EISSN: 2654-525X| PISSN: 0216-6534
Volume 21 Nomor 2 Agustus 2025: 285-295
DOI: 10.30996/dih.v0i0.132295

DiH: Jurnal Ilmu Hukum

A Critical Analysis of Criminal Accomplice Provision in Employment Law Violations

Sarta[1*], Moh Soleh[2].
[1]Universitas Narotama Surabaya, Indonesia
[2]Universitas Narotama Surabaya, Indonesia
*Corresponding Author: sartash3@gmail.com

Article History:
Submitted:
08-07-2025
Received:
05-08-2025
Accepted:
24-08-2025

Keywords:
Biometric Data, Legal Certainty,PDP Law.

Abstract

The increasing use of artificial intelligence (AI), deepfake technology, and advanced medical procedures has transformed the landscape of biometric data, particularly facial features. This study examines the extent to which Indonesia's Law No. 27 of 2022 on Personal Data Protection (PDP Law) ensures legal certainty for altered biometric facial data, including digitally or medically modified images. Employing a normative juridical research method with statutory and conceptual approaches, the paper interprets legal provisions, evaluates their adequacy, and compares them with international frameworks such as the EU's General Data Protection Regulation (GDPR) and Singapore's Personal Data Protection Act (PDPA). Findings reveal that the PDP Law classifies altered facial data as "specific personal data," mandating explicit consent, robust security measures, and recognition of data subjects' rights. The law's extraterritorial scope further extends protection to Indonesian citizens' data processed abroad. However, enforcement challenges persist, particularly in cross-border contexts and automated profiling. The novelty of this research lies in its focused analysis of altered biometric data as a unique legal category, coupled with comparative insights to address regulatory gaps. The study recommends strengthening implementing regulations, adopting AI-specific safeguards, and enhancing cross-border enforcement cooperation to ensure sustainable protection of biometric privacy in the digital era.

1. Introduction

Technological advancements have significantly reshaped the way individuals express identity, interact, and share personal data. Facial recognition systems, deepfake applications, augmented reality (AR), and AI-driven image reconstruction now allow the alteration of biometric facial data for entertainment, commercial, medical, and security purposes. While such technologies generate creative and economic opportunities, they raise complex legal and ethical issues regarding privacy and data protection[1].

Under most modern legal systems, including Indonesia's, the human face is considered a primary identifier and is classified as sensitive or "specific personal data." This categorization is reflected in Article 1(1) and Article 3(c) of the PDP Law, which impose heightened protection standards. However, the emergence of altered biometric data facial features modified yet still identifiable creates a legal grey area: should such modified data be treated with the same level of protection as original biometric data? This paper addresses this underexplored issue by critically analyzing the PDP Law's treatment of altered biometric facial data, assessing legal certainty, and comparing it with international norms, particularly the

[1] Arash Heidari et al., "A Novel Blockchain-Based Deepfake Detection Method Using Federated and Deep Learning Models," *Cognitive Computation* 16, no. 3 (May 1, 2024): 1073–91, https://doi.org/10.1007/S12559-024-10255-7.

GDPR and PDPA[2]. The discussion emphasizes both normative provisions and practical enforcement challenges, offering forward-looking recommendations for AI-era data protection.

The rapid advancement of digital technology in recent decades has profoundly transformed how individuals interact, communicate, and express themselves, especially in the digital environment. Among the various domains affected by this transformation, personal identity and data privacy have emerged as areas facing complex legal, ethical, and technological challenges. One of the most notable developments is the ability to manipulate or alter biometric data particularly facial features through increasingly accessible technologies such as face recognition systems, deepfake applications, augmented reality (AR), and artificial intelligence (AI). These technologies allow users to modify, reconstruct, or recreate facial images for entertainment, commercial promotion, social media filters, medical reconstruction, or even identity concealment[3].

While these advancements open up vast opportunities in creative and medical industries, they also raise critical concerns regarding the legal status and protection of such altered biometric data. The face is considered one of the most essential identifiers of an individual and falls under the category of sensitive or specific personal data in most modern legal systems, including that of Indonesia. When facial data is altered either digitally or surgically the legal question arises: should such modified data still be subject to the same level of legal protection as original biometric data? If the answer is yes, how does the law conceptualize and enforce such protections?[4]

In Indonesia, the need to address this legal vacuum was formally recognized with the enactment of Law Number 27 of 2022 concerning Personal Data Protection (hereinafter referred to as the PDP Law). The PDP Law represents Indonesia's first comprehensive regulatory framework aimed at protecting personal data and aligning national data protection principles with international standards. Under Article 1 point 1 of the PDP Law, personal data is defined broadly to include any data concerning an identified or identifiable individual. This includes data processed through both electronic and non-electronic systems and encompasses any data that may directly or indirectly identify a person, whether individually or in combination with other information.

Facial data, being biometric in nature, is explicitly classified as "*specific personal data*" under the PDP Law, thereby requiring a higher standard of protection. This includes the obligation to obtain explicit consent from data subjects prior to collection, use, processing, or distribution of the data. The law also enshrines principles of transparency, accountability, data minimization, and data security, as well as the rights of data subjects, including the right to

[2] J. O'Byrne and M. E. Cates, "Geometric Theory of (Extended) Time-Reversal Symmetries in Stochastic Processes: I. Finite Dimension," *Journal of Statistical Mechanics: Theory and Experiment* 2024, no. 11 (November 30, 2024), https://doi.org/10.1088/1742-5468/ad8f2b.
[3] Saputra, "Aspek Hukum Telematika Dalam Perlindungan Data Pribadi," *Jurnal Kepastian Hukum Dan Keadilan* 1, no. 5 (2023): 54–74.
[4] Brian Dolhansky et al., "The DeepFake Detection Challenge (DFDC) Dataset," October 28, 2020, http://arxiv.org/abs/2006.07397.

withdraw consent, the right to access, and the right to request erasure[5]. Despite the existence of such legal provisions, there remains an underexplored area in Indonesian legal scholarship regarding how the law applies to facial data that has been altered or manipulated. In practice, numerous applications and platforms store, analyze, and even distribute users' modified facial images without adequately informing them or obtaining consent. These altered images, often processed for marketing algorithms, facial analysis, or synthetic training data, are not always recognized by developers or users as falling within the scope of protected biometric data. This raises the potential for privacy violations, misuse, digital profiling, and discrimination.

Several international studies have addressed similar concerns. For example, Zhang et al. in their study on deepfake regulations in China emphasized the lack of explicit legal protection for synthetically generated facial data and its implications for identity theft and misinformation. Sütőová and Kováčiková explored how European Union's GDPR applies to AI-generated and transformed biometric data, noting significant enforcement challenges. In the Indonesian context, Hartati provided a general legal commentary on the PDP Law but did not specifically address the implications of altered facial features. Other scholars such as Wijaya and Ramadhani discussed biometric data categorization but lacked focus on the evolving nature of facial data manipulation in digital platforms. [6]

The limitation of these studies lies in the absence of a focused analysis on legal certainty in protecting altered biometric data particularly facial features that remain identifiable despite transformation. This paper aims to fill that gap by providing a legal interpretation of the PDP Law with respect to modified facial data, examining whether such data should be regarded as personal data and how legal protection mechanisms should apply. The paper also explores the extraterritorial aspect of the PDP Law as stated in Article 2 paragraph (2), which allows the law to extend its jurisdiction to foreign entities processing the data of Indonesian citizens. This provision is particularly relevant given the dominance of global tech companies and foreign platforms in data processing practices in Indonesia. The objective of this research is to analyze how the PDP Law ensures legal certainty for individuals whose facial data has been altered, either by choice or through platform algorithms, and to determine the boundaries of legal protection under Indonesian data protection norms. The novelty of this study lies in its focus on transformed facial data as a unique category of biometric information that continues to possess identification potential. In doing so, the paper contributes to the broader legal discourse on digital privacy and provides a critical legal basis for strengthening enforcement and advocacy concerning biometric data protection in Indonesia[7].

2. Methods

[5] Matyáš Boháček and Hany Farid, "Protecting President Zelenskyy against Deep Fakes," June 24, 2022, http://arxiv.org/abs/2206.12043.
[6] Riccardo Guidotti et al., "A Survey of Methods for Explaining Black Box Models," *ACM Computing Surveys* 51, no. 5 (September 30, 2019), https://doi.org/10.1145/3236009.
[7] Samin, "Perlindungan Terhadap Kebocoran Data Pribadi Oleh Pengendali Data Melalui Pendekatan Hukum Progresif," *Jurnal Ilmiah Research Student* 1, no. 3 (2024): 1–15, https://doi.org/https://doi.org/10.61722/jirs.v1i3.386.

This study employs a normative legal research method, which focuses on the examination of prevailing positive legal norms, particularly those concerning the protection of Indonesian citizens' personal data as regulated under Law Number 27 of 2022 on Personal Data Protection (PDP Law). The approaches used in this research are the statutory approach and the conceptual approach. The data utilized in this study are derived from primary legal materials, such as legislation, and secondary legal materials, including legal literature, academic journals, and relevant official documents. The data are analyzed qualitatively by interpreting legal norms, principles, and applicable provisions in order to address the legal issue concerning legal certainty over modified biometric data in the form of facial images.

3. Results and Discussion

3.1. Legal Certainty Regulation on the Protection of Personal Data of Indonesian Citizens Who Modify Facial Features (Biometric Data) Under Law Number 27 of 2022 on Personal Data Protection

Norms are (1) rules or provisions that bind members of a group in society, used as a guide, order and control of appropriate and acceptable behavior: every member of society must comply with what applies; The protection of personal data within the Indonesian legal system has undergone significant development with the enactment of Law Number 27 of 2022 concerning Personal Data Protection (PDP Law). This legislation was introduced to address the legal demands of society in the digital era, particularly in ensuring legal certainty for citizens' personal data, including biometric data such as facial features that may be altered through digital manipulation (e.g., deepfakes, AI reconstruction, or facial modifications due to medical procedures). Philosophically, the protection of personal data is a manifestation of human rights as reflected in the values of Pancasila and enshrined in the 1945 Constitution of the Republic of Indonesia (UUD NRI 1945), particularly Article 28G paragraph (1) and Article 28H paragraph (4). These provisions provide a strong constitutional foundation for the recognition and protection of the right to privacy as an essential component of fundamental citizens' rights, including the safeguarding of data that is inherently attached to personal identity, such as facial features[8].

The enactment of Law No. 27 of 2022 on Personal Data Protection (PDP Law) represents a landmark in Indonesia's legal architecture, not only by introducing a comprehensive framework for personal data governance but also by addressing emergent risks posed by evolving biometric technologies. Among these risks is the manipulation or alteration of facial biometric data through advanced means such as *deepfake* algorithms, generative AI facial reconstruction, and medically induced modifications. Such altered data poses unique challenges to both the definitional boundaries and enforcement mechanisms of privacy law.

Philosophically, the right to personal data protection in Indonesia is grounded in the constitutional guarantees of privacy under Article 28G(1) and Article 28H(4) of the 1945 Constitution (UUD NRI 1945). This aligns with the *Right to Privacy Theory* as developed in Warren and Brandeis's seminal 1890 Harvard Law Review article, which conceptualises privacy as the "*right to be let alone*." In the context of modern data protection, scholars such as Daniel J. Solove (2008) have expanded this into the "*taxonomy of privacy*," recognising

[8] Samin.

informational privacy including biometric data as a discrete and critical component of human dignity and autonomy[9].

The PDP Law's classification of biometric identifiers, including facial features, as "*specific personal data*" (Article 3(c)) resonates with Lee Bygrave's *Information Privacy Framework*, which asserts that certain categories of data require heightened protection due to their intrinsic capacity for uniquely identifying individuals and their susceptibility to misuse[10]. Altered biometric facial data retains this quality of identifiability, whether through residual biometric markers or by correlation with auxiliary datasets, a concern supported by empirical findings in re-identification research[11].

From a regulatory standpoint, Article 1(1) of the PDP Law adopts a broad definition of personal data, ensuring that identifiability whether direct or indirect remains the cornerstone of legal classification. This is consistent with the European Union's GDPR, which in Recital 26 maintains that the criterion for protection lies in the potential for identification, regardless of whether data has been technically altered. Similarly, Singapore's PDPA maintains jurisdiction over biometric identifiers, while California's CCPA extends its scope to "*inferences*" drawn from biometric data, thus recognising the predictive potential of altered or synthesised identities. In practice, the inclusive approach adopted by the PDP Law mitigates the risk of regulatory evasion through superficial data alteration a loophole that could otherwise enable data controllers to argue that modified images fall outside the ambit of "*personal data*." warns that failing to account for such altered data in legal definitions creates a "*blind spot*" in privacy enforcement, especially in the era of AI-based data fusion[12].

The PDP Law embeds fundamental principles of processing—transparency, accountability, purpose limitation, accuracy, and security (Articles 20–22)—mirroring the OECD Privacy Guidelines and GDPR's Article 5. Of particular relevance is the requirement for *explicit consent* in processing specific personal data. This aligns with the *Doctrine of Informed Consent*, a principle well established in both medical ethics and data protection law, requiring that consent be specific, informed, and freely given. For altered biometric data, this means that generic terms of service are insufficient; data subjects must be clearly informed that their facial images may be modified and the implications of such modification. A further dimension of legal certainty under the PDP Law is its recognition of data subjects' rights to access, rectify, erase, and object to processing (Articles 5–15). These provisions echo the GDPR's "*right to be forgotten*" (Article 17) and "*right to object*" (Article 21), as well as the United Nations' *Guiding Principles on Business and Human Rights* which mandate corporate respect for privacy as part of broader human rights due diligence.

Governance responsibilities are divided between the Personal Data Controller and the Personal Data Processor (Articles 1(8)–(9)), with both bearing joint liability for breaches. This dual-responsibility model aligns with Bygrave's *Accountability Principle*, which posits that

[9] C Kuner, C., Bygrave, L. A., & Docksey, *The EU General Data Protection Regulation (GDPR): A Commentary* (Oxford University Press, 2022).
[10] et al. Floridi, L., Cowls, J., Beltrametti, M., "An Ethical Framework for a Good AI Society," *Minds and Machines* 4, no. 28 (2018): 689–707.
[11] D. J. Schwartz, P. M., & Solove, "The PII Problem: Privacy and a New Concept of Personally Identifiable Information," *NYU Law Review* 6, no. 86 (2020).
[12] Guidotti et al., "A Survey of Methods for Explaining Black Box Models."

responsibility for compliance cannot be fully delegated and must rest with those determining processing purposes and means. Violations under the PDP Law attract administrative sanctions (warnings, suspension, deletion orders) and criminal penalties (up to six years' imprisonment and multi-billion rupiah fines). Comparative analysis reveals that while the GDPR's penalty regime (up to €20 million or 4% of annual turnover) may have stronger deterrent effect, Indonesia's inclusion of custodial sanctions reflects a hybrid approach combining administrative deterrence with criminal culpability[13].

One of the PDP Law's most progressive features is its extraterritorial application (Article 2(2)), enabling jurisdiction over foreign entities processing the personal data of Indonesian citizens where such processing has legal consequences within Indonesia. However note in their commentary on extraterritorial data protection laws, practical enforcement in cross-border contexts is often hindered by jurisdictional fragmentation, lack of mutual legal assistance treaties, and divergent evidentiary standards[14]. For example, if a foreign-based AI platform uses altered images of an Indonesian citizen in an unauthorised advertising campaign, asserting jurisdiction may be straightforward under the PDP Law but achieving compliance or redress may require diplomatic and procedural cooperation. The PDP Law currently faces two principal challenges in addressing altered biometric data[15]:

1. Absence of AI specific processing standards The law provides general principles but lacks granular provisions on algorithmic manipulation, synthetic identity creation, and deepfake detection protocols.
2. Risk of function creep Data collected for benign purposes, such as augmented reality filters, may be repurposed for surveillance, targeted advertising, or political manipulation without renewed consent a phenomenon widely documented in privacy scholarship.

To address these gaps, the Indonesian regulatory framework could benefit from incorporating principles from the *Precautionary Approach* in environmental law requiring risk assessments and preventive measures before deploying technologies with uncertain but potentially severe impacts. This principle has been adapted for AI governance in works by who argue for ex ante evaluation of algorithmic interventions in personal data[16].

In sum, the PDP Law provides a constitutionally grounded and internationally aligned basis for safeguarding altered biometric facial data, drawing on principles of human dignity, informational self-determination, and accountability. Nevertheless, ensuring true legal certainty requires targeted implementing regulations for AI era risks, stronger cross border enforcement mechanisms, and public education initiatives to empower citizens in exercising

---

[13] Smita Khade et al., "Iris Liveness Detection for Biometric Authentication: A Systematic Literature Review and Future Directions," *Inventions* 6, no. 4 (December 1, 2021), https://doi.org/10.3390/INVENTIONS6040065.

[14] By A Elizabeth Holm, "In Defense of the Black Box Black Box Algorithms Can Be Useful in Science and Engineering," *Mon. Not. R. As Tron. Soc* 364, no. Ml (2020): 3282, http://science.sciencemag.org/.

[15] Boquan Li et al., "How Generalizable Are Deepfake Image Detectors? An Empirical Study," August 3, 2024, http://arxiv.org/abs/2308.04177.

[16] Felipe Romero-Moreno, "Deepfake Detection in Generative AI: A Legal Framework Proposal to Protect Human Rights," *Computer Law & Security Review* 58 (September 1, 2025): 106162, https://doi.org/10.1016/J.CLSR.2025.106162.

their data rights[17]. Without these, the normative robustness of the PDP Law risks being undermined by the very technological advances it seeks to regulate.

3.2. Legal Implications of Processing and Using Personal Data in the Form of Digitally Altered or Biometrically Modified Facial Images under the Principles of Personal Data Protection in the Indonesian Personal Data Protection Law (PDP Law)

The processing and use of personal data in the form of facial images that have been digitally altered or processed through biometric technology give rise to significant legal implications, particularly in the context of protecting individual privacy rights as guaranteed under Law Number 27 of 2022 on Personal Data Protection (PDP Law). Philosophically, personal data that is inherent to individuals is part of human rights, as reflected in the values of *Pancasila* and safeguarded under Article 28G paragraph (1) and Article 28H paragraph (4) of the 1945 Constitution of the Republic of Indonesia. Therefore, the face, as a form of biometric data capable of identifying individuals either in its original or altered form, remains within the scope of strict legal protection. The human face, as biometric data, is classified as specific personal data under Article 3 letter (c) of the PDP Law. The defining characteristic of biometric data lies in its ability to uniquely identify a person, even when digitally modified through filters, AI-generated transformations (*such as deepfakes*), or other forms of graphical manipulation. Digitally altered facial data remains subject to legal protection because it retains the potential to identify individuals, either directly or through correlation with supplementary data. The PDP Law does not solely regulate static data but also encompasses data processed through information technology, meaning digitally modified or manipulated facial data remains under the purview of personal data protection[18].

The processing and utilisation of biometric data particularly facial images that have been digitally altered or technologically modified engage profound legal implications, especially within the framework of individual privacy rights guaranteed under Law No. 27 of 2022 on Personal Data Protection (PDP Law). Philosophically, this protection emanates from the constitutional recognition of privacy as a human right under Article 28G(1) and Article 28H(4) of the 1945 Constitution of the Republic of Indonesia (UUD NRI 1945), reflecting Pancasila's commitment to human dignity (*martabat manusia*). In doctrinal terms, this is consistent with the *Right to Informational Self-Determination*, first articulated by the German Federal Constitutional Court in the *Census Decision* (1983), which affirms an individual's authority to control the collection, use, and dissemination of personal information[19].

Facial biometric data is expressly classified as "*specific personal data*" under Article 3(c) of the PDP Law. This classification extends to digitally altered variants whether manipulated through AI-based transformations, *deepfake* synthesis, or graphical modifications if they retain any capacity to uniquely identify an individual. This position aligns with Recital 26 of the EU General Data Protection Regulation (GDPR), which extends protection to data that remains

[17] L. A Bygrave, *Data Privacy Law: An International Perspective.* (Oxford University Press, 2014).
[18] Milkias Ghilom and Shahram Latifi, "The Role of Machine Learning in Advanced Biometric Systems," *Electronics (Switzerland)* 13, no. 13 (July 1, 2024), https://doi.org/10.3390/ELECTRONICS13132667.
[19] Maria Paz Sandoval et al., "Threat of Deepfakes to the Criminal Justice System: A Systematic Review," *Crime Science* 13, no. 1 (December 1, 2024), https://doi.org/10.1186/S40163-024-00239-1.

indirectly identifiable through correlation with supplementary datasets. As noted by Narayanan and Shmatikov, advances in computational analytics have shown that re-identification of altered data is not merely possible but increasingly probable when such data is aggregated with auxiliary information[20].

From a legal standpoint, Article 20(2) of the PDP Law enumerates legitimate grounds for processing, including explicit consent, contractual necessity, legal obligations, vital interests, public interest tasks, and other legitimate interests. Where processing is conducted without valid legal basic particularly for purposes such as commercial advertising, behavioural profiling, or automated decision-making—violations may trigger administrative and criminal sanctions under Articles 57–74. Paul M. Schwartz and Daniel J. Solove have emphasised that in the age of AI, "purpose limitation" must be rigorously enforced to prevent *function creep*, whereby data initially collected for innocuous uses is repurposed for invasive surveillance or targeted manipulation without renewed consent[21].

A particularly salient legal implication concerns profiling. Article 13(f) of the PDP Law grants data subjects the right to object to profiling as the basis for decisions producing legal or similarly significant effects. This reflects Article 22 of the GDPR and resonates with Shoshana Zuboff's critique of "*surveillance capitalism*," in which algorithmic profiling commodifies personal identity traits for predictive and behavioural control. In the context of altered facial data, profiling may lead to discriminatory practices in employment, insurance, or credit scoring, often without the subject's awareness[22].

Responsibility for compliance is shared between the Personal Data Controller and the Personal Data Processor (Articles 1(8)–(9) PDP Law). Under the *Accountability Principle* endorsed by the OECD Privacy Guidelines and elaborated by Lee Bygrave both actors are obliged to implement robust safeguards, including encryption, access controls, and audit mechanisms[23]. Negligent or intentional breaches can result in administrative measures such as suspension of processing and data deletion orders, or criminal penalties, including imprisonment of up to five years and substantial fines (Article 67).

The PDP Law's extraterritorial reach, enshrined in Article 2, allows Indonesia to assert jurisdiction over foreign entities processing its citizens' personal data, provided there is a tangible impact on legal interests within Indonesia. While this mirrors the GDPR's global scope (Article 3), Kuner et al. caution that practical enforcement in cross-border scenarios is constrained by the absence of mutual legal assistance treaties and standardised cross border investigative protocols. Hypothetically, if a Singapore-based AR application uses altered images of Indonesian users for targeted political advertising without consent, jurisdiction may be asserted under the PDP Law, but enforcement would require coordinated international regulatory action[24].

---

[20] Soumyya Kanti Datta, Shan Jia, and Siwei Lyu, "Exposing Lip-Syncing Deepfakes from Mouth Inconsistencies," June 3, 2024, http://arxiv.org/abs/2401.10113.
[21] Florinel-Alin Croitoru et al., "Deepfake Media Generation and Detection in the Generative AI Era: A Survey and Outlook," November 29, 2024, http://arxiv.org/abs/2411.19537.
[22] Croitoru et al.
[23] Kuner, C., Bygrave, L. A., & Docksey, *The EU General Data Protection Regulation (GDPR): A Commentary*.
[24] Kuner, C., Bygrave, L. A., & Docksey.

Another critical implication lies in data security. Article 39 of the PDP Law imposes an obligation on Controllers and Processors to protect personal data against unauthorised access, alteration, or destruction. In the realm of altered biometric data, breaches can have heightened harm potential, as such data may be weaponised for identity theft, misinformation campaigns, or reputational damage. The *Privacy by Design* principle, as advocated by Ann Cavoukian (2011), suggests that security measures should be integrated from the inception of system architecture rather than applied as reactive safeguards.

The explicit consent requirement for processing specific personal data (Article 22 PDP Law) demands heightened clarity and granularity. In practical terms, this necessitates dedicated consent mechanisms for example, opt in checkboxes specifically for biometric data use rather than bundled or implied consent through general terms of service. This aligns with the GDPR's Article 9 and the Council of Europe's Convention 108+, which emphasise the necessity of unambiguous, informed consent for sensitive data processing.

With the rapid proliferation of AI, augmented reality (AR), and virtual reality (VR) technologies, the complexity of regulating altered biometric data has intensified. The PDP Law's provisions on Data Protection Impact Assessments (Articles 34–35) embody the *Precautionary Principle*, mandating that risks to privacy, dignity, and autonomy be evaluated before deployment. However, without AI-specific risk assessment criteria such as bias detection, algorithmic explainability, and synthetic media traceability the practical efficacy of these assessments remains limited[25].

The legal implications of processing and using altered biometric facial images under the PDP Law extend far beyond mere compliance with consent and security requirements. They touch upon deeper normative questions of identity, dignity, and autonomy in a hyper-digitalised society. While the PDP Law provides a robust baseline, its long-term effectiveness will depend on the integration of AI-governance frameworks, international enforcement cooperation, and societal literacy on biometric privacy rights. Without these, the risk remains that legal certainty will be undermined by the very technologies it seeks to regulate.

4. Conclusions

Based on the above discussion, it can be concluded that Law Number 27 of 2022 concerning Personal Data Protection (PDP Law) provides a strong and comprehensive legal certainty for the protection of Indonesian citizens' personal data, including biometric data in the form of facial features, whether in its original form or digitally modified through technologies such as deepfake, AI reconstruction, or medical transformation. The face, as a biometric element, is classified as specific personal data that is sensitive and highly vulnerable to misuse. Therefore, its processing must strictly adhere to fundamental data protection principles, including purpose limitation, accuracy, security, and explicit consent from the data subject. The PDP Law also grants clear legal rights to data subjects to access, amend, withdraw, or delete their personal data and to seek compensation for any violations committed by

[25] Mirko Casu et al., "GenAI Mirage: The Impostor Bias and the Deepfake Detection Challenge in the Era of Artificial Illusions," *Forensic Science International: Digital Investigation* 50 (September 1, 2024), https://doi.org/10.1016/J.FSIDI.2024.301795.

personal data controllers or processors. Through the principle of extraterritoriality, the PDP Law is also capable of addressing transnational violations involving Indonesian citizens.

In terms of recommendations, first, it is essential to increase digital literacy and legal awareness among the public so that individuals are better informed about their rights concerning personal data, including facial data, and more cautious when granting consent on digital platforms. Second, the government and the appointed supervisory authorities must proactively conduct oversight and enforce the law against violations committed by both domestic and foreign entities, especially concerning the misuse of biometric data for commercial or manipulative purposes. Third, electronic system operators, digital applications, and social media platforms must implement strict data security measures, accompanied by clear, transparent, and non-deceptive mechanisms for obtaining explicit consent. Fourth, there is a pressing need for synergy between policymakers, technology experts, and law enforcement authorities in formulating more detailed and adaptive implementing regulations that respond to technological advancements, including artificial intelligence (AI) related to facial data manipulation. Through these efforts, it is expected that the protection of individual privacy rights, particularly regarding digitally altered facial data, can be ensured fairly, effectively, and sustainably in line with the spirit of the PDP Law.

5. Acknowledgments

The author extends sincere gratitude to the academic supervisor, colleagues, and all parties who have provided valuable input and references in the preparation of this article. Appreciation is also conveyed to the educational institution for providing the necessary facilities to support this research.

6. Reference

Boháček, Matyáš, and Hany Farid. "Protecting President Zelenskyy against Deep Fakes," June 24, 2022. http://arxiv.org/abs/2206.12043.

Bygrave, L. A. *Data Privacy Law: An International Perspective.* Oxford University Press, 2014.

Casu, Mirko, Luca Guarnera, Pasquale Caponnetto, and Sebastiano Battiato. "GenAI Mirage: The Impostor Bias and the Deepfake Detection Challenge in the Era of Artificial Illusions." *Forensic Science International: Digital Investigation* 50 (September 1, 2024). https://doi.org/10.1016/J.FSIDI.2024.301795.

Croitoru, Florinel-Alin, Andrei-Iulian Hiji, Vlad Hondru, Nicolae Catalin Ristea, Paul Irofti, Marius Popescu, Cristian Rusu, Radu Tudor Ionescu, Fahad Shahbaz Khan, and Mubarak Shah. "Deepfake Media Generation and Detection in the Generative AI Era: A Survey and Outlook," November 29, 2024. http://arxiv.org/abs/2411.19537.

Datta, Soumyya Kanti, Shan Jia, and Siwei Lyu. "Exposing Lip-Syncing Deepfakes from Mouth Inconsistencies," June 3, 2024. http://arxiv.org/abs/2401.10113.

Dolhansky, Brian, Joanna Bitton, Ben Pflaum, Jikuo Lu, Russ Howes, Menglin Wang, and Cristian Canton Ferrer. "The DeepFake Detection Challenge (DFDC) Dataset," October 28, 2020. http://arxiv.org/abs/2006.07397.

Elizabeth Holm, By A. "In Defense of the Black Box Black Box Algorithms Can Be Useful in Science and Engineering." *Mon. Not. R. As Tron. Soc* 364, no. Ml (2020): 3282. http://science.sciencemag.org/.

Floridi, L., Cowls, J., Beltrametti, M., et al. "An Ethical Framework for a Good AI Society." *Minds and Machines* 4, no. 28 (2018): 689–707.

Ghilom, Milkias, and Shahram Latifi. "The Role of Machine Learning in Advanced Biometric Systems." *Electronics (Switzerland)* 13, no. 13 (July 1, 2024). https://doi.org/10.3390/ELECTRONICS13132667.

Guidotti, Riccardo, Anna Monreale, Salvatore Ruggieri, Franco Turini, Fosca Giannotti, and Dino Pedreschi. "A Survey of Methods for Explaining Black Box Models." *ACM Computing Surveys* 51, no. 5 (September 30, 2019). https://doi.org/10.1145/3236009.

Heidari, Arash, Nima Jafari Navimipour, Hasan Dag, Samira Talebi, and Mehmet Unal. "A Novel Blockchain-Based Deepfake Detection Method Using Federated and Deep Learning Models." *Cognitive Computation* 16, no. 3 (May 1, 2024): 1073–91. https://doi.org/10.1007/S12559-024-10255-7.

Khade, Smita, Swati Ahirrao, Shraddha Phansalkar, Ketan Kotecha, Shilpa Gite, and Sudeep D. Thepade. "Iris Liveness Detection for Biometric Authentication: A Systematic Literature Review and Future Directions." *Inventions* 6, no. 4 (December 1, 2021). https://doi.org/10.3390/INVENTIONS6040065.

Kuner, C., Bygrave, L. A., & Docksey, C. *The EU General Data Protection Regulation (GDPR): A Commentary*. Oxford University Press, 2022.

Li, Boquan, Jun Sun, Christopher M. Poskitt, and Xingmei Wang. "How Generalizable Are Deepfake Image Detectors? An Empirical Study," August 3, 2024. http://arxiv.org/abs/2308.04177.

O'Byrne, J., and M. E. Cates. "Geometric Theory of (Extended) Time-Reversal Symmetries in Stochastic Processes: I. Finite Dimension." *Journal of Statistical Mechanics: Theory and Experiment* 2024, no. 11 (November 30, 2024). https://doi.org/10.1088/1742-5468/ad8f2b.

Romero-Moreno, Felipe. "Deepfake Detection in Generative AI: A Legal Framework Proposal to Protect Human Rights." *Computer Law & Security Review* 58 (September 1, 2025): 106162. https://doi.org/10.1016/J.CLSR.2025.106162.

Samin. "Perlindungan Terhadap Kebocoran Data Pribadi Oleh Pengendali Data Melalui Pendekatan Hukum Progresif." *Jurnal Ilmiah Research Student* 1, no. 3 (2024): 1–15. https://doi.org/https://doi.org/10.61722/jirs.v1i3.386.

Sandoval, Maria Paz, Maria de Almeida Vau, John Solaas, and Luano Rodrigues. "Threat of Deepfakes to the Criminal Justice System: A Systematic Review." *Crime Science* 13, no. 1 (December 1, 2024). https://doi.org/10.1186/S40163-024-00239-1.

Saputra. "Aspek Hukum Telematika Dalam Perlindungan Data Pribadi." *Jurnal Kepastian Hukum Dan Keadilan* 1, no. 5 (2023): 54–74.

Schwartz, P. M., & Solove, D. J. "The PII Problem: Privacy and a New Concept of Personally Identifiable Information." *NYU Law Review* 6, no. 86 (2020).