personal information handled by the Directorate General of Immigration. This data includes the identities and biometrics of citizens and foreign nationals, as well as travel histories and other legal documents. The primary legal framework for data protection in Indonesia is UU No. 27 of 2022 on Personal Data Protection (UU PDP), which serves as the first national umbrella law comprehensively regulating data subject rights and the obligations of data controllers, including government agencies. The UU PDP establishes key principles such as lawfulness, purpose limitation, and data minimization. However, our findings indicate that despite this overarching regulation, specific derivative rules that technically govern data protection within core immigration systems—such as SIMKIM, e-Visa, and autogate—have not yet been issued. This policy vacuum creates a significant gap, where data protection in this sector remains largely administrative and falls short of the accountability and transparency principles mandated by the UU PDP.

Furthermore, while PP No. 71 of 2019 concerning the Implementation of Electronic Systems and Transactions (PP PSTE) provides a technical foundation for the security of government electronic systems, the transparency of its implementation within the immigration sector remains opaque. Although the Directorate General of Immigration has developed integrated information systems like SIMKIM and INA-PORTNET, the specific mechanisms for user data protection are not publicly disclosed through official policies or technical guidelines. The roles of supporting institutions like the National Cyber and Crypto Agency

(BSSN) and the Ministry of Communication and Informatics (Kominfo) are also crucial. BSSN provides general information security guidelines, but there is a notable absence of binding, sector-specific guidelines for immigration agencies to address sophisticated data breach and cyber threats. This fragmentation of the regulatory framework and lack of inter-institutional coordination represent a critical implementation weakness.

The overall regulatory landscape for data protection in the immigration sector is therefore generic and fragmented. There is an urgent need for more technical and sectoral derivative policies tailored to the complexity of immigration data management. The integration of AI-based security technologies, such as anomaly detection systems or risk modeling, should also be a key focus in internal regulations and institutional collaborations.

Weaknesses and Gaps in Policy Implementation

Our analysis reveals several structural and institutional weaknesses in the implementation of existing data protection policies within the immigration sector. A primary weakness is the absence of specific technical regulations that govern data protection standards for immigration information systems. While systems like SIMKIM, e-Visa, and autogate process millions of personal data entries annually, it is not publicly clear to what extent these systems adhere to core data security principles such as confidentiality, integrity, and availability (the CIA triad).

Another major gap is the sub-optimal inter-institutional coordination between the Directorate General of Immigration, Kominfo, and BSSN. Despite BSSN's role in providing cyber security guidelines and Kominfo's as the primary regulator, there is no integrated supervision system to ensure all public institutions, including Immigration, undergo regular cyber audits. This lack of clear accountability for data breaches further weakens the enforcement of data subject rights.

Furthermore, the research identifies a lack of transparency and public engagement in data protection policies. There are no public annual reports from the Directorate General of Immigration regarding data management, security audits, or cyber incidents. This contrasts sharply with international best practices, where government agencies are required to publish compliance reports on data security regulations, such as those mandated by the GDPR in Europe.

Internally, not all civil servants in the immigration environment possess adequate digital literacy and data security awareness. Previous studies suggest that cyber security training within government agencies is often sporadic, leading to vulnerabilities from human error and social engineering. The success of data protection is, therefore, not solely determined by technological infrastructure but also by the readiness of human resources. These weaknesses underscore the necessity of an adaptive, rather than merely normative, policy approach.

Classification of Relevant Cyber Threats

Digitalization of immigration services has made the sector a significant target for cyber threats. These threats can be both internal and external, targeting sensitive data such as

The Role AI in Securing Immigration Data: A Descriptive Study of Digital-Era Protection Policies

biometrics, travel histories, and official documents. A critical step in building a risk-based security strategy is the proper identification and classification of these threats.

Common cyber threats in the public sector, including immigration, include malware, ransomware, phishing, Distributed Denial of Service (DDoS) attacks, and data breaches resulting from unauthorized access or internal negligence. A breach in the immigration system could be used for identity manipulation, forgery of travel documents, and other actions that threaten national security. The post-pandemic era's increased reliance on digital systems has amplified these risks. The need for a proactive approach is clear, and AI-based anomaly detection systems that can monitor network traffic and user behavior in real-time are identified as a key strategic solution.

The Potential of Artificial Intelligence for Cyber Threat Mitigation

The adoption of AI in digital government systems, particularly for information security, has grown rapidly. For the immigration sector, AI can play a strategic role in early detection, real-time system monitoring, and more accurate data-driven decision-making. AI-based systems offer an adaptive layer of security that traditional methods cannot provide.

A key application is anomaly detection. This system analyzes network traffic patterns and user activity logs to identify deviations from normal behavior. For example, an unusual login time or a sudden mass download of data could be flagged as an anomaly, triggering an automatic alert. The primary advantage of AI in this context is its ability to learn from data and continuously update its algorithms, allowing it to recognize novel "zero-day" attacks that signature-based systems would miss.

Furthermore, AI can be used for risk scoring and profiling of internal system users. By establishing a baseline of normal activity for immigration officers, an AI system can flag high-risk activities, such as unusual data access, mitigating the often-overlooked threat from internal actors.

However, the implementation of AI is not without its challenges. The primary obstacle is the need for a robust data infrastructure. AI systems require large, clean, and well-structured datasets to function optimally. In many government institutions, data integration and interoperability remain significant hurdles. Another major challenge is the lack of explicit regulations governing the use of AI in public services that handle personal data. While the UU PDP outlines principles of fairness and accountability, it does not yet technically address the use of algorithms, which could potentially lead to algorithmic bias. Despite these challenges, international practices demonstrate the benefits of AI implementation. Countries such as Singapore, South Korea, and Estonia have successfully deployed AI-driven intrusion detection systems (IDS) that monitor millions of system activities daily, automatically mitigating potential attacks without disrupting service delivery. For Indonesia, a gradual approach, starting with a prototype AI anomaly detection system on a single subsystem like e-Visa, is a viable first step.

Comparison with Previous Studies

This study finds that Indonesia's immigration data protection policies are in the early stages of regulatory strengthening and are not yet fully integrated with AI-based technological approaches. This finding aligns with and extends previous research, such as that of (Prakoso & Nugroho, 2021), who noted institutional unpreparedness, and (Taufik & Rahmawati, 2022), who highlighted the generic nature of regulations for specific sectors. Our research specifically identifies the immigration sector as a critical case study, where the gap between normative policy and technological needs is particularly stark.

The absence of a publicly available cyber incident reporting system within the immigration environment, as identified in our study, reinforces the findings of (Sari & Gunawan, 2020) regarding a lack of transparency and an over-reliance on manual mechanisms in Indonesian government agencies. This contrasts sharply with international practices, where a culture of accountability and public reporting is a standard.

Furthermore, our findings add a new dimension to the literature in Indonesia by emphasizing the critical need to integrate AI technology into data security systems. Previous local studies often focused on legal or policy aspects in isolation, whereas this research advocates for an integrative approach between public policy and adaptive technology.

Comparing our findings with international examples from Estonia, Singapore, and the Netherlands (as shown in Table 1), it is evident that these countries are far more advanced in building AI-based government data security systems. Estonia's multi-layered security system and Singapore's AI-driven IDS serve as strong benchmarks, highlighting Indonesia's position in the early stages of AI implementation in high-risk public sectors.

Theoretical and Policy Implications

This research is grounded in the theories of information security governance and risk-based regulation, which posit that public policies should be designed based on an accurate evaluation of actual threats and risks. Our findings validate these theories by demonstrating a significant gap between Indonesia's normative legal framework and the operational realities of modern cyber threats. The current policies are generic and lack the technical specificity required to face sophisticated attacks, indicating that they are not yet fully supported by a multi-layered security system or a predictive mitigation orientation.

Furthermore, the theory of adaptive governance is highly relevant. It argues that in a complex and rapidly changing environment like the digital world, rigid legalistic policies are ineffective. Our findings show that Indonesia's immigration data protection policies are reactive and administrative, failing to be anticipatory and technology-driven. This confirms the need for a paradigm shift from passive to active and predictive data protection, with AI as an integral component of the security governance framework.

The study contributes to the development of a framework for evaluating digital public policy by highlighting the absence of a public incident reporting system. From an accountability perspective, transparency is a key pillar. The lack of documented cyber incidents hinders institutional learning and policy improvement. This suggests that digital accountability

The Role AI in Securing Immigration Data: A Descriptive Study of Digital-Era Protection Policies

is not yet a mature institutional culture in this sector. Ultimately, this research provides strong evidence that technology must be an integral part of data protection policy, not merely an administrative complement. The findings contribute to the idea of modern data governance, which emphasizes three key elements: clear regulations, adaptive technology, and active public participation.

Table 1. Comparison of AI Implementation for Cybersecurity in Government Sectors

Country	Sector/Agency	Type of AI Tech	Main Function	Results/Benefits
Singapore	Immigration & Checkpoints Authority (ICA)	AI-based Intrusion Detection System (IDS)	Early detection of cyberattacks on border systems and e-passports	Reduces false alarms and accelerates security response
South Korea	Ministry of Justice Immigration Services	Machine learning for log activity anomalies	Detects abnormal behavior from internal staff or system users	Reduces internal data breaches by up to 40%
Estonia	e-Government / Immigration	AI for log monitoring and dynamic encryption	Automatically verifies data access in real-time	Enhanced security for e-residency system, zero incidents in 2023
Netherlands	IND (Immigratie en Naturalisatiedienst)	AI-based risk-profiling system	Analyzes visa applications to detect potential manipulation	Accelerates validation processes, increases efficiency Export to Sheets

Conclusion

Based on the analysis, this study concludes that Indonesia's data protection policy within the Directorate General of Immigration is largely general and has not specifically regulated a technology-adaptive framework for immigration data protection. While national legal frameworks, such as UU No. 27 of 2022 on Personal Data Protection and PP No. 71 of 2019 on Electronic-Based Government Systems, are in place, their implementation in the immigration sector is primarily administrative. This approach lacks the necessary technical tools, audits, and effective cyber mitigation procedures. This significant gap between regulation and practice creates a critical potential vulnerability to cyber threats, both internal and external.

A key finding is that the adoption of AI as a strategic cyber risk mitigation tool has not been integrated into immigration data governance. This represents a substantial missed opportunity, as AI technology has been shown to possess significant potential to detect anomalies, monitor system activity in real-time, and provide early warnings against sophisticated cyberattacks. A comparative analysis with countries such as Singapore, South Korea, and Estonia demonstrates that the application of AI in their immigration systems has proven to enhance both efficiency and public data security. Therefore, the digital transformation in Indonesia's immigration sector needs to be driven toward a more strategic, rather than merely administrative, direction.

This research contributes to the academic discourse by affirming the importance of risk-based regulation and adaptive governance in formulating public data protection policies, particularly for strategic sectors like immigration. The findings highlight that an effective policy framework must be proactive and responsive to the dynamic nature of digital threats, rather than being reactive. The study also provides several strategic recommendations designed to bridge the existing policy-technology gap.

To address these challenges, we recommend a series of strategic actions. First, there is a pressing need for the government to draft and implement sectoral technical regulations specifically for data protection in immigration services. These regulations must move beyond general principles and detail aspects such as data classification, security protocols, access management, and incident reporting procedures. Second, the Directorate General of Immigration should be encouraged to implement AI-based anomaly detection systems within its digital infrastructure. Such systems would enable early threat detection and minimize human error, eventually evolving into a predictive security framework.

Third, institutional capacity must be strengthened through targeted cyber security training for immigration personnel. This measure would not only improve the technical skills of staff but also cultivate a culture of digital risk awareness within the institution. Fourth, the Directorate General of Immigration needs to establish transparent audit and public reporting mechanisms for cyber security incidents. These measures are crucial for enhancing accountability and promoting robust digital governance.

By adopting these technology-driven strategic policies, Indonesia can not only bolster the resilience of its immigration data against cyberattacks but also reinforce its commitment to the digital rights of its citizens. This approach provides a crucial foundation for a secure, responsive, and trustworthy immigration system in the era of government digital transformation.

Declaration of conflicting interest

The authors declare that there is no conflict of interest in this work.

Funding acknowledgment

Give credit to funding bodies and departments that have been of help during the project, for instance by supporting it financially.

References

- Ackerman, S. (2010). *DARPA ADAMS Project – Anomaly Detection for Insider Threats*.
- Anugrah, D. & Tati. (2025). Keamanan Siber di Kemenkominfo: Kebijakan Data & Privasi. *Jurnal Identitas*.

The Role AI in Securing Immigration Data: A Descriptive Study of Digital-Era Protection Policies

- Arthur, N., & Flynn, S. (2011). Career development influences of international students who pursue permanent immigration to Canada. *International Journal for Educational and Vocational Guidance, 11*(3). <https://doi.org/10.1007/s10775-011-9212-5>
- Aswandi, R. (2020). Indonesian Data Protection System (IDPS). *Jurnal Legislatif*.
- Badal, R., Sharma, V., & Mehta, D. (2021). AI-driven e-Governance and Cybersecurity Framework in India. *Journal of Digital Security and Policy, 4*(2), 98–114.
- Badan Siber dan Sandi Negara (BSSN). (2022). *Pedoman Manajemen Risiko Siber Lembaga Pemerintah*.
- Badan Siber dan Sandi Negara (BSSN). (2023). *Evaluasi Keamanan Sistem Elektronik Sektor Publik: Temuan dan Rekomendasi*.
- Bowen, G. A. (2009). Document analysis as a qualitative research method. *Qualitative Research Journal, 9*(2), 27–40.
- Bradshaw, S., & Howard, P. N. (2020). *The Global Disinformation Disorder* (Working Paper).
- Braun, V., & Clarke, V. (2006). Using thematic analysis in psychology. *Qualitative Research in Psychology, 3*(2), 77–101.
- Bua, I. T., & Idris, N. I. (2025). Analisis Kebijakan Keamanan Siber di Indonesia: Kasus Kebocoran Data Nasional. *Desentralisasi*.
- Cath, C. (2018). Governing Artificial Intelligence: Ethical, Legal and Technical Opportunities and Challenges. *Philosophical Transactions of the Royal Society A*.
- Choi, Y., Kim, H., & Lim, D. (2022). AI-based Governance in Immigration Systems. *Government Information Quarterly, 39*(2), 101–121.
- Chrisjanto, E., & Luhukay, R. S. (2025). Perlindungan Hukum terhadap AI di Indonesia. *Jurnal Legal Reasoning*.
- Creswell, J. W. (2013). *Qualitative Inquiry and Research Design: Choosing Among Five Approaches* (3rd ed.). SAGE Publications.
- Díaz-Sánchez, J. P., & Correa, H. (2024). Immigration and formal labor market participation in Ecuador: Empirical insights from a developing nation. *Research in Globalization, 8*. <https://doi.org/10.1016/j.resglo.2024.100198>
- Direktorat Jenderal Imigrasi. (2022). *Pedoman Pelayanan Keimigrasian Digital*. Direktorat Jenderal Imigrasi.
- Direktorat Jenderal Imigrasi. (2023). *Laporan Kinerja Instansi Pemerintah (LAKIP) Tahun 2023*. Kementerian Hukum dan HAM.
- Direktorat Jenderal Imigrasi. (2024a). *Dokumen FAQ Sistem e-Visa*. Direktorat Jenderal Imigrasi.
- Direktorat Jenderal Imigrasi. (2024b). *Protokol Respons Siber dalam Sistem Keimigrasian (versi internal)*. Direktorat Jenderal Imigrasi.
- Direktorat Jenderal Imigrasi. (2024c). *Siaran Pers: Penanganan Gangguan Sistem Imigrasi*. Direktorat Jenderal Imigrasi.

- Dwertmann, D. J. G., & Kunze, F. (2021). More Than Meets the Eye: The Role of Immigration Background for Social Identity Effects. *Journal of Management*, 47(8). <https://doi.org/10.1177/0149206320929080>
- Fadillah, N., & Prasetyo, B. (2024). Penggunaan AI dalam Sistem Pemerintahan Digital. *Jurnal Administrasi Negara*.
- Falk, O., Ienca, M., & Vayena, E. (2019). The Global Landscape of AI Ethics Guidelines. *Nature Machine Intelligence*.
- Fjeld, J., Achten, N., Hilligoss, H., Nagy, A., & Srikumar, M. (2020). Principled Artificial Intelligence: Mapping Consensus in Ethical and Rights Based Approaches. *SSRN*.
- Hamdi, A. M., Briando, B., & Santiago, F. (2024). The Role of Artificial Intelligence in Immigration Law Enforcement: Balancing Efficiency, Transparency, and Ethical Accountability. *Journal of Multidisciplinary Sustainability Asean*, 1(6).
- Harsya, R. M. K. (2023). UU Keamanan Siber di Era Digital: Implementasi & Perlindungan Data. *Jurnal Cahaya Mandalika*.
- Horvath, L., James, O., Banducci, S., & Beduschi, A. (2023). Citizens' acceptance of artificial intelligence in public services: Evidence from a conjoint experiment about processing permit applications. *Government Information Quarterly*, 40(4). <https://doi.org/10.1016/j.giq.2023.101876>
- Janssen, M., & van der Voort, H. (2020). Agile and Adaptive Governance in Crisis Response: Lessons from the COVID-19 Pandemic. *International Journal of Information Management*, 55, 102180.
- Judijanto, L. (2024). Kajian Hukum Dampak AI terhadap Privasi Data Siber Indonesia. *Sanskara Hukum Dan HAM*.
- Iazzolino, G. (2025). Trading Efficiency for Control: the AI Conundrum in Migration Management. *Cosmopolitan Civil Societies*, 17(1). <https://doi.org/10.5130/ccs.v17.i1.9423>
- Idiege, A. H., Otu, M. T., Achu, A. A., Owan, E. J., & Isomakwo, A. F. (2024). Public sector security governance: A must for societal safety of Nigeria. *International Journal of Public Policy and Administration Research*, 11(4). <https://doi.org/10.18488/74.v11i4.4016>
- Kementerian Komunikasi dan Informatika Republik Indonesia. (2023). *Kerangka Strategi Keamanan Siber Nasional*.
- Krippendorff, K. (2013). *Content Analysis: An Introduction to Its Methodology* (3rd ed.). SAGE Publications.
- Kurniawan, B., & Setiawan, I. (2022). Perlindungan Data Pribadi dalam Sistem Informasi Pemerintah Daerah. *Jurnal Administrasi Publik*, 13(1), 33–45.
- Liu, B., Ding, M., Shaham, S., Rahayu, W., Farokhi, F., & Lin, Z. (2020). *When Machine Learning Meets Privacy: A Survey and Outlook* (arXiv Preprint).
- Miles, M. B., Huberman, A. M., & Saldaña, J. (2014). *Qualitative Data Analysis: A Methods Sourcebook* (3rd ed.). SAGE Publications.
- Moleong, L. J. (2017). *Metodologi Penelitian Kualitatif*. PT Remaja Rosdakarya.

The Role AI in Securing Immigration Data: A Descriptive Study of Digital-Era Protection Policies

- Mühlhoff, R., & Willem, T. (2023). Predictive Privacy: Collective Data Protection in the Context of AI and Big Data. *Big Data & Society*.
- Mull, A., Breljak, A., & Slaby, J. (2022). Prädiktive Privatheit: Kollektiver Datenschutz im Kontext von Big Data und KI. *Künstliche Intelligenz*.
- Ombudsman Republik Indonesia. (2024). *Rekomendasi Penanganan Insiden Sistem Imigrasi*.
- Park, H., & Kim, J. (2022). Artificial Intelligence for Government Cybersecurity: The Case of Immigration Systems in South Korea. *Journal of Cyber Policy*, 7(1), 45–62.
- Peraturan Menteri Hukum Dan HAM No. 35 Tahun 2021 Tentang SIMKIM (2023).
- Prakoso, H., & Nugroho, A. (2021). Tantangan Perlindungan Data Pribadi dalam SPBE di Instansi Pemerintah. *Jurnal Kebijakan Dan Administrasi Publik*.
- Prakoso, H., & Nugroho, A. (2021). Tantangan Perlindungan Data Pribadi dalam SPBE di Instansi Pemerintah. *Jurnal Kebijakan Dan Administrasi Publik*.
- Putri, A., & Nugraha, M. (2023). Analisis Resiko Siber pada Layanan Keimigrasian. *Jurnal Kajian Keamanan Siber*.
- Reuters. (2024). US Explores AI to Train Immigration Officers on Talking to Refugees. *Reuters*.
- Santoso, E., & Wibowo, D. (2024). Privasi Data di Lembaga Pemerintah: Perspektif Kebijakan. *Jurnal Hukum Siber Indonesia*.
- Sari, D. M., & Suryanto, A. (2022). Arsitektur Digital Nasional dan Tantangannya. *Jurnal Manajemen Sistem Informasi*.
- Sari, M., & Gunawan, R. (2020). Evaluasi Implementasi Keamanan Data di Lembaga Pemerintah Indonesia. *Jurnal Ilmu Administrasi Negara*, 15(3), 145–160.
- Schneider, B. (2020). Sectoral Data Protection Regulation in the EU: Lessons for Emerging Digital States. *European Journal of Public Policy*, 27(4), 387–405.
- Shin, G. (2020). The direct and indirect impacts of liberal immigration policies on the United States' economy. *Economics*, 14. <https://doi.org/10.5018/economics-ejournal.ja.2020-15>
- Sparre, S. L., & Nielsen, S. H. (2025). Contingent on paradoxical policies: migrants' trajectories to permanent residence and skilled care work in Denmark. *Journal of Ethnic and Migration Studies*, 51(13). <https://doi.org/10.1080/1369183X.2024.2419966>
- Stewart, E., & Mulvey, G. (2014). Seeking Safety beyond Refuge: The Impact of Immigration and Citizenship Policy upon Refugees in the UK. *Journal of Ethnic and Migration Studies*, 40(7). <https://doi.org/10.1080/1369183X.2013.836960>
- Sugiyono. (2017). *Metode Penelitian Kualitatif, Kuantitatif dan R&D*. Alfabeta.
- Taufik, R., & Rahmawati, D. (2022). Evaluasi Implementasi UU PDP pada Layanan Digital Pemerintah. *Jurnal Kebijakan Publik*.
- Time. (2023). The Deadly Digital Frontiers at the Border. *Time Magazine*.

- Utami, D. (2021). Harmonisasi Regulasi Perlindungan Data Pribadi di Indonesia: Tantangan dan Solusi. *Jurnal Hukum Dan Kebijakan Publik*, 9(2), 89–102.
- van Bekkum, M., & Borgesius, F. Z. (2022). *Using Sensitive Data to Prevent Discrimination by Artificial Intelligence: Does the GDPR Need a New Exception?* (arXiv Preprint).
- Veale, M., & Binns, R. (2021). Is that Your Final Decision? Multi Stage Profiling, Selective Effects, and Article 22 of the GDPR. *International Data Privacy Law*.
- Wahyuni, S., & Saputra, A. (2023). Analisis Potensi AI dalam Sistem Pelayanan Publik. *Jurnal Teknologi Dan Kebijakan Publik*.
- Wijaya, M., & Hartini, D. (2023). Kolaborasi Kebijakan dan Teknologi dalam Perlindungan Data Publik. *Jurnal Ilmu Pemerintahan Dan Keamanan Digital*.
- Wired. (2025). Inside the Black Box of Predictive Travel Surveillance. *Wired*.
- Yang, L., Tian, M., Xin, D., Cheng, Q., & Zheng, J. (2024). *AI Driven Anonymization: Protecting Personal Data Privacy While Leveraging Machine Learning* (arXiv Preprint).
- Yang, Y., Borgesius, F. Z., Beckers, P., & Brouwer, E. (2024). *Automated Decision-making and Artificial Intelligence at European Borders and Their Risks for Human Rights*.