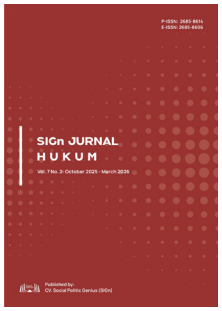

SIGn Jurnal Hukum

E-ISSN: 2685 – 8606 || P-ISSN: 2685 – 8614
https://jurnal.penerbitsign.com/index.php/sjh/article/view/v7n2-13

Vol. 7 No. 2: October 2025 - March 2026 Published Online: November 28, 2025

Article Title

The Limitations of Lex Generalis: Analyzing the Readiness of the GDPR and PDP Law for AI-Based Facial Recognition Technology

Author(s)

Komang Suputra Kurniawan*
Universitas Pendidikan Nasional, Indonesia || putrakurniawanlegal@gmail.com
**Corresponding Author*

I Gede Agus Kurniawan
Universitas Pendidikan Nasional, Indonesia || gedeaguskurniawan@undiknas.co.id

How to cite:

Kurniawan, K. S., & Kurniawan, I. G. A. (2025). The Limitations of Lex Generalis: Analyzing the Readiness of the GDPR and PDP Law for AI-Based Facial Recognition Technology. *SIGn Jurnal Hukum, 7*(2), 838-852. https://doi.org/10.37276/sjh.v7i2.533

ABSTRACT

The implementation of AI-based FRT creates a fundamental conflict between security innovation and the protection of the human right to personal data. This research aims to (1) analyze the fundamental juridical-ethical challenges of AI-based identity systems; (2) examine the effectiveness and limitations of the GDPR (European Union) and the PDP Law (Indonesia) in responding to these risks; and (3) formulate recommendations for an adaptive regulatory framework. This research employs a normative legal research method, utilizing critical-comparative and prescriptive approaches. The analysis reveals two main findings. First, FRT presents unique systemic risks. These risks include discriminatory algorithmic bias, the normalization of mass surveillance, and an accountability crisis resulting from its "black-box" nature. These risks cannot be mitigated by conventional legal frameworks for privacy. Second, critical analysis proves that the GDPR and the PDP Law, as lex generalis instruments, are normatively and practically insufficient in regulating the specific and predictive dynamics of AI technology. This limitation creates a significant rechtsvacuüm, wherein technology adoption operates without adequate juridical oversight. Therefore, this research concludes that reliance on these two regulations is no longer sufficient. This research recommends a shift in Indonesia's regulatory paradigm. The prescriptive solution proposed is the adoption of a lex specialis (derivative regulation) framework that is proactive, preventive, and adopts a risk-based approach. This framework is essential to ensure that AI innovation remains aligned with the principles of data protection and human dignity.

Keywords: *Artificial Intelligence; Facial Recognition Technology; Personal Data Protection; Risk-Based Regulation.*

INTRODUCTION

Digital transformation has propelled Artificial Intelligence (AI) into a major disruptive force. This technology fundamentally alters paradigms of human interaction, industrial operations, and governance (Verheij, 2020). AI's capacity to process data on a massive scale has revolutionized various sectors, from precision healthcare to autonomous financial systems. In the context of security and public administration, one of the most influential yet controversial AI implementations is Facial Recognition Technology (FRT). FRT is no longer science fiction. It has become an integral instrument in modern identity systems, employed by law enforcement authorities (Sihombing et al., 2024), border control (Mas'adi, 2025), and commercial digital service authentication(Atmawijaya & Radiyah, 2024). FRT offers unprecedented efficiency and security. However, it simultaneously triggers profound juridical and ethical debates (Surden, 2019).

The core of this controversy lies in the data processed: facial biometric data. Unlike other personal data, facial data is unique and permanent. It can also be collected remotely without the data subject's explicit consent. FRT's ability to identify and track individuals in real-time transforms the human face into a universal identifier, vulnerable to misuse. It creates a direct conflict between the need for security innovation and the protection of the fundamental right to privacy (Kavoliūnaitė-Ragauskienė, 2024). The use of FRT by states and corporations raises serious concerns about the potential for mass surveillance, the erosion of anonymity in public spaces, and systemic

discrimination resulting from algorithmic bias (Gasiokwu et al., 2025). Consequently, FRT has become the epicenter of AI governance challenges. Its functional benefits must be critically weighed against the risks of human rights violations (Almeida et al., 2022).

On the global stage, awareness of these risks prompted the European Union to establish Regulation (EU) 2016/679 (General Data Protection Regulation/GDPR) as the gold standard for data protection. The GDPR explicitly classifies biometric data as "special categories of personal data," the processing of which is prohibited unless very strict exceptional conditions are met (Raposo, 2023). This seriousness is reinforced by the Regulation (EU) 2024/1689 (*Artificial Intelligence Act*/EU AI Act) (full implementation on August 2, 2026), which adopts a risk-based approach. Under the EU AI Act, the use of FRT in public spaces is classified as "high-risk," or even "unacceptable risk" in certain contexts. It indicates an acknowledgment that the GDPR alone is insufficient to mitigate the specific risks of AI (Urquhart & Miranda, 2022; Gültekin-Várkonyi, 2024).

In comparison, other jurisdictions, such as the United States, rely on a fragmented sectoral framework. Despite lacking a comprehensive federal data protection law equivalent to the GDPR, state-level legislation, such as the Illinois Biometric Information Privacy Act (BIPA), has demonstrated its stringency. BIPA's success in holding major technology corporations accountable through class action mechanisms for collecting biometric data without consent highlights the effectiveness of a different approach to technology governance (Montgomery, 2025).

Indonesia, in response to these digital dynamics, has enacted Law Number 27 of 2022 on Personal Data Protection (PDP Law). The enactment of the PDP Law marks a new era in data governance in Indonesia. Philosophically and normatively, the PDP Law adopts many principles contained in the GDPR (Soemitro et al., 2023). Similar to the GDPR, the PDP Law classifies biometric data as specific (sensitive) data, requiring explicit consent and a strong legal basis for its processing (Kennedy, 2025).

The presence of this law provides optimism for strengthening citizens' privacy rights amid the rapid adoption of technology. The PDP Law is expected to function as a lex generalis that mitigates the negative excesses of data processing. This function is not limited to social media or population administration contexts. The PDP Law is also expected to cover various other new technologies that process personal data on a massive scale, such as smartwatch technology in the healthcare sector (Irwanto et al., 2025) or verification systems in digital banking that are vulnerable to phishing (Ekawati et al., 2025).

Nevertheless, this optimism is confronted by the reality that AI technology implementation moves far faster than legislative cycles. The adoption of FRT in

Indonesia has been widespread, not only among the private sector but also among state institutions. This is evident in the implementation of population identity verification systems (Mas'adi, 2025). At the same time, the reality on the ground shows that the PDP Law, as a lex generalis, is beginning to show its limitations. The PDP Law was designed to regulate data processing in general. However, it is not yet equipped with specific technical regulatory instruments to address the unique characteristics of AI, such as its predictive, autonomous, and black-box nature (Purwanti et al., 2025). Consequently, a legal vacuum (*rechtsvacuüm*) exists in the practical implementation of FRT in Indonesia (Girsang, 2024).

This gap between the law as it ought to be (*das sollen*) in the PDP Law and the law as it is (*das sein*) in technological implementation has led to tangible juridical consequences. Case studies in Indonesia reveal incidents of misidentification by FRT systems used by authorities. These incidents have resulted in immaterial damages and violations of civil rights (Razaq, 2023; Hilmi & Marpaung, 2025). Such cases expose the vulnerability of citizens when high-risk technology is operated without clear standards for accuracy, algorithmic transparency, and accountability mechanisms. This failure confirms that biometric data protection cannot be guaranteed solely by on-paper consent. Instead, it requires strict technical oversight and audits (Simanjuntak et al., 2023). This is an area not yet detailed by the PDP Law or its implementing regulations.

The literature review above indicates that while research on the GDPR and FRT is abundant in the European context (Almeida et al., 2022; Raposo, 2023; Gültekin-Várkonyi, 2024), along with general analyses of AI and law (Surden, 2019; Verheij, 2020; Cole, 2024), a significant research gap exists in the Indonesian context. The majority of research in Indonesia concerning the PDP Law still focuses on general implementation (Kennedy, 2025) or its application in the healthcare (Irwanto et al., 2025) and banking (Ekawati et al., 2025) sectors. Although some preliminary studies have highlighted the regulatory gap for FRT in Indonesia (Simanjuntak et al., 2023; Girsang, 2024) and identified cases of misidentification (Razaq, 2023; Hilmi & Marpaung, 2025), no in-depth comparative-critical analysis has been conducted. Such analysis is necessary to systematically examine the extent to which the PDP Law's limitations are directly confronted by the standards of the GDPR and the EU AI Act in the specific context of FRT.

Based on the background and research gap described, the objectives of this research are: (1) To analyze the fundamental ethical and legal challenges posed by AI-based facial recognition systems to privacy rights and personal data protection; (2) To critically and comparatively examine the effectiveness, limitations, and normative ambiguities of the GDPR and the PDP Law in responding to the specific risks of FRT; and (3) To formulate recommendations for an adaptive, risk-based regulatory framework for FRT governance in Indonesia. The contribution of this research is to provide an

academic contribution to the development of technology law, particularly in analyzing the limitations of the lex generalis in the face of AI disruption. Furthermore, this research is expected to offer prescriptive input for policymakers, regulators, and implementing institutions in Indonesia in drafting specific, proactive derivative regulations for the PDP Law that can ensure the accountability of AI technology implementation.

METHOD

This study is classified as normative legal research, also known as doctrinal legal research. It fundamentally focuses on the analysis of library-based materials or secondary data. This research type is employed to examine the norms, principles, concepts, and statutory regulations about the principal research issue (Qamar & Rezah, 2020). This issue is the friction between AI-based FRT innovation and the legal framework for protecting personal data. The study concentrates on analyzing legal texts (the PDP Law and the GDPR) and academic literature to construct a juridical argument. The nature of this research is descriptive-analytical with a prescriptive orientation. Its objective is not only to describe (description) but also to analyze and provide recommendations (prescription) for the identified legal issues.

To address the research objectives, three main approaches are employed simultaneously. *First*, the statute approach. This approach is utilized to examine and interpret the hierarchy and substance of relevant statutory regulations, primarily the PDP Law and the GDPR. *Second*, the comparative approach. This approach is used to critically compare the substantive provisions, implementation, and biometric data protection standards between the legal regimes of Indonesia (the PDP Law) and the European Union (the GDPR and the EU AI Act). The objective is to identify the strengths and weaknesses of each system. *Third*, the conceptual approach. This approach is employed to analyze the ethical and legal concepts that underpin this issue, such as "privacy," "algorithmic bias," "AI accountability," and the "risk-based approach."

The sources of legal materials in this research consist of primary and secondary legal materials. Primary legal materials comprise binding statutory regulations, namely the PDP Law, the GDPR, and the EU AI Act. Secondary legal materials encompass all literature relevant to the research topic. This literature includes international and national scientific journals, books, research reports, policy discussion proceedings, and academic articles that specifically address the issues of FRT, AI, the GDPR, and the PDP Law. The collection of primary and secondary legal materials was conducted through library research and online research of verified legal databases and scientific journal portals (Sampara & Husen, 2016).

All collected legal materials were analyzed using qualitative analysis techniques with a deductive-inductive approach. Data analysis was conducted in three systematic

stages to address the three research objectives. The first stage is descriptive-interpretive analysis. At this stage, data from the literature are used to describe and interpret the dimensions of the ethical and legal challenges associated with FRT. The second stage is critical-comparative analysis. Here, primary legal materials (the GDPR and the PDP Law) are critically analyzed and compared to identify regulatory gaps. The third stage is prescriptive analysis. In this stage, findings from stages one and two are synthesized to formulate policy recommendations and an adaptive lex specialis regulatory model. This entire analytical process aims to construct a systematic, coherent, and sound legal argument (Irwansyah, 2020).

RESULTS AND DISCUSSION

A. Fundamental Challenges of AI-Based Identity Systems: A Juridical and Ethical Analysis of Privacy, Bias, and Accountability

The implementation of AI-based FRT fundamentally alters the paradigm of human identification, presenting numerous challenges. This technology operates by processing biometric data, which is recognized as the most sensitive data category in modern data protection regimes. Article 9(1) of the GDPR explicitly classifies "biometric data for uniquely identifying a natural person" as "special categories of personal data." The processing of this data is prohibited by default. Indonesia adopts a similar principle in Article 4 section (2) point b of the PDP Law, which categorizes "biometric data" as part of "specific personal data." This classification is crucial because facial data is unique, permanent, and immutable (Kim et al., 2023). Unlike a password that can be reset, a breach of facial biometric data is permanent and poses a lifelong risk to the data subject.

The first juridical-ethical challenge is the normalization of mass surveillance and the erosion of anonymity in public spaces. FRT enables the continuous, real-time tracking of individuals without requiring physical interaction. The use of this technology by law enforcement authorities, as critically examined in the context of UK and EU policing, creates an invasive surveillance infrastructure (Urquhart & Miranda, 2022). This is not merely passive data collection, but rather an infrastructure for proactive social control. The ability to identify every individual in public spaces—such as parks, streets, or during protests—effectively eliminates the right to anonymity. Furthermore, this practice can induce a "chilling effect" on the freedom of expression and assembly. Citizens often feel as though they are constantly being monitored, which alters their behavior. This challenge extends beyond mere violations of individual privacy; it has the potential to undermine the "checks and balances" mechanism between the state and its citizens (Almeida et al., 2022).

The second, most pressing challenge is algorithmic bias, which has implications for systemic discrimination. AI-based FRT systems are not objectively neutral. Their effectiveness is highly dependent on the quality and representation of the data used to train them. Numerous studies have empirically proven that many commercial FRT systems exhibit significantly lower accuracy rates for people with darker skin tones, women, and other minority groups (Gasiokwu et al., 2025). This bias is not merely a technical error. It is a fundamental ethical and juridical failure, as it violates the principle of non-discrimination. When these biased systems are deployed in critical contexts, such as law enforcement (Sihombing et al., 2024; Zahro, 2025), the result is "automated discrimination." Individuals from marginalized groups are more likely to experience misidentification (a false positive). It can lead to wrongful arrests, denial of services, or stigmatization, all of which constitute clear violations of the principle of equality before the law.

The third challenge is the accountability crisis arising from the black-box nature of AI algorithms. When an FRT system makes a decision—for example, flagging an individual as "suspected" or "high-risk"—the decision-making process is often opaque. This process is complex and inexplicable, even by its own developers. In a legal context, this creates a fundamental problem (Almeida et al., 2022). The data subject's right to a "meaningful explanation" for automated decisions, as mandated by Article 22 of the GDPR, becomes difficult to fulfill. In the event of misidentification, individuals struggle to challenge the decision due to the lack of transparency in the algorithmic process. This absence of accountability impedes access to justice and effective legal remedies for victims.

Furthermore, the evolution of AI is now moving into a more invasive domain: emotional AI, also known as affective computing. This technology not only identifies who a person is but also attempts to interpret their emotional state (such as anger, honesty, or suspicion) through the analysis of facial micro-expressions (Salami, 2025). The use of this technology in contexts such as job interviews, interrogations, or insurance opens a new Pandora's box regarding violations of mental privacy and cognitive autonomy. The processing of such "emotional data" is often conducted without a strong scientific basis. This magnifies the risk of discrimination and arbitrary decision-making. Current regulations, which focus on "identification," are entirely unprepared to govern technology that seeks to "interpret" the thoughts and feelings of individuals (Kavoliūnaitė-Ragauskienė, 2024). The combination of these fundamental risks (mass surveillance, systemic bias, accountability crises, and emotional intrusion) demonstrates that FRT is not merely an ordinary technical tool. Instead, FRT is a high-risk instrument that demands an exceptionally stringent juridical and ethical governance framework.

B. The Effectiveness of Biometric Data Protection Regulations: A Critical Analysis of the Readiness of the GDPR and the PDP Law

In addressing the multidimensional challenges presented in the previous Subchapter, the data protection legal framework plays a central role. The GDPR is considered the global standard, theoretically providing the most robust protection for biometric data. Article 9(1) of the GDPR establishes a strict prohibition on the processing of "biometric data for uniquely identifying a natural person." However, this prohibition is not absolute. It can be overridden by various exceptions in Article 9(2) of the Regulation, such as "explicit consent" from the data subject or if processing is necessary for "substantial public interest." In practice, it is these very exception clauses that create loopholes. Analysis of GDPR implementation indicates that European Union member states have differing interpretations of "substantial public interest." This exception is often used to justify the use of FRT by law enforcement (Gültekin-Várkonyi, 2024). Furthermore, the concept of "explicit consent" becomes fragile in contexts of power imbalances, such as between citizens and state authorities (Raposo, 2023).

The GDPR's limitations in addressing FRT become more apparent when confronted with the speed of AI innovation. The GDPR is a regulation designed after the fact (ex-post) (focusing on what happens after data is collected). However, the GDPR struggles to regulate technology design before the fact (ex-ante) (before the technology is deployed). Recognizing this gap, the European Union is now moving beyond the GDPR by initiating the EU AI Act. This step is an implicit acknowledgment that the GDPR alone is insufficient. The EU AI Act shifts the paradigm from "data protection" to "product risk management." This regulation classifies FRT as high-risk, subject to a series of strict compliance obligations before it can be marketed or used (Cole, 2024). This layered approach (GDPR + AI Act) demonstrates that the lex generalis (the GDPR) necessitates a lex specialis (the AI Act) to address the unique risks associated with AI (Urquhart & Miranda, 2022).

In Indonesia, the PDP Law adopts many GDPR principles, including the classification of biometric data as specific data (Article 4 section (2) point b of the PDP Law). The processing of specific data, according to Article 20 section (2) of the PDP Law, must be based on the "explicit consent" of the data subject or other legal bases such as the data controller's "legal obligation." Normatively, this foundation appears strong. However, critical analysis indicates that the PDP Law faces implementation challenges far greater than the GDPR. It is primarily due to a void in technical regulations (Purwanti et al., 2025). The PDP Law is a lex generalis that establishes "what" must be protected, but it does not regulate "how" specific technologies, such as FRT, must be supervised, audited, or tested for accuracy. The absence of minimal technical standards, guidelines for Data Protection

Impact Assessments (DPIAs) specific to AI, and algorithm audit mechanisms risks rendering the biometric data protection under the PDP Law a "paper tiger" (Kennedy, 2025).

This *rechtsvacuüm* is extremely dangerous because the adoption of FRT in Indonesia continues without adequate oversight. Unlike the European Union, which is actively debating a moratorium or ban on FRT in public spaces, in Indonesia, this technology is already widely used by government institutions. Examples include implementation for population administration (Mas'adi, 2025) and for law enforcement purposes (Girsang, 2024). A paradox arises when this high-risk technology is operated under the general assumption of legality, despite the specific technical oversight and audit frameworks mandated by modern data protection standards (such as DPIAs) not yet being available or effectively enforced.

This regulatory void has demonstrably caused real-world consequences. It exposes the gap between the *das sollen* (the law as it ought to be) and the *das sein* (the law as it is). Case studies of misidentification incidents involving FRT systems used by authorities in Indonesia, such as the Abdul Manaf case, provide empirical evidence of algorithmic bias risks (Razaq, 2023; Hilmi & Marpaung, 2025; Zahro, 2025). This case demonstrates what happens when flawed (biased) technology is operated without strict verification and accountability mechanisms. In such situations, the current PDP Law has not provided a clear and swift framework for legal remedies for victims of such misidentification.

A comparative analysis between the PDP Law and other legal regimes further clarifies this limitation. When compared to Singapore's Personal Data Protection Act (PDPA), Indonesia's PDP Law does carry far heavier criminal sanctions. It reflects a focus on ex-post enforcement. However, Singapore's PDPA is considered more mature in providing technical guidance and proactive compliance for the industry (Soemitro et al., 2023). This highlights a philosophical difference: Indonesia emphasizes punishment, whereas Singapore prioritizes prevention.

Meanwhile, when compared to United States jurisdictions, such as the BIPA cases in Illinois, the US legal system (despite being fragmented) demonstrates the strength of civil litigation (class actions). This mechanism has proven effective in demanding corporate accountability for unlawful biometric data collection (Montgomery, 2025). A robust class action mechanism for addressing such privacy violations has yet to be tested for its effectiveness in Indonesia under the PDP Law. Consequently, the burden of enforcement is placed solely on the state.

This limitation of the PDP Law as a lex generalis is not unique to FRT. The same pattern of gaps is also identified in case studies on other new technologies. For example, research on smartwatches in the healthcare sector (Irwanto et al., 2025)

and digital banking services (Ekawati et al., 2025) also reveals similar challenges. In those cases, the PDP Law struggles to address the technical complexities of data processing, algorithmic transparency, and the validity of consent. This recurring pattern confirms the core finding of this research: that the PDP Law, as a general lex, is insufficient to effectively address the dynamics, speed, and specific risks associated with AI technology.

C. Reconstructing an Adaptive Regulatory Framework: A Projection of Risk-Based AI and FRT Governance in Indonesia

The finding that the PDP Law, as a lex generalis, is insufficient implies that Indonesia cannot rely solely on this legal framework for its protection. To mitigate the fundamental risks of AI-based FRT, Indonesia must immediately shift from a reactive regulatory paradigm (waiting for violations to occur) to one that is proactive, preventive, and adaptive. The most urgent prescriptive solution is the formulation of a lex specialis (a derivative regulation of the PDP Law). This regulation must specifically govern the acquisition, development, and implementation of high-risk AI systems, including those related to FRT. This regulation must shift the focus from a mere "consent-based" model, which is often illusory in practice, toward a risk-based governance approach (Cole, 2024).

This risk-based approach requires policymakers to adopt the regulatory model proposed by Poirson (2021). This model includes three main pillars: Limited Scope, Controlled Use, and Dual Oversight. "Limited Scope" refers to establishing strict prohibitions (red lines) for FRT applications whose risks are deemed unacceptable (e.g., social scoring or indiscriminate mass surveillance). "Controlled Use" refers to obligating entities that utilize FRT (especially law enforcement) to comply with minimal technical standards and adhere to strict transparency and proportionality. "Dual Oversight" refers to establishing independent audit mechanisms, both internal and external (involving the Data Protection Authority and civil society), to oversee on-the-ground implementation.

More technically, this lex specialis must translate the abstract principles within the PDP Law into concrete juridical obligations. For example, the principles of Privacy by Design and by Default, as enshrined in Articles 27 and 39 of the PDP Law, must be operationalized into legal obligations. This obligation includes conducting AI-specific DPIAs before such systems are operated. This DPIA must explicitly analyze the risks of bias, discrimination, and misidentification, and provide clear mitigation plans (Almeida et al., 2022). Furthermore, the principle of algorithmic accountability must be enforced through transparency obligations. Data subjects must have the right to know when they are interacting with an AI system and how decisions affecting them are made (Rambe & Abdurrahman, 2024).

Furthermore, the urgency for this specific regulation does not only apply to AI-based FRT. The same regulatory gap is also apparent in AI-driven disruptions in other fields. An example is AI-generated art. This technology now fundamentally challenges the conventional copyright regime, which is centered on the concept of the "human creator" (Wibowo, 2025). It confirms that AI is a unique phenomenon (*sui generis*). This phenomenon requires a *sui generis* legal response, not merely the forced application of old laws.

In designing this regulation, Indonesia can learn from the general principles of "AI as Law." This principle emphasizes the importance of building AI systems that are explainable, accountable, and aligned with human values (Surden, 2019; Verheij, 2020). Ultimately, the goal of this adaptive regulatory framework is not to hinder innovation. Innovations such as the development of "smart cities" (Azam et al., 2024) or more secure authentication systems (Atmawijaya & Radiyah, 2024) must continue to be supported. However, the goal is to ensure that such innovation proceeds within ethical and legal corridors that guarantee the protection of fundamental rights.

CONCLUSIONS AND SUGGESTIONS

Based on the results and discussion, it is concluded that the innovation of AI-based identity systems, particularly through the implementation of FRT, has created a fundamental and multidimensional conflict with the personal data protection framework. *First*, this research concludes that the challenges posed by FRT are not merely technical in nature. These challenges are fundamentally juridical-ethical. They manifest in three primary forms: (1) the risk of systemic discrimination due to algorithmic bias; (2) the normalization of mass surveillance, which erodes anonymity in public spaces; and (3) the accountability crisis resulting from the black-box nature of algorithms, which impedes due process. *Second*, this research concludes that existing data protection legal instruments, at both the global (GDPR) and national (PDP Law) levels, have proven to be normatively and practically insufficient. As lex generalis regulations, both laws were designed for an era of data processing but fail to address the specific, dynamic, and predictive risks of AI technology. This limitation creates a significant *rechtsvacuüm*, wherein the rapid adoption of AI-based FRT in practice operates without adequate technical and juridical oversight.

The failure of this lex generalis framework implies that personal data protection in the AI era can no longer depend on a reactive, sanction-based (ex-post) regulatory model. Therefore, this research recommends a fundamental shift in Indonesia's regulatory paradigm. Indonesia is urged not to rely solely on the PDP Law. Instead, Indonesia must immediately formulate a lex specialis regulatory framework (a derivative regulation) that specifically governs high-risk AI. This new framework must

be proactive, preventive, and adaptive, adopting the risk-based approach pioneered by the EU AI Act. Prescriptively, this regulation must translate abstract principles (such as those enshrined in Articles 27 and 39 of the PDP Law, concerning Privacy by Design and by Default) into concrete technical obligations. These obligations include auditable minimum accuracy standards and layered oversight mechanisms (such as the "Limited Scope, Controlled Use, and Dual Oversight" model) to ensure that technological innovation remains aligned with the protection of human rights and individual dignity.

REFERENCES

Almeida, D., Shmarko, K., & Lomas, E. (2022). The Ethics of Facial Recognition Technologies, Surveillance, and Accountability in an Age of Artificial Intelligence: A Comparative Analysis of US, EU, and UK Regulatory Frameworks. *AI and Ethics, 2*(3), 377-387. https://doi.org/10.1007/s43681-021-00077-w

Atmawijaya, R., & Radiyah, U. (2024). Perancangan Autentikasi Multi Faktor dengan Pengenalan Wajah dan Fido (Fast Identity Online). *INTI Nusa Mandiri, 19*(1), 46-53. https://doi.org/10.33480/inti.v19i1.5263

Azam, M., Javaid, N., Rafiq, T., Zafar, S., Adnan, M., & Munir, K. (2024). Smart Cities towards Artificial Intelligence. *The Asian Bulletin of Big Data Management, 4*(2), 344-359. https://doi.org/10.62019/abbdm.v4i02.185

Cole, M. D. (2024). AI Regulation and Governance on a Global Scale: An Overview of International, Regional and National Instruments. *Journal of AI Law and Regulation, 1*(1), 126-142. https://doi.org/10.21552/aire/2024/1/16

Ekawati, D., Herdiana, D., & Haryanti, A. (2025). Phishing in the Banking Sector: Between Cybercrime and Consumer Protection. *SIGn Jurnal Hukum, 7*(1), 133-151. https://doi.org/10.37276/sjh.v7i1.422

Gasiokwu, P. I., Oyibodoro, U. G., & Nwabuoku, M. O. I. (2025). GDPR Safeguards for Facial Recognition Technology: A Critical Analysis. *International Research Journal of Multidisciplinary Scope, 6*(1), 407-423. https://doi.org/10.47857/irjms.2025.v06i01.02025

Girsang, S. Y. B. (2024). Pentingnya Regulasi Khusus Sistem Face Recognition Technology Sebagai Produk Artificial Intelligence dalam Peningkatan Keamanan dan Penegakan Hukum di Indonesia. *Nommensen Journal of Legal Opinion, 5*(2), 86-98. https://doi.org/10.51622/njlo.v5i2.1817

Gültekin-Várkonyi, G. (2024). Navigating Data Governance Risks: Facial Recognition in Law Enforcement under EU Legislation. *Internet Policy Review, 13*(3), 1-36. https://doi.org/10.14763/2024.3.1798

Hilmi, F., & Marpaung, Z. A. (2025). Perlindungan Hukum bagi Korban Penggunaan Teknologi Pengenalan Wajah. *Jurnal Antologi Hukum, 5*(1), 18-37. https://doi.org/10.21154/antologihukum.v5i1.5128

Illinois General Assembly: Biometric Information Privacy Act (Public Act 095-0994). https://www.ilga.gov/Legislation/publicacts/view/095-0994

Irwansyah. (2020). *Penelitian Hukum: Pilihan Metode & Praktik Penulisan Artikel*. Mirra Buana Media.

Irwanto, H. T., Wiranti, W., Dahlan, M. F., & Kadir, N. K. (2025). Ethics and Law of Personal Data Protection for Smartwatches in the Healthcare Sector. *SIGn Jurnal Hukum, 7*(1), 421-436. https://doi.org/10.37276/sjh.v7i1.489

Kavoliūnaitė-Ragauskienė, E. (2024). Right to Privacy and Data Protection Concerns Raised by the Development and Usage of Face Recognition Technologies in the European Union. *Journal of Human Rights Practice, 16*(2), 658-674. https://doi.org/10.1093/jhuman/huad065

Kennedy, A. (2025). Tantangan Implementasi dan Perkembangan Hukum Telematika di Indonesia. *Ethics and Law Journal: Business and Notary, 3*(2), 1-9. https://doi.org/10.61292/eljbn.262

Kim, M. W., Kim, I. H., Kim, J., Oh, J. H., Chang, J., & Park, S. (2023). A Study on the Protection of Biometric Information against Facial Recognition Technology. *KSII Transactions on Internet & Information Systems, 17*(8), 2124-2139. https://doi.org/10.3837/tiis.2023.08.009

Law of the Republic of Indonesia Number 27 of 2022 on Personal Data Protection (State Gazette of the Republic of Indonesia of 2022 Number 196, Supplement to the State Gazette of the Republic of Indonesia Number 6820). https://www.dpr.go.id/dokumen/jdih/undang-undang/detail/1814

Mas'adi, D. R. A. (2025). Digitalisasi Administrasi Migrasi: Implementasi Teknologi dalam Pengelolaan Imigrasi dan Kependudukan. *Journal of Administrative and Sosial Science, 6*(1), 24-33. https://doi.org/10.55606/jass.v6i1.1832

Montgomery, L. R. (2025). Facebook and the Biometric Information Privacy Act Litigation. *Endnotes: The Journal of the New Members Round Table, 13*(1), 72-82. Retrieved from https://journals.ala.org/index.php/endnotes/article/view/8492

Parliament of Singapore: Personal Data Protection Act 2012 [2020 Revised Edition]. https://sso.agc.gov.sg/Act/PDPA2012

Poirson, C. (2021). The Legal Regulation of Facial Recognition. In K. Miller & K. Wendt (Eds.), *The Fourth Industrial Revolution and Its Impact on Ethics: Solving the Challenges of the Agenda 2030* (pp. 283-302). Springer. https://doi.org/10.1007/978-3-030-57020-0_21

Purwanti, N., Barthos, M., & Saputra, T. E. (2025). The Role of Artificial Intelligence in the Implementation of Personal Data Protection Law in Indonesia. *INJURITY: Journal of Interdisciplinary Studies, 4*(6), 325-336. https://doi.org/10.58631/injurity.v4i6.1448

Qamar, N., & Rezah, F. S. (2020). *Metode Penelitian Hukum: Doktrinal dan Non-Doktrinal*. CV. Social Politic Genius (SIGn). https://books.google.co.id/books?id=TAQHEAAAQBAJ

Rambe, R., & Abdurrahman, L. (2024). Implikasi Etika dan Hukum dalam Penggunaan Teknologi Pengenalan Wajah: Perlindungan Privasi Versus Keamanan Publik. *Jurnal Hukum Caraka Justitia, 4*(2), 90-104. https://doi.org/10.30588/jhcj.v4i2.1828

Raposo, V. L. (2023). (Do Not) Remember My Face: Uses of Facial Recognition Technology in Light of the General Data Protection Regulation. *Information & Communications Technology Law, 32*(1), 45-63. https://doi.org/10.1080/13600834.2022.2054076

Razaq, M. L. (2023). Penggunaan Teknologi Pengenalan Wajah dalam Keamanan Publik. *Journal of Education Religion Humanities and Multidiciplinary, 1*(2), 482-486. https://doi.org/10.57235/jerumi.v1i2.1403

Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the Protection of Natural Persons with Regard to the Processing of Personal Data and on the Free Movement of Such Data, and Repealing Directive 95/46/EC (General Data Protection Regulation). http://data.europa.eu/eli/reg/2016/679/oj

Regulation (EU) 2024/1689 of the European Parliament and of the Council on Laying Down Harmonised Rules on Artificial Intelligence and Amending Regulations (EC) No 300/2008, (EU) No 167/2013, (EU) No 168/2013, (EU) 2018/858, (EU) 2018/1139 and (EU) 2019/2144 and Directives 2014/90/EU, (EU) 2016/797 and (EU) 2020/1828 (Artificial Intelligence Act) [OJ L, 2024/1689, 12.7.2024]. https://eur-lex.europa.eu/eli/reg/2024/1689/oj

Salami, E. (2025). Personal Data Protection in Emotional AI: The Facial Coding Example. In R. Ballardini et al. (Eds.), *Emotional Data Applications and Regulation of Artificial Intelligence in Society* (pp. 113-124). Springer. https://doi.org/10.1007/978-3-031-80111-2_7

Sampara, S., & Husen, L. O. (2016). *Metode Penelitian Hukum*. Kretakupa Print.

Sihombing, R. P., Kusno, K., & Siregar, A. A. (2024). Investigative Effectiveness in the Digital Era: A Case Study of Technological Innovation at the Rokan Hilir Police Resort. *SIGn Jurnal Hukum, 6*(2), 52-67. https://doi.org/10.37276/sjh.v6i2.368

Simanjuntak, Y. K., Putra, D. T., Panjaitan, G. L., Siregar, C. G., & Pangaribuan, N. S. P. (2023). Privacy Protection and the Use of Facial Recognition Technology in Public Surveillance: Legal Perspectives and Policy Implementation in the Digital Era. *Problematika Hukum, 9*(1), 14-23. https://doi.org/10.33021/ph.v9i1.5200

Soemitro, D. P., Wicaksono, M. A., & Putri, N. A. (2023). Penal Provisions in the Personal Data Protection Law: A Comparative Legal Study between Indonesia and Singapore. *SIGn Jurnal Hukum, 5*(1), 155-167. https://doi.org/10.37276/sjh.v5i1.272

Surden, H. (2019). Artificial Intelligence and Law: An Overview. *Georgia State University Law Review, 35*(4), 1305-1337. Retrieved from https://readingroom.law.gsu.edu/gsulr/vol35/iss4/8

Urquhart, L., & Miranda, D. (2022). Policing Faces: The Present and Future of Intelligent Facial Surveillance. *Information & Communications Technology Law, 31*(2), 194-219. https://doi.org/10.1080/13600834.2021.1994220

Verheij, B. (2020). Artificial Intelligence as Law: Presidential Address to the Seventeenth International Conference on Artificial Intelligence and Law. *Artificial Intelligence and Law, 28*(2), 181-206. https://doi.org/10.1007/s10506-020-09266-0

Wibowo, A. M. (2025). The Future of Copyright Protection for AI-Generated Art: Lessons from the Ghiblification Phenomenon. *SIGn Journal of Social Science, 6*(1), 1-27. https://doi.org/10.37276/sjss.v6i1.436

Zahro, A. K. (2025). Perlindungan Privasi Individu dalam Penggunaan Face Recognition Tinjauan Hukum dan Etika. *Jurnal Spektrum Hukum, 21*(2), 150-159. https://doi.org/10.56444/sh.v21i2.5779