Volume 22, Number 2, (2025). Pages: 230–262
Istinbath : Jurnal Hukum
ISSN : Print 1829-8117 – Online 2527-3973

ISTINBATH
Jurnal Hukum

Regulating Digital Privacy in Indonesia: The Practice of Data Subject Rights and Controller Duties in the FotoYu App

Dwita Tarisa Putri
Fakultas Hukum, Universitas Padjadjaran, Bandung, Indonesia
E-mail: dwitatarisaputri@gmail.com

Abstract

The practice of personal data protection in artificial intelligence (AI)-based marketplace applications that utilize facial recognition technology (FRT) in Indonesia has not been comprehensively studied. This study analyzes the implementation of data subject rights and the fulfillment of data controller obligations by FotoYu under Law Number 27 of 2022 concerning Personal Data Protection (PDP Law). This study employs a normative juridical method, utilizing primary legal sources such as legislation, secondary sources including scholarly literature and doctrine, and tertiary materials as supporting references. The findings indicate that FotoYu and its Creators have not fully met the core obligations of data controllers, particularly regarding explicit consent, transparency, and effective data deletion mechanisms. Additional challenges arise from inaccurate FRT performance, limited regulatory frameworks on FRT and AI, the absence of implementing regulations for the PDP Law, and a lack of a dedicated data protection authority. This study contributes by providing a normative interpretation of PDP Law provisions in the context of AI-based FRT platforms and offers policy recommendations, including strengthening regulations specific to FRT and AI, accelerating PDP Law implementation regulations, and establishing an independent data protection authority to ensure effective oversight and law enforcement in Indonesia.

Keywords: *Personal Data Protection; Personal Data Subject Rights; Personal Data Control Oblligation; FotoYu.*

Abstrak

Praktik pelindungan data pribadi pada aplikasi marketplace berbasis kecerdasan buatan (AI) yang menggunakan teknologi pengenalan wajah (FRT) di Indonesia belum mendapatkan kajian yang komprehensif. Penelitian ini menganalisis pelaksanaan hak subjek data dan pemenuhan kewajiban pengendali data oleh FotoYu berdasarkan Undang-Undang Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi (UU PDP). Penelitian ini menggunakan metode yuridis normatif dengan memanfaatkan bahan hukum primer berupa peraturan perundang-undangan, bahan hukum sekunder seperti literatur ilmiah dan doktrin, serta bahan hukum tersier sebagai penunjang. Hasil penelitian menunjukkan bahwa FotoYu dan para Kreatornya belum sepenuhnya memenuhi kewajiban utama pengendali data, khususnya terkait persetujuan eksplisit, transparansi, dan mekanisme penghapusan data yang efektif. Tantangan lain juga muncul dari ketidakakuratan kinerja FRT, keterbatasan regulasi mengenai FRT dan AI, belum adanya peraturan pelaksana UU PDP, serta belum terbentuknya otoritas pelindungan data pribadi. Penelitian ini memberikan kontribusi melalui interpretasi normatif terhadap ketentuan UU PDP dalam konteks platform AI berbasis FRT serta menawarkan rekomendasi kebijakan yang mencakup penguatan regulasi khusus FRT dan AI, percepatan penerbitan peraturan pelaksana UU PDP, dan pembentukan lembaga pelindungan data pribadi sebagai otoritas independen untuk memastikan efektivitas pengawasan dan penegakan hukum di Indonesia.

Kata kunci: *Pelindungan Data Pribadi; Hak Subjek Data Pribadi; Kewajiban Pengendali Data Pribadi; FotoYu.*

Istinbath: Jurnal Hukum

Website : http://e-journal.metrouniv.ac.id/index.php/istinbath/index

Received : 2025-06-09 | Published : 2025-12-05.

Introduction

The personal data of Indonesian citizens are currently being used on a massive scale by irresponsible parties as a result of the rapid growth of technology, information, and communication. This phenomenon is an inevitable consequence of the digital age in which we live.[1] According to data from the Ministry of Communication and Digital Affairs (Komdigi) of the Republic of Indonesia, the number of Indonesians using the internet in 2025 will reach 221 million, equivalent to 79.5 percent of the total population of Indonesia. This makes Indonesia is one of the countries with the largest number of

[1] F.U. Puluhulawa, J. Puluhulawa, and M.G. Katili, "Legal Weak Protection of Personal Data in the 4.0 Industrial Revolution Era," *Jambura Law Review* 2, no. 2 (2020): 182–200, https://doi.org/10.33756/jlr.v2i2.6847; J. Nawawi, "LEGAL PROTECTION OF PERSONAL DATA BASED ON REGULATION IN INDONESIA," *Jurnal Al-Dustur* 5, no. 1 (2022): 96–106, https://doi.org/10.30863/jad.v5i1.2581.

Internet users worldwide.[2] The large number of Internet users indicates a high level of technology adoption.[3]

Digital applications that rely on the collection and processing of users' personal data have increased significantly because of increased Internet access.[4] Although digital advances and ease of access have significant economic and social benefits, they also increase the risk of misuse and leakage of personal information. Although Indonesia has Law Number 27 of 2022 concerning Personal Data Protection (PDP Law), academic concerns continue to arise due to the high rate of data leakage.[5]

Although this regulation should provide protection, data show that there is a gap in the current implementation. A report released by one of the national cyber threat intelligence platforms shows that, during the first half of 2025, there were 133.4 million cyber-attacks.[6] Furthermore, based on Global Data Breach Statistics, Indonesia currently ranks 14th in the world in terms of personal data breaches.[7] This phenomenon shows that it is very important to implement a comprehensive personal data protection system, especially with the increasing use of digital applications based on personal data.

In this case, digital applications such as FotoYu are relevant case studies. FotoYu is a marketplace that sells photos of people running in marathons. FotoYu utilizes artificial intelligence (AI) and facial recognition technology (FRT). In the photo buying and selling process, this application connects photographers (called Creators) with users (called *Yusers*) through facial biometric data processing,[8] which is specific personal data based on Article 4 paragraph (2) letter b of the PDP Law. Therefore, FotoYu faces the challenge of implementing personal data protection, which is quite complex, especially

[2] Kementerian Komunikasi dan Digital, "Komitmen Pemerintah Melindungi Anak Di Ruang Digital," Komdigi, 2025, https://www.komdigi.go.id/berita/artikel/detail/komitmen-pemerintah-melindungi-anak-di-ruang-digital.

[3] U. Enggarsasi, N.K. Sa'diyah, and P.A. Martio, "LEGAL SAFEGUARDS FOR VICTIMS OF DATA DISSEMINATION CRIMES AND CYBERCRIME PROTECTION," *Jurnal Hukum Unissula* 40, no. 2 (2024): 258–77, https://doi.org/10.26532/jh.v40i2.39974.

[4] F.S. Utama, D.E. Purwoleksono, and T. Rachman, "Data Leakage of the Indonesian Elections Commission in Legal Aspects of Personal Data Protection," *Media Iuris* 7, no. 3 (2024): 479–98, https://doi.org/10.20473/mi.v7i3.55931.

[5] N.A. Rendreana, S. Cahyono, and R.A. Wijayanti, "Implementation of Gamification to Enhance Understanding of Personal Data Protection Based on Republic of Indonesia Law Number 27 of 2022," 2023, 246–51, https://doi.org/10.1109/ICIMCIS60089.2023.10349080.

[6] Cahyadaru Kuncorojati, "133 Juta Serangan Siber Hantam Indonesia, Ancam Celah Keamanan Dan Botnet Iot," Medcom.Id, 2025, https://www.medcom.id/teknologi/news-teknologi/5b2wOjnk-133-juta-serangan-siber-hantam-indonesia-ancam-celah-keamanan-dan-botnet-iot.

[7] Personal data protection in P2P lending: What Indonesia should learn from Malaysia?

[8] FotoYu, "Cara Kerja FotoYu," FotoYu, https://www.fotoyu.com/how-it-works.

in relation to fulfilling the rights of personal data subjects and FotoYu's responsibility as a personal data controller mandated by the PDP Law.

Several previous studies have examined the implementation of the PDP Law, including Nabiha's study on the data leak at the Temporary National Data Center (PDNS) on June 20, 2024, which shows that public agencies and personal data controllers have not fully complied with the data protection obligations mandated by the PDP Law, resulting in weak security systems, a lack of transparency, and slow handling of personal data leak incidents.[9] Jonathan's study also shows that awareness of the urgency of the role as a controller and processor of personal data can be increased through legal education, so that it can result in good law implementation.[10] Furthermore, Aulia [11] and Adri[12] also found that the implementation of the PDP Law faces challenges such as low public awareness, inadequate infrastructure, unprepared legal and institutional systems, and low accountability.

Regarding FRT, research by Rahmat and Lukman emphasizes that regulations regarding the use of FRT and improving FRT security are needed. This is because there is a risk of misuse that could threaten privacy. [13] Sarimah (2024) also found that more specific regulations are needed for the use of FRT because Indonesia does not yet have specific regulations on this matter. In addition, the regulations on FRT currently available in the PDP Law are limited.[14]

[9] Nabiha Khansa Rusyda, "Perlindungan Hukum Erhadap Subjek Data Kebocoran Data Oleh Badan Publik Menurut UU Nomor 27 Tahun 2022," *Desentralisasi : Jurnal Hukum, Kebijakan Publik, Dan Pemerintahan* 2, no. 3 (2025): 260, https://doi.org/10.62383/desentralisasi.v2i3.940.

[10] Jonathan Matthew Pakpahan, "Kesadaran Urgensi Peran Pengendali Dan Prosesor Data Pribadi Dalam Rangka Pelindungan Data Pribadi Individu Berdasarkan Undang-Undang Nomor 27 Tahun 2022 Tentang Pelindungan Data Pribadi," *Jurnal Hukum To-Ra : Hukum Untuk Mengatur Dan Melindungi Masyarakat* 10, no. 1 (2024): 131, https://doi.org/10.55809/tora.v10i1.331.

[11] Aulia Alayna Suvil et al., "Implementasi Perlindungan Data Pribadi Berdasarkan Undang-Undang Nomor 11 Tahun 2020," *Jurnal Hukum, Politik Dan Ilmu Sosial* 3, no. 4 (2024): 75, https://doi.org/10.55606/jhpis.v3i4.4235.

[12] Muhamad Adri Rinjani and Ricky Firmansyah, "Hambatan Implementasi UU 27/2022 Dan Strategi Penguatan Perlindungan Data Pribadi Di Indonesia," *Jurnal Analisis Hukum* 8, no. 1 (2025): 78, https://doi.org/10.38043/jah.v8i1.6793.

[13] Rahmat Rambe and Lukman Abdurrahman, "Implikasi Etika Dan Hukum Dalam Penggunaan Teknologi Pengenalan Wajah: Perlindungan Privasi Versus Keamanan Publik," *Jurnal Hukum Caraka Justitia* 4, no. 2 (2024): 99, https://doi.org/10.30588/jhcj.v4i2.1828.

[14] Sarimah Yemima Br Girsang, "Pentingnya Regulasi Khusus Sistem Face Recognition Technology Sebagai Produk Artificial Intelligence Dalam Peningkatan Keamanan Dan Penegakan Hukum Di Indonesia," *Nommensen Journal of Legal Opinion* 05 (2024): 87, https://doi.org/10.51622/njlo.v5i2.1817.

In the context of FotoYu, previous research by Athallah examined how economic rights over portraits are applied in commercialization through the FotoYu application. This study focused on copyright aspects by examining Law Number 28 of 2014 concerning Copyright (Copyright Law), which indicates that a person's portrait sold on the FotoYu application without that person's permission has the potential to violate the provisions of Article 12 of the Copyright Law.[15] However, this study has not comprehensively discussed the mechanism of explicit consent for personal data processing and the obligations of personal data controllers under the PDP Law, as well as the use of FRT in the FotoYu application.

Based on the above description, unlike the studies mentioned above, this study examines how the obligations of personal data controllers in the PDP Law are applied concretely in AI-based platforms, as in the case of FotoYu. This gap in the literature forms the research gap and becomes the position of this study. Therefore, this study aims to comprehensively analyze the provisions of the PDP Law in the case of FotoYu, focusing on two main issues: (1) how are the rights of personal data subjects and the obligations of personal data controllers implemented in the FotoYu application based on the PDP Law? (2) What are the challenges and legal loopholes that arise in the practice of personal data processing in the FotoYu application? This study is important because it addresses a contemporary social phenomenon that needs to be addressed with comprehensive, up-to-date research.

Methods

This study uses a normative juridical approach, focusing on the norms, principles, and legal regulations that apply and are relevant to the issues discussed. Theoretically, this study is based on the theory of law enforcement proposed by Soerjono Soekanto, who views law enforcement as a process of harmonizing the values embodied in legal rules with actual behavior patterns in society. Law enforcement aims to realize, maintain, and preserve peace in social interaction. Thus, the essence of law enforcement is an effort to realize the values of justice and truth contained in legal norms in a concrete social practice.[16]

[15] Athallah Rafidiansyah, "Hak Atas Potret Dalam Komersialisasi Pada Aplikasi FotoYu: Tinjauan Hak Cipta" (2025).

[16] Soerjono Soekanto, *Penegakan Hukum* (Jakarta: Bina Citra, 1983), 13.

The research specification used is descriptive analytical, which explains legislation by relating it to legal principles and doctrines and assessing its implementation in practice. The data used come from secondary legal sources, including primary legal materials (laws and regulations), secondary legal materials (literature, doctrines, previous research results), and tertiary legal materials (dictionaries and other supporting sources). All these materials were used complementarily to support the normative analysis that is the focus of this study. Textual analysis was used to analyze the content of legal norms, comparative analysis to compare regulations and implementation practices in the FotoYu application, and critical analysis to evaluate the suitability and obstacles in the implementation of data subject rights and data controller obligations based on the PDP Law. The use of artificial intelligence (AI) in this research is positioned as a tool to assist in data display, digital reference management, and translation (although the manuscript is still proofread by experts).

Results and Discussion

Implementation of Personal Data Subject Rights and Personal Data Controller Obligations in the FotoYu Application

In Indonesia, the massive adoption of digital applications and advances in AI technology have resulted in many innovations and challenges in personal data protection.[17] In the global landscape, Indonesia's position is often compared to that of the European Union, which has already established data protection standards through the GDPR. This regulation is one of the most comprehensive and strictest regulations.[18]

Compared to the GDPR, the PDP Law has not yet established a classification of personal data types that can be deleted. In addition, the technical concept of personal data has not been clearly explained in legislation. A data deletion notification mechanism is also not yet available because, in practice, this process must go through a court decision.[19] This situation is inseparable from the absence of a special and independent institution

[17] Y. Hoca, D. Firat, and E. Çağlar, "Principles of Data Privacy and Security in a Cyber World," in *Handbook of Research on Cyber Law, Data Protection, and Privacy* (2022), 1–19, https://doi.org/10.4018/978-1-7998-8641-9.ch001.

[18] Rizka Putri Awwaliyah and Sony Juniarti, "Perbandingan General Data Protection Regulation (GDPR) Dengan Regulasi Perlindungan Data Di Negara-Negara Asia Tenggara," *Jurnal Hukum Dan Kewarganegaraan* 4, no. 4 (2024): 1, https://doi.org/10.3783/causa.v4i4.3535.

[19] K. Kaczmarek, M. Karpiuk, and C. Melchior, "A Holistic Approach to Cybersecurity and Data Protection in the Age of Artificial Intelligence and Big Data," *Prawo i Wiez* 50, no. 3 (2024): 103–21, https://doi.org/10.36128/PRIW.VI50.907.

authorized to oversee the use of data by service providers, as well as the lack of standardization of a uniform Privacy Policy.[20]

In this context, the PDP Law serves as a national legal umbrella that provides an important foundation for personal data protection. Article 1 paragraph 1 of the PDP Law defines personal data as *"data about an individual who is identified or can be identified individually or in combination with other information, either directly or indirectly, through electronic or non-electronic systems."* Based on this definition, there is a strong legal foundation for protecting various types of information that can be linked to an individual's identity.[21]

Furthermore, Article 4 of the PDP Law classifies personal data into two categories: general and specific. General personal data include full name, gender, nationality, religion, marital status, and/or personal data that are combined to identify a person. Specific personal data include health data and information, biometric data, genetic data, criminal records, child data, personal financial data, and/or other data in accordance with laws and regulations. In addition, the PDP Law stipulates a number of rights for personal data subjects and imposes obligations on personal data controllers.

In this case, case studies are very important to evaluate the effectiveness of the PDP Law's implementation, particularly the fulfillment of the rights of personal data subjects and the implementation of the obligations of personal data controllers. One of the things that can be studied is the implementation of the provisions of the PDP Law in the FotoYu application, which is a marketplace that sells photos of people running. FotoYu utilizes artificial intelligence (AI) and facial recognition technology (FRT). In the process of buying and selling photos, this application connects photographers (called creators) with users (called *Yusers*) through facial biometric data processing.[22]

To examine the implementation of the PDP Law in the FotoYu application, it is important to first understand the legal position of the parties involved in the FotoYu application. In the process of buying and selling photos on the FotoYu application, the

[20] Syafira Agata Ramadhani, "Komparasi Pengaturan Perlindungan Data Pribadi Di Indonesia Dan Uni Eropa Comparison of Personal Data Protection Regulation in Indonesia and the European Union," *Rewang Rencang : Jurnal Hukum Lex Generalis.* 3, no. 1 (2022): 81, https://doi.org/10.56370/jhlg.v3i1.173.

[21] Muhamad Hasan Rumlus and Hanif Hartadi, "Kebijakan Penanggulangan Pencurian Data Pribadi Dalam Media Elektronik," *Jurnal HAM* 11, no. 2 (2020): 285, https://doi.org/10.30641/ham.2020.11.285-299.

[22] FotoYu, "Cara Kerja FotoYu."

activities are carried out by Creators and Users, with FotoYu as the platform that connects the two. This creates complex legal issues, especially in terms of determining who has the obligation to act as the controller of personal data, as well as how to fulfill the rights of personal data subjects.

Article 1 paragraph 6 of the PDP Law states that "*personal data subjects are individuals to whom personal data is attached.*" In the context of FotoYu, people who are photographed by Creators and whose photos are uploaded to the FotoYu application are categorized as personal data subjects because personal data in the form of photos of themselves, which is general personal data, is attached to them.[23] Meanwhile, Article 1 point 4 of the PDP Law states that "*a personal data controller is any person, public agency, and international organization that acts individually or jointly in determining the purpose and controlling the processing of personal data*." Therefore, in this case, the role of the personal data controller is held by the company that manages FotoYu.

However, complexity arises from the role of creators as the parties who upload photos to the FotoYu application. Creators are not merely content providers; they are the first parties to collect personal data, such as facial photos and location data, which are uploaded and processed by the RoboYu system. In this case, joint controllership can be seen from the involvement of both parties, namely FotoYu and the Creator, in determining the purpose (selling photos) and exercising control over the processing of personal data, so that the controller of personal data is not only the FotoYu company but also the Creator.

Although the PDP Law does not explicitly define joint controllers, the concept in the GDPR provides a relevant analytical framework. The GDPR states that two or more controllers can be considered joint controllers if they jointly determine the purpose and means of processing personal data.[24] Based on this framework, FotoYu's practices show a substantial division of roles between the platform and creators, so that both are factually involved in determining the purposes and means of processing. [25] Thus, from a GDPR

[23] Hayatun Nufus and Moh Soleh, "Tinjauan Yuridis Dalam Kasus Memotret Orang Tanpa Izin Untuk Kepentingan Komersial," *Jurnal Cakrawala Akademika* 2, no. 1 (2025): 1004, https://doi.org/10.70182/JCA.

[24] I. Rahmatullah, "FINANCIAL TECHNOLOGY AND THE LEGAL PROTECTION OF PERSONAL DATA: The Case of Malaysia and Indonesia," *Al-Risalah: Forum Kajian Hukum Dan Sosial Kemasyarakatan* 20, no. 2 (2020): 197–214, https://doi.org/10.30631/alrisalah.v20i2.602.

[25] Ayça Zorluoğlu Yilmaz, "Joint Controllership Under the GDPR - Concept, Responsibilities, and Liability," *Juridical Tribune - Review of Comparative and International Law* 15, no. 1 (2025): 97, https://doi.org/10.62768/TBJ/2025/15/1/06.

perspective, the relationship between FotoYu and Creators potentially qualifies as joint controllership, implying that several conditions must be met.

The PDP Law requires the existence of an agreement between the controllers of personal data that contains the roles, responsibilities, and relationships between the controllers of personal data; interrelated purposes and methods of processing personal data that are determined jointly; and a jointly appointed contact person, as stipulated in Article 18, paragraphs (1) and (2) of the PDP Law.

Furthermore, the processing of personal data by FotoYu and Creators requires them to implement very strict compliance standards. The PDP Law has become a strong foundation for guaranteeing the rights of personal data subject. The rights of personal data subjects are regulated in Articles 5–11 of the PDP Law, including:

Table 1. Rights of Personal Data Subjects in Articles 5 - 11 of the Personal Data Protection Act (PDP)

No.	Data Subject Rights	Explanation
1.	Right to obtain information	Obtain information regarding the clarity of identity, legal basis, purpose of request and use of personal data, as well as the accountability of the party requesting personal data
2.	Right to correct data	Complete, update, and/or correct errors or inaccuracies in personal data in accordance with the purpose of personal data processing
3.	Right of access and copy	Obtain access to and copies of personal data in accordance with the provisions of laws and regulations
4.	Right to terminate processing/deletion	Terminate processing, delete, and/or destroy personal data in accordance with the provisions of laws and regulations
5.	Right to withdraw consent	Withdraw consent to the processing of personal data that has been given to the data controller
6.	Right to object	Object to decisions based solely on automated processing, including profiling, which produce legal effects or significantly affect you

7.	Right to suspend or restrict processing	Suspend or restrict the processing of personal data in accordance with the purposes of the processing
8.	Right to sue and receive compensation	Sue and obtain compensation for violations of personal data processing in accordance with the provisions of laws and regulations
9.	Right to obtain/use data in a specific format	Obtaining or using personal data in a form that is compatible with commonly used or machine-readable structures or formats
10.	Right to transfer data	Using and sending personal data to another data controller as long as the systems can communicate securely with each other

Source: Data processed by the author

To ensure the fulfillment of the rights of personal data subjects, the PDP Law imposes a number of obligations on personal data controllers, as stipulated in Articles 20-49 of the PDP Law, with the following details:

Table 2. Obligations of Personal Data Controllers

No.	Obligations Data Controller	Explanation
1.	Have a basis for data processing	Personal data processing must have a legal basis
2.	Provide evidence of consent	Keep evidence of consent given by the data subject
3.	Processing of children's data	Performing specific processing of children's personal data
4.	Processing of data on persons with disabilities	Processing personal data on persons with disabilities in a specific manner
5.	Limited and transparent processing	Processing data in a limited, lawful, and transparent manner
6.	Processing in accordance with the purpose	Processing data in accordance with the specified purpose

7.	Ensuring data accuracy	Ensuring accuracy, completeness, and consistency through verification
8.	Updating/correcting data	Updating or correcting errors within 3x24 hours and notifying the results
9.	Recording of activities	Recording all personal data processing activities
10.	Providing access	Providing access and processing records to data subjects in accordance with the storage period
11.	Impact assessment	Conducting high-risk assessments on personal data processing
12.	Data security	Protecting and ensuring the security of personal data
13.	Data confidentiality	Maintaining the confidentiality of personal data
14.	Supervision of related parties	Supervising every party involved in data processing under the controller's control
15.	Protecting from unlawful processing	Protecting personal data from unlawful processing
16.	Preventing unauthorized access	Preventing illegal access using reliable and secure electronic systems
17.	Stopping processing	Stopping processing if consent is withdrawn
18.	Delaying/limiting processing	Delay or restrict processing in whole or in part within 3x24 hours of the request
19.	Delete data	Delete personal data that is no longer needed or for which consent has been withdrawn
20.	Destroy data	Destroy personal data after the retention period has expired or under certain conditions
21.	Notification of deletion/destruction	Notify the data subject of the deletion or destruction of data
22.	Notification of protection failure	Provide written notification within a maximum of 3x24 hours in the event of a data protection failure
23.	Accountability	Be responsible for data processing and demonstrate compliance with PDP principles

24.	Notification of data transfer	Notify the transfer of personal data in the event of a merger, separation, takeover, consolidation, or dissolution of a legal entity
25.	Carry out institutional orders	Carry out institutional orders related to the implementation of personal data protection

Source: Data processed by the author

As controllers of personal data, FotoYu and Creators must fulfill the above obligations, one of which is to have a basis for processing personal data in accordance with Article 20 of the PDP Law. One such basis for processing personal data is the existence of explicit and valid consent from the subject of the personal data for specific purposes communicated by the data controller to the subject of the personal data. In addition to the purpose of processing, when requesting consent, the personal data controller must also provide information regarding the legality of personal data processing, the type and relevance of personal data to be processed, the retention period of documents containing personal data, details of the information collected, the period of personal data processing, and the rights of the personal data subject, as stipulated in Article 21 of the PDP Act, as follows: Furthermore, Article 22 of the PDP Law emphasizes that such consent must be written or recorded, either electronically or non-electronically.

In the context of FotoYu, the Creator took photos freely without obtaining permission from the concerned parties. The Creator continues to photograph anyone they deem suitable for photography amid the hustle and bustle of the runners, which is then uploaded to the FotoYu application.[26] This shows that in the processing of personal data, namely the photos, FotoYu and the Creator did not have explicit legal consent. In this case, the practice can be classified as a violation and is subject to administrative sanctions, as stipulated in Article 57, paragraph (1) of the PDP Law.

This not only shows non-compliance with written norms but also illustrates the weakness of law enforcement in a broader sense. According to Soerjono Soekanto, law enforcement is the process of harmonizing the relationship between the legal values

[26] Rizal Amril Yahya, "Pudarnya Privasi Kita Di Hadapan Kamera Liar," Tirto.Id, 2025, https://tirto.id/pudarnya-privasi-kita-di-hadapan-kamera-liar-hdcD#google_vignette.

contained in the rules and actual behavior in society, so that justice and truth are created.[27] When basic mechanisms such as explicit consent are not implemented, the values that should be embodied by the PDP Law are not properly enforced. Thus, FotoYu's practice shows that legal norms are in place, but their effectiveness is not achieved because their implementation and fulfillment are not carried out as they should be.

FotoYu and Kreator can also be sued by personal data subjects for violations of personal data processing, in accordance with Article 12 paragraph (1) of the PDP Law. In addition, this practice has the potential to lead to criminal acts, as regulated in Article 65 of the PDP Law, which reads as follows:

> *"(1) Everyone is prohibited from unlawfully obtaining or collecting personal data that does not belong to them with the intention of benefiting themselves or others, which may result in harm to the subject of the personal data.*
> *(2) Everyone is prohibited from unlawfully disclosing personal data that does not belong to them.*
> *(3) Everyone is prohibited from unlawfully using personal data that does not belong to them."*

FotoYu and Creators must also fulfill the rights of each personal data subject to terminate the processing, deletion, and/or destruction of their personal data, as stated in Article 8 of the PDP Law. In the FotoYu application, there is no deletion mechanism for personal data subjects who object to being photographed. This makes the implementation of the rights of personal data subjects not systematically integrated. In practice, FotoYu Creators acknowledge that photo subjects can only submit objections directly to the Creators and request that the photos be deleted.[28] Dependence on the response of each creator is a serious weakness in implementation. If the Creator refuses or does not respond, the right to delete the data cannot be effectively fulfilled. This mechanism creates legal uncertainty because rights that should be guaranteed by law become highly dependent on the good faith of other parties rather than on technical procedures guaranteed by the system.

Furthermore, FotoYu does not provide clear information regarding the processing period for personal data in the form of photos; therefore, it is unclear how long the photos

[27] Soerjono Soekanto, *Kesadaran Hukum Dan Kepatuhan Hukum* (Jakarta: CV. Rajawali, 1982).

[28] Ali, "FH UNS-Mafindo Bahas Marketplace Fotografi, Pengguna Dan Fotografer FotoYu Harus Saling Melindungi," Joglosemar News.Com, 2025, https://joglosemarnews.com/2025/03/fh-uns-mafindo-bahas-marketplace-fotografi-pengguna-dan-fotografer-fotoyu-harus-saling-melindungi/.

will remain on the FotoYu application. This information should be provided when requesting consent for the processing of personal data as the basis for processing personal data, as stipulated in Article 21, paragraph (1), letter f of the PDP Law. However, neither FotoYu nor the Creator requested consent from the data subjects regarding the processing of personal data in the form of photos of the runners, as mentioned earlier.

In addition to photos, FotoYu processes general personal data in the form of location data. Although location data are considered general personal data, they can pose a significant risk when combined with other data.[29] A person's movement patterns can reveal sensitive information about their political or religious affiliations, workplace, place of residence, and daily routine. FotoYu processes not only general personal data but also specific personal data, namely, facial biometric data. In FotoYu, facial biometric and location data are combined to display photos of people, including the places where they were at a certain time.

Biometric data are highly sensitive and vulnerable to misuse owing to their unique, difficult-to-falsify, and permanent nature. [30] First, these data cannot be changed, which means that a person cannot change their identity as they would change a password.[31] Second, advances in deepfake technology show that facial biometric data can be used to create highly sophisticated and manipulative content. [32] Third, with increasingly sophisticated algorithms, facial biometric data can reveal other sensitive information, such as health conditions. As a result, biometric data require higher protection. This is regulated in Article 34 paragraphs (1) and (2) letter b, which states that in the processing of specific personal data that has a high potential risk, the personal data controller is required to conduct a personal data protection impact assessment.

In the FotoYu application, Yuser's facial biometric data are processed by RoboYu using FRT, which generates documentation photos that match Yuser's face. After the

[29] Edi Saputra Hasibuan and Elfirda Ade Putri, "Perlindungan Keamanan Atas Data Pribadi Di Dunia Maya," *Jurnal Hukum Sasana* 10, no. 1 (2024): 72, https://doi.org/10.31599/sasana.v10i1.2134.

[30] Miyuki Fattah Rizki and Abdul Salam, "Pertanggungjawaban Hukum Pengumpulan Data Biometrik Melalui Artificial Intelligence Tanpa Persetujuan Pemilik Data (Studi Kasus Clearview AI Inc. Di Yunani Dan Inggris)," *Lex Patrimonium* 2, no. 2 (2023): 2.

[31] Felix Yeovandi and Eko Prasetyo, "Evaluasi Keamanan Sistem Autentikasi Biometrik Pada Smartphone Dan Rekomendasi Implementasi Optimal," *JTIM : Jurnal Teknologi Informasi Dan Multimedia Evaluasi Keamanan Sistem Autentikasi Biometrik* 7, no. 1 (2025): 134, https://doi.org/10.35746/jtim.v7i1.653.

[32] Michelle Lucia Korengkeng, Roy Ronny Lembong, and Feiby S. Wewengkang, "ANALISIS TINDAK PIDANA DEEPFAKE PORNOGRAFI DALAM PERSPEKTIF UNDANG-UNDANG INFORMASI DAN TRANSAKSI ELEKTRONIK," *Jurnal Fakultas Hukum UNSRAT* 13, no. 3 (2025): 7.

matching process, RoboYu asks for confirmation with the question “Is this you?”, which can only be answered with the options “Yes or No”. However, another problem that arises is that someone can still choose the “Yes” option and purchase the photo, even if the photo is not of them. This practice raises critical questions regarding FotoYu's obligation to prevent illegal access to personal data by other parties using a reliable, secure, and responsible security and/or electronic system.

In fact, FotoYu only urges that “*sometimes RoboYu will offer documentation photos that are considered similar, but may not be you. Ethically, you should only confirm if the documentation photo is really, you and reject documentation photos that are not you*”.[33] However, this shows that FotoYu only takes preventive measures by urging users to purchase only photos of themselves; in other words, it only expects self-awareness from the users, but does not implement reliable, secure, and responsible security and/or electronic systems.

Another problem that arises from this practice is accountability. The absence of a clear accountability mechanism in FotoYu creates legal uncertainty and has the potential to harm the rights of personal data subjects in the event of a personal data breach. FotoYu and Creators, as personal data controllers, should have an agreement that outlines the roles, responsibilities, and relationships between personal data controllers. However, it is not difficult to become a Creator in the FotoYu application. In the application, there are three categories of creators: basic, verified, and host creators. Basic creators are all *Yusers* aged 13 years or older, who are automatically registered as basic creators. Verified creators are *Yusers* who have verified their accounts using their ID cards or passports. Meanwhile, host creators are verified creators who are members of the hashtag hosts.[34]

All Creator categories can upload photos to the FotoYu app to sell them, without any prior agreement between FotoYu and the Creator. Therefore, there is no clear accountability mechanism regarding who is responsible in the event of a breach of personal data. This ambiguity creates a legal loophole that can be exploited to avoid responsibility, where creators can argue that they only provide content, while FotoYu can argue that they only provide a platform. This situation reflects a broader problem in the

[33] FotoYu, “Cara Kerja FotoYu.”

[34] FotoYu.

digital economy, where the platform business model often blurs the boundaries of legal responsibilities.

Based on the above description, it can be seen that FotoYu and Creators, as controllers of personal data who have a number of obligations to fulfill the rights of personal data subjects, have not fully implemented these obligations. This shows that FotoYu has not yet fully developed an adequate system to guarantee the fulfillment of the rights of personal data subjects in the EU.

Challenges and Legal Loopholes Arising from Personal Data Processing Practices in Photo Applications

The processing of personal data in FotoYu applications faces significant challenges and legal loopholes in terms of personal data protection in Indonesia. FotoYu, a personal documentation marketplace platform with AI technology that uses FRT in its RoboYu feature for facial recognition, operates in a legal environment that still has various regulatory limitations. FotoYu's use of AI with FRT raises complex legal issues because it involves the processing of biometric data, which is specific personal data as regulated in the PDP Law.

FotoYu collects facial biometric data through the FRT feature and combines it with location data to enable users to find their photos based on facial likeness. A negative impact of using FRT is that it can identify a person's face without their knowledge or consent. In addition, facial biometric data collected by electronic system operators in the industry can be used for purposes that are not desired by the person or are distributed without their consent.[35]

Another negative impact of using FRT is its inaccuracy, which is a major challenge in the practice of personal data processing in the FotoYu application. The FRT used in the FotoYu application faces a fundamental problem: its accuracy level is not optimal. Various studies have shown that FRT technology has a relatively high error rate. The FRT currently used in Indonesia has weaknesses in its algorithm processing, which is an obstacle when recognizing faces. For example, the maximum camera distance for capturing images using FRT is only between 2 and 5 m, and the height position cannot exceed 3 m. This technology has the worst potential, with an error rate of up to 35% when

[35] Ghazali Hasan Nasakti, "IUS CONSTITUENDUM PENGGUNAAN TEKNOLOGI PENGENALAN WAJAH DALAM INDUSTRI DAN PENEGAKAN HUKUM DI INDONESIA," *Prosiding Konferensi Mahasiswa Nasional Ubaya Law Fair Tahun 2021*, 2021, 356.

trying to recognize the faces of dark-skinned women; however, it is more accurate when used to recognize men with lighter skin.[36]

The case of Ade Armando is an example of the inaccuracy of the FRT. The Metro Jaya Regional Police successfully identified several perpetrators of an assault on a lecturer at the University of Indonesia using FRT, but the FRT failed to identify the actual perpetrators of the assault. It was not proven that Try Setia Budi Purwanto and Abdul Manaf were involved in the assault on the victim. The police claimed that the inaccurate FRT was the cause of the error.[37]

Therefore, despite the sophistication of FRT, this technology is not error-free and is prone to misidentifications.[38] The inaccuracy of this system can be influenced by various factors, such as poor lighting conditions, physical changes, and algorithmic biases that discriminate against individuals with certain skin colors.[39] The impact of this inaccuracy can be far-reaching, potentially violating the privacy rights of data subjects whose photos are used without their permission. As the controller of personal data, FotoYu has an obligation to prevent illegal access to personal data. In this case, FotoYu claims that Yuser's facial biometric and location data cannot be accessed by all FotoYu staff, except for maintenance purposes.[40] However, FotoYu's actions are misguided because they do not prevent runners' photos from being accessed without authorization by others but only prevent unauthorized access to users' facial biometric data and location data.

Furthermore, in the FotoYu application, there is an option that Yusers can select to set the RoboYu search accuracy level to nine levels, ranging from "medium" to find more content, to "high" for fewer but more accurate results. [41] However, providing a lower-accuracy option creates new problems. Indirectly, FotoYu transfers some of the risk of misidentification to Yuser. If Yuser chooses the "medium" accuracy level and

[36] Floubianca Viola, "Potensi Pelanggaran Hak Privasi Dalam Penggunaan Face Recognition Untuk Pengawasan Keamanan Di Ruang Publik" (Universitas Katolik Parahyangan, 2023), 3.

[37] Yopi Prayitno, "Pertanggungjawaban Perdata Perusahaan Nodeflux Atas Kerugian Pengguna Akibat Kesalahan Output Teknologi Artificial Intelligence (Face Recognition)" (Universitas Sriwijaya, 2024), 19.

[38] M.A. Tulay and S. Olatunbosun, "Cybersecurity Techniques, Emerging Threats, and Industry Responses," 2262 (2025): 336–53, https://doi.org/10.1007/978-3-031-85933-5_25.

[39] Aldi Pebrian Simatupang, *Penerapan Algoritma Deep Learning Dalam Pengenalan Wajah Untuk Sistem Keamanan*, 01 (2025): 9.

[40] FotoYu, "Cara Kerja FotoYu."

[41] FotoYu.

RoboYu mistakenly displays photos that do not belong to Yuser; FotoYu can argue that it was Yuser who chose the "medium" accuracy option. This issue provides clear evidence of the urgent need for specific regulations related to FRT, including accuracy standards.

Although the PDP Law recognizes biometric data as specific personal data in Article 4, paragraph (1), letter b, this law does not provide specific operational provisions regarding the use of facial recognition technology, including minimum accuracy standards.[42] The absence of specific FRT regulations may hinder FotoYu in determining the limits of permissible biometric data processing, particularly for algorithm training and long-term storage.[43] In addition, the use of FRT without a strong legal basis can easily be misused for the purposes of mass surveillance, tracking citizens without transparency, and excessive monitoring of public spaces, all of which can reduce freedom of expression and assembly and undermine the integrity and honor of individuals before the state and society.

The importance of specific regulations on the use of FRT systems in improving security and law enforcement in Indonesia cannot be ignored, given that the rapid and increasing development of AI requires a strong legal basis beyond general regulations, such as the PDP Law. Indonesia must have detailed regulations governing the use of biometric technologies, such as FRT, to provide legal certainty and adequate protection for personal data subjects.

The necessary regulations on FRT must include specific requirements, such as accountability reports, ongoing training, accuracy benchmark testing, data resilience and security, and impact assessments on individuals from the use of FRT. These regulations also need to include stricter consent mechanisms, algorithm transparency, and the right of data subjects to refuse the processing of biometric data.

In addition to the legal vacuum regarding the use of FRT, Indonesia currently faces a legal vacuum regarding the use of AI, resulting in uncertainty regarding legal liability when AI systems make mistakes or cause losses. In Indonesian law, legal liability

[42] M.H. Hisbulloh, "URGENSI RANCANGAN UNDANG-UNDANG (RUU) PERLINDUNGAN DATA PRIBADI," *Jurnal Hukum Unissula* 37, no. 2 (2021): 119–33, https://doi.org/10.26532/jh.v37i2.16272.

[43] Nur Husna, Moh Nurman, and Yudhistira Nugroho, "Pembentukan Peraturan Pemerintah Tentang Face Recognition Technology Ditinjau Dari Undang-Undang Nomor 27 Tahun 2022 Tentang Perlindungan Data Pribadi," *Jurnal Ilmiah AKSES*, no. 2 (2025): 4.

can generally only be imposed on legal subjects, namely individuals (*natuurlijke persoon*) or legal entities (*rechtspersoon*).[44] This fundamental problem complicates the determination of responsibility when the RoboYu system in FotoYu makes an identification error, resulting in unauthorized access to photos that do not belong to the person.

AI is a form of programming on a computer device to perform careful data processing and/or analysis, as stated in the Circular Letter of the Minister of Communication and Information Technology Number 9 of 2023 concerning Artificial Intelligence Ethics. Article 1 point 8 of Law Number 11 of 2008 concerning Electronic Information and Transactions, as last amended by Law Number 1 of 2024 concerning the Second Amendment to Law Number 11 of 2008 concerning Information and Electronic Transactions (ITE Law), states that, "An Electronic Agent is a device of an Electronic System that is made to perform an action on certain Electronic Information automatically, which is organized by a Person." In this case, AI can be equated to an electronic agent because it has the characteristics of automated information processing; therefore, AI as an electronic agent cannot be used as a legal subject but can only be classified as a legal object.[45]

Currently, regulations regarding the use and accountability of AI are still scattered across various regulations, including the ITE Law and Government Regulation Number 71 of 2019 concerning the Implementation of Electronic Systems and Transactions (PP PSTE) as a derivative of the ITE Law. Therefore, liability for AI still refers to Article 21 paragraph (2) letter c of the ITE Law, which states that electronic agent operators are liable for all legal consequences of electronic agents, provided that the error or failure of the electronic agent is not caused by the user's negligence. This is in line with the doctrine of vicarious liability contained in Article 1367, paragraph (1) of the Civil Code, which explains that a person who supervises is responsible for losses caused by goods under their supervision.[46]

However, this regulation is considered inadequate to address the various challenges of the era of rapid AI development. The ambiguity of AI liability becomes even more complex in the context of the FotoYu application, which uses machine

[44] Fence M. Wantu, *Pengantar Ilmu Hukum*, ed. UNG Press (Gorontalo, 2015), 40.

[45] Fence M. Wantu, 40.

[46] Djaja S. Meliala, *Hukum Perdata Dalam Perspektif BW* (Bandung: Nuansa Aulia, 2012), 189.

learning technology to continuously improve the accuracy of facial recognition. As algorithms evolve and change through the process of automatic learning, it becomes difficult to determine whether errors are caused by initial flaws in the design, biased training data, or unpredictable algorithm evolution. This creates challenges in establishing clear responsibilities between the initial developers of the system, training data providers, and application operators.

To develop comprehensive AI regulations, Indonesia can refer to the EU AI Act Regulation. This regulation is quite clear in adopting principles such as human agency and oversight, technical robustness and safety, privacy and data governance, transparency, diversity, non-discrimination, fairness, and social and environmental well-being. In addition, the EU AI Act Regulation regulates the classification of risk levels of AI systems. The EU AI Act Regulation also regulates independent, transparent, accountable, professional supervisory, and regulatory bodies. The European Union even plans to establish an AI Office to ensure compliance with these regulations throughout Europe.[47]

In the context of future regulatory development, Indonesia can adopt the risk-based approach used in the EU AI Act. This approach categorizes AI systems based on their risk level, ranging from minimal to unacceptable risk, and sets different obligations according to the risk level. This model allows for more adaptive regulation that does not hinder innovation but still provides adequate protection for security, safety, and individual rights of the users. If implemented in Indonesia, a risk-based approach can help ensure that high-risk AI systems are more strictly regulated, while low-risk AI systems still have the potential for growth.

In addition to the EU AI Act Regulation, Indonesia can refer to China's AI regulations. These regulations govern content monitoring and training data restrictions, with the responsibility falling on AI providers. The regulations also stipulate the obligation to map risks and periodically update the risk management policies. In addition, China's Ministry of Science and Technology has issued guidelines entitled Generation

[47] Adnasohn Aqilla Respati, "Reformulasi Undang-Undang ITE Terhadap Artificial Intelligence Dibandingkan Dengan Uni Eropa Dan China AI Act Regulation," *Jurnal USM Law Review* 7, no. 3 (2024): 47.

the Artificial Intelligence Ethics Specification stipulates that AI must remain under human supervision to ensure that it produces accurate and non-discriminatory data.[48]

Based on AI regulations in the European Union and China, the concept of AI regulation related to accountability in Indonesia must be based on at least three main aspects that need to be considered. First, a clear legal status for AI must be established in the national legal system. Second, the development of an accountability framework that considers the complexity of modern AI technology. Third, a special supervisory agency with technical expertise in AI should be established to assess AI-related cases. These regulations are necessary to specifically regulate the ethics and policies of AI development and utilization, including accountability mechanisms that are proportional to the level of autonomy and complexity of the AI system.[49]

The rapid development of FRT and AI technology requires adaptive and responsive regulations to ensure that the law does not become outdated and can truly protect the interests of society. FRT and AI regulations are needed not only as formal rules but also as instruments to respond to new moral and social challenges arising from the use of this technology, to protect human rights, and to ensure proportional accountability.

The third significant challenge in implementing personal data protection in applications such as FotoYu is the delay in the ratification of regulations for the PDP Law. The lack of formal and substantial implementing regulations for the PDP Law has caused considerable legal uncertainty regarding the procedures for processing personal data, the obligations of data controllers, and the technical and administrative protections that must be implemented by FotoYu. Although the PDP Law, as the parent law, has provided a solid legal basis for personal data protection in Indonesia, including regulations on data processing principles, data subject rights, and data controller obligations, implementing regulations are still needed.[50]

The implementing regulations in question include several derivative regulations, such as Government Regulations (PP) and Presidential Regulations (Perpres), which are expected to provide applicable technical and operational details for personal data

[48] Adnasohn Aqilla Respati, 47.

[49] Adnasohn Aqilla Respati, 47.

[50] Danil Erlangga Mahameru et al., “IMPLEMENTASI UU PERLINDUNGAN DATA PRIBADI TERHADAP KEAMANAN INFORMASI IDENTITAS DI INDONESIA,” *Jurnal Esensi Hukum* 5, no. 20 (2023): 128.

controllers, including FotoYu. However, in practice, the process of formulating and ratifying derivative regulations has been slow and has not yet reached the final stage, resulting in a void in technical regulations that should fill the normative void in the PDP Law. At the time of this study, the government had not yet issued derivative regulations in the form of government and presidential regulations.

The direct impact of the absence of implementing regulations is evident in various aspects of FotoYu's personal-data governance implementation. Without clear and detailed technical guidelines, data controllers, such as FotoYu, must interpret the general provisions of the PDP Law themselves, which allows for differences in practice and potential non-compliance.

A crucial example is the implementation of personal data processing systems. Article 16, paragraph (1) of the PDP Law explains the types of personal data processing, which include acquisition and collection, processing and analysis, storage, correction and updating, display, announcement, transfer, dissemination, or disclosure, and/or deletion or destruction. However, the rules regarding the procedures for processing personal data have not been regulated in the PDP Law, so they are mandated to be regulated in government regulations, as stated in Article 16 (3) of the PDP Law.

In addition to the procedures for processing personal data, the PDP Law also mandates further provisions in government regulations, including the procedures for filing objections to automated processing; the imposition of compensation in cases where the subject of personal data suffers harm as a result of a violation of the processing of their personal data; rules regarding the rights of the subject of personal data to use and send their personal data to other personal data controllers; the assessment of the impact of personal data protection in cases where the processing of personal data has a high potential risk; and the procedures for notification of the transfer of personal data.

Provisions regarding Personal Data Protection Officers (PPDP) should also be further regulated in government regulations. Article 53 of the PDP Law states:

> *"(1) Personal Data Controllers and Personal Data Processors shall appoint an official or officer to perform Personal Data Protection functions in the following cases:*
>
> *a. processing of Personal Data for the purposes of public services*
>
> *b. the core activities of the Personal Data Controller have a nature, scope, and/or purpose that requires regular and systematic monitoring of Personal Data on a large scale; and*

> c. *The core activities of the Personal Data Controller consist of processing Personal Data on a large scale for Personal Data that is specific in nature and/or Personal Data related to criminal acts.*
>
> *(2) Officials or officers who carry out the Personal Data Protection function as referred to in paragraph (1) shall be appointed based on their professionalism, knowledge of the law, Personal Data Protection practices, and ability to fulfill their duties.*
>
> *(3) Officials or officers who carry out the Personal Data Protection function referred to in paragraph (2) may come from within and/or outside the Personal Data Controller or Personal Data Processor.*

Furthermore, in Constitutional Court Decision Number 151/PUU-XXII/2024 regarding the constitutionality of Article 53 (1) of the PDP Law against the 1945 Constitution of the Republic of Indonesia (UUD NRI), the Court stated that the word "and" in Article 53 (1) (b) of the PDP Law is contrary to the 1945 Constitution of the Republic of Indonesia, so that the word "and" does not have binding legal force as long as it is not interpreted as 'and/or'.

This article was challenged by the petitioners concerned because there was concern that if the elements/criteria in letters a, b, and c were all fulfilled, then personal data controllers and personal data processors would be required to appoint a PPDP when carrying out new personal data processing activities. Meanwhile, if only one or two elements/criteria are met in the personal data processing activity, then there is no obligation for the personal data controller and personal data processor to appoint a PPDP.

This is because the word "and" has a cumulative meaning. Therefore, the Court granted the petition to ensure that the protection and guarantee of the constitutional rights of personal data subjects are truly protected. This decision fundamentally strengthens the personal data protection framework by changing the word "and" to "and/or" in the article, so that the obligation to appoint a PPDP is no longer only cumulative but alternative-cumulative.

However, there is still another legal uncertainty, namely the phrase "large scale" in Article 53 paragraph (1) letters b and c of the PDP Law. There is no clear definition of what is meant by "large scale" in the processing of personal data, thus creating a broad room for interpretation and potentially causing uncertainty in implementation. In the context of the FotoYu application, the uncertainty regarding the definition of "large scale" creates its own challenges. The processing of personal data in the form of photos of runners, as well as the use of RoboYu to identify faces in photos uploaded by creators, has the potential to process thousands or even millions of Yuser facial biometric data.

Without clear parameters regarding the threshold for “large scale,” FotoYu faces difficulties in determining whether it meets these criteria and is therefore subject to the obligation to appoint a PPDP. Therefore, future implementing regulations of the PDP Law should further regulate the parameters of the phrase “large scale,” not just the regulations regarding the duties and functions of the PPDP.

In addition to the PPDP, the PDP Law mandates the establishment of a personal data protection agency by the President, as well as further provisions regarding this agency in a presidential regulation, as stated in Article 58 of the PDP Law. Furthermore, Article 59 of the PDP Law regulates the duties of this agency as follows:

> *"The institution referred to in Article 58, paragraph (2), shall carry out the following:*
>
> *a. The formulation and establishment of Personal Data Protection policies and strategies that serve as guidelines for Personal Data Subjects, Personal Data Controllers, and Personal Data Processors.*
> *b. supervision of the implementation of Personal Data Protection*
> *c. administrative law enforcement against violations of this Law; and*
> *d. facilitation of out-of-court dispute resolution."*

Not only does it regulate the duties of the institution, but it also regulates the authority of the institution in Article 60 of the PDP Law, as follows:

> *"The institution referred to in Article 58 paragraph (2) has the authority to:*
>
> *a. formulate and establish policies in the field of Personal Data Protection;*
> *b. supervise the compliance of Personal Data Controllers;*
> *c. impose administrative sanctions for violations of Personal Data Protection committed by Personal Data Controllers and/or Personal Data Processors.*
> *d. assist law enforcement officials in handling alleged Personal Data crimes, as referred to in this Law;*
> *e. cooperating with personal data protection agencies of other countries to resolve alleged cross-border personal data protection violations;*
> *f. assessing compliance with the requirements for the transfer of Personal Data outside the jurisdiction of the Republic of Indonesia;*
> *g. issuing orders to Personal Data Controllers and/or Personal Data Processors as a follow-up to the results of the supervision;*
> *h. publishing the results of Personal Data Protection supervision in accordance with the provisions of laws and regulations;*
> *i. receiving complaints and/or reports of alleged violations of Personal Data Protection;*

> *j. conducting examinations and investigations of complaints, reports, and/or supervision results regarding alleged violations of Personal Data Protection;*
> *k. summon and bring in any person and/or public agency related to alleged violations of the Personal Data Protection;*
> *l. request information, data, and documents from any person and/or public agency related to alleged violations of Personal Data Protection;*
> *m. summon and bring in experts as needed in the examination and investigation of alleged violations of Personal Data Protection;*
> *n. conduct examinations and investigations of electronic systems, facilities, rooms, and/or places used by Personal Data Controllers and/or Personal Data Processors, including obtaining access to data and/or appointing third parties; and request legal assistance from the prosecutor's office in resolving Personal Data Protection disputes."*

Based on the above provisions, it can be seen that the personal data protection agency has very broad duties and authority, as stipulated in Articles 59 and 60. However, since the PDP Law was enacted until this study was conducted, a personal data protection agency has not yet been established. The absence of a personal data protection agency has resulted in a void in the functional authority that is essential for carrying out prevention, supervision, and dispute resolution activities regarding personal data violations that can directly impact the personal data processing practices of applications such as FotoYu. As an application that processes personal data extensively, particularly in facial recognition technology, FotoYu is in dire need of strict supervision and effective law enforcement mechanisms to comply with the PDP Law and protect the rights of personal data subjects.[51]

This lack of oversight directly impacts the weak effectiveness of administrative sanctions. The PDP Law has given personal data protection agencies the authority to impose administrative sanctions for data protection violations, including administrative measures, fines, and temporary restrictions on data processing activities. However, without a personal data protection agency, the sanctioning process will be very limited

[51] Gunawasn Widjaja and Fransiska Milenia Cesarianti, "Urgensi Pembentukan Lembaga Pengawas Pelindungan Data Pribadi Di Indonesia Berdasarkan Pasal 58 Juncto Pasal 59 Dan Pasal 60 Undang – Undang Nomor 27 Tahun 2022 Tentang Pelindungan Data Pribadi," *SINERGI : Jurnal Riset Ilmiah* 1, no. 4 (2024): 237, https://doi.org/10.62335/8qf44b59.

and unclear, so that data controllers and processors, including FotoYu, will not have strong pressure to comply with their legal obligations. [52]

The absence of a personal data protection agency also results in a lack of mechanisms to facilitate out-of-court dispute resolution, which could provide a quick and efficient alternative for subjects of personal data who have suffered losses in the interim. Users of the FotoYu application, for example, when experiencing misidentification or data leaks, do not have a formal institution that can accommodate complaints and conduct mediation as a quick resolution without the need for lengthy and expensive litigation. This condition has the potential to create injustice and ongoing losses for personal data subjects and weaken the authority of legal protection in practice.[53]

In addition, legal credibility and trust in the context of data protection decline significantly without a personal data protection agency. [54] The existence of this agency is a concrete manifestation of the state's guarantee of the protection of citizens' privacy and personal data rights. If the agency does not function, legal norms will become weak in practice, and public trust in data protection will decline.[55] This situation poses a serious challenge to the operation of applications that rely on consumer trust and an adequate level of data protection, such as FotoYu.

From a procedural perspective, the absence of a personal data protection agency limits the mechanisms for handling complaints and investigating such violations. In the PDP Law, the supervisory agency is given the authority to conduct examinations, investigations, and even request assistance from experts and third parties to follow up on reports of violations. Without this agency, reports of violations tend to be scattered and uncoordinated, and investigations cannot be conducted thoroughly and systematically.

[52] Fanisa Mayda Ayiliani and Elfia Farida, "Urgensi Pembentukan Lembaga Pengawas Data Pribadi Sebagai Upaya Pelindungan Hukum Terhadap Transfer Data Pribadi Lintas Negara," *Jurnal Pembangunan Hukum Indonesia* 6, no. 3 (2024): 449, https://doi.org/10.14710/jphi.v6i3.%25p.

[53] M.I. Nurzihad, M. Ichsan, and F. Fitriyanti, "Personal Data Protection in Indonesian E-Commerce Platforms: The Maqasid Sharia Perspective," 693 LNNS (2023): 1077–86, https://doi.org/10.1007/978-981-99-3243-6_88.

[54] R. Nayak et al., "Cyber Security for Personal Data," in *Developing AI, IoT and Cloud Computing-Based Tools and Applications for Women's Safety* (2024), 123–41, https://doi.org/10.1201/9781003538172-9.

[55] D. Xanthidis et al., "Information Privacy and Emerging Technologies in the U.A.E.: Current Standing and Research Directions," 2019, 314–18, https://doi.org/10.1109/ITT48889.2019.9075076.

This complicates the law enforcement process and allows for repeated data violations without any firm action.[56]

The absence of this institution is significant in the context of administrative and criminal law enforcement. Personal data protection agencies should collaborate with law enforcement officials to investigate and assist in prosecuting alleged criminal violations of personal data. Without this institution, the process of coordination and technical support for law enforcement is hampered, allowing violators to find loopholes to avoid legal consequences, thereby reducing the deterrent effect.

The importance of a personal data protection agency also lies in its ability to provide legal certainty through the establishment of binding policies and technical standards for the management of personal data. Standards and guidelines must be able to respond to new technological challenges, such as those related to AI and FRT, which are prone to privacy violations and data misuse.

Without this institution, personal data processing practices, such as those carried out by FotoYu, have the potential to violate the rights of personal data subjects due to FotoYu's lack of supervision, legal certainty, and accountability, and the legal system's inability to address violations that occur. This is a warning signal for policymakers to immediately end the delay in establishing this institution to realize a personal data protection system that can guarantee the privacy rights of Indonesian citizens.

Therefore, the establishment of a personal data protection agency is not only a formal obligation under the PDP Law but also an absolute and urgent legal measure to fill the regulatory void that currently hinders the effective enforcement of personal data protection. Thus, FotoYu still faces many challenges in implementing its obligations as a personal data controller, as stipulated in the PDP Law. In addition, there are still legal loopholes that prevent the effective supervision and law enforcement of personal data protection in the Foto application.

Conclusion

The implementation of the PDP Law in the FotoYu application shows that there are several aspects that need to be improved to fulfill the obligations of personal data

[56] M. Ati, "Big Data Security and Privacy Implementation: The Way Ahead," paper presented at 7th IEEE International Conference on Engineering Technologies and Applied Sciences, ICETAS 2020, 2020, https://doi.org/10.1109/ICETAS51660.2020.9484196.

controllers. Explicit consent from data subjects has not been fully obtained legally, transparency in how data are processed needs to be improved, and effective and structured data deletion mechanisms are not yet fully available. This shows that the application of personal data protection principles needs to be strengthened so that the rights of data subjects are protected.

The use of FRT in FotoYu also poses its own challenges, such as the potential for misidentification, lack of specific regulations related to AI and FRT, and absence of implementing regulations and an independent personal data protection agency. This situation creates uncertainty regarding legal accountability, emphasizing the need for clearer and more comprehensive rules to regulate the use of such technology. For platforms such as FotoYu, it is important to ensure that all data controller obligations are fulfilled. This includes obtaining explicit consent from users, ensuring transparency in data processing, providing secure and easily accessible data deletion mechanisms, and improving security and confidentiality of personal data. These measures are important for building user trust and complying with the provisions of the PDP Law.

For the government, it is necessary to strengthen regulations governing the use of FRT and AI, accelerate the issuance of implementing regulations for the PDP Law, and establish an independent personal data protection agency. All of this is important to ensure effective supervision and law enforcement so that the personal data rights of the public can be properly protected. This research contributes by offering a practical and normative evaluation of the implementation of the PDP Law in AI-based applications with FRT, while also presenting policy recommendations that can serve as a guide for developers and regulators to strengthen the data protection framework in Indonesia.

Bibliography

Adnasohn Aqilla Respati. "Reformulasi Undang-Undang ITE Terhadap Artificial Intelligence Dibandingkan Dengan Uni Eropa Dan China AI Act Regulation." *Jurnal USM Law Review* 7, no. 3 (2024): 1737–58.

Agata Ramadhani, Syafira. "Komparasi Pengaturan Perlindungan Data Pribadi Di Indonesia Dan Uni Eropa Comparison of Personal Data Protection Regulation in Indonesia and the European Union." *Rewang Rencang : Jurnal Hukum Lex Generalis.* 3, no. 1 (2022): 73–84. https://doi.org/10.56370/jhlg.v3i1.173.

Ali. “FH UNS-Mafindo Bahas Marketplace Fotografi, Pengguna Dan Fotografer FotoYu Harus Saling Melindungi.” Joglosemar News.Com, 2025. https://joglosemarnews.com/2025/03/fh-uns-mafindo-bahas-marketplace-fotografi-pengguna-dan-fotografer-fotoyu-harus-saling-melindungi/.

Athallah Rafidiansyah. “Hak Atas Potret Dalam Komersialisasi Pada Aplikasi FotoYu: Tinjauan Hak Cipta.” 2025.

Ati, M. “Big Data Security and Privacy Implementation: The Way Ahead.” Paper presented at 7th IEEE International Conference on Engineering Technologies and Applied Sciences, ICETAS 2020. 2020. https://doi.org/10.1109/ICETAS51660.2020.9484196.

Aulia Alayna Suvil, Firdaus Firdaus, M. Arif Ramadhan, Wanda Darma Putra, and Dwi Putri Lestarika. “Implementasi Perlindungan Data Pribadi Berdasarkan Undang-Undang Nomor 11 Tahun 2020.” *Jurnal Hukum, Politik Dan Ilmu Sosial* 3, no. 4 (2024): 70–80. https://doi.org/10.55606/jhpis.v3i4.4235.

Awwaliyah, Rizka Putri, and Sony Juniarti. “Perbandingan General Data Protection Regulation (GDPR) Dengan Regulasi Perlindungan Data Di Negara-Negara Asia Tenggara.” *Jurnal Hukum Dan Kewarganegaraan* 4, no. 4 (2024). https://doi.org/10.3783/causa.v4i4.3535.

Ayiliani, Fanisa Mayda, and Elfia Farida. “Urgensi Pembentukan Lembaga Pengawas Data Pribadi Sebagai Upaya Pelindungan Hukum Terhadap Transfer Data Pribadi Lintas Negara.” *Jurnal Pembangunan Hukum Indonesia* 6, no. 3 (2024): 431–55. https://doi.org/10.14710/jphi.v6i3.%25p.

Br Girsang, Sarimah Yemima. “Pentingnya Regulasi Khusus Sistem Face Recognition Technology Sebagai Produk Artificial Intelligence Dalam Peningkatan Keamanan Dan Penegakan Hukum Di Indonesia.” *Nommensen Journal of Legal Opinion* 05 (2024): 86–98. https://doi.org/10.51622/njlo.v5i2.1817.

Cahyadaru Kuncorojati. “133 Juta Serangan Siber Hantam Indonesia, Ancam Celah Keamanan Dan Botnet Iot.” Medcom.Id, 2025. https://www.medcom.id/teknologi/news-teknologi/5b2wOjnk-133-juta-serangan-siber-hantam-indonesia-ancam-celah-keamanan-dan-botnet-iot.

Djaja S. Meliala. *Hukum Perdata Dalam Perspektif BW*. Bandung: Nuansa Aulia, 2012.

Enggarsasi, U., N.K. Sa'diyah, and P.A. Martio. "LEGAL SAFEGUARDS FOR VICTIMS OF DATA DISSEMINATION CRIMES AND CYBERCRIME PROTECTION." *Jurnal Hukum Unissula* 40, no. 2 (2024): 258–77. https://doi.org/10.26532/jh.v40i2.39974.

Fattah Rizki, Miyuki, and Abdul Salam. "Pertanggungjawaban Hukum Pengumpulan Data Biometrik Melalui Artificial Intelligence Tanpa Persetujuan Pemilik Data (Studi Kasus Clearview AI Inc. Di Yunani Dan Inggris)." *Lex Patrimonium* 2, no. 2 (2023): 1–16.

Fence M. Wantu. *Pengantar Ilmu Hukum*. Edited by UNG Press. Gorontalo, 2015.

Floubianca Viola. "Potensi Pelanggaran Hak Privasi Dalam Penggunaan Face Recognition Untuk Pengawasan Keamanan Di Ruang Publik." Universitas Katolik Parahyangan, 2023.

FotoYu. "Cara Kerja FotoYu." FotoYu. https://www.fotoyu.com/how-it-works.

Hasibuan, Edi Saputra, and Elfirda Ade Putri. "Perlindungan Keamanan Atas Data Pribadi Di Dunia Maya." *Jurnal Hukum Sasana* 10, no. 1 (2024): 70–83. https://doi.org/10.31599/sasana.v10i1.2134.

Hisbulloh, M.H. "URGENSI RANCANGAN UNDANG-UNDANG (RUU) PERLINDUNGAN DATA PRIBADI." *Jurnal Hukum Unissula* 37, no. 2 (2021): 119–33. https://doi.org/10.26532/jh.v37i2.16272.

Hoca, Y., D. Firat, and E. Çağlar. "Principles of Data Privacy and Security in a Cyber World." In *Handbook of Research on Cyber Law, Data Protection, and Privacy*, 1–19. 2022. https://doi.org/10.4018/978-1-7998-8641-9.ch001.

Husna, Nur, Moh Nurman, and Yudhistira Nugroho. "Pembentukan Peraturan Pemerintah Tentang Face Recognition Technology Ditinjau Dari Undang-Undang Nomor 27 Tahun 2022 Tentang Perlindungan Data Pribadi." *Jurnal Ilmiah AKSES*, no. 2 (2025): 1–6.

Kaczmarek, K., M. Karpiuk, and C. Melchior. "A Holistic Approach to Cybersecurity and Data Protection in the Age of Artificial Intelligence and Big Data." *Prawo i Wiez* 50, no. 3 (2024): 103–21. https://doi.org/10.36128/PRIW.VI50.907.

Kementerian Komunikasi dan Digital. "Komitmen Pemerintah Melindungi Anak Di Ruang Digital." Komdigi, 2025.

https://www.komdigi.go.id/berita/artikel/detail/komitmen-pemerintah-melindungi-anak-di-ruang-digital.

Korengkeng, Michelle Lucia, Roy Ronny Lembong, and Feiby S. Wewengkang. "ANALISIS TINDAK PIDANA DEEPFAKE PORNOGRAFI DALAM PERSPEKTIF UNDANG-UNDANG INFORMASI DAN TRANSAKSI ELEKTRONIK." *Jurnal Fakultas Hukum UNSRAT* 13, no. 3 (2025).

Mahameru, Danil Erlangga, Aisyah Nurhalizah, Ahmad Wildan, Mochamad Haikal, and Mohamad Haikal Rahmadia. "IMPLEMENTASI UU PERLINDUNGAN DATA PRIBADI TERHADAP KEAMANAN INFORMASI IDENTITAS DI INDONESIA." *Jurnal Esensi Hukum* 5, no. 20 (2023): 115–31.

Nasakti, Ghazali Hasan. "IUS CONSTITUENDUM PENGGUNAAN TEKNOLOGI PENGENALAN WAJAH DALAM INDUSTRI DAN PENEGAKAN HUKUM DI INDONESIA." *Prosiding Konferensi Mahasiswa Nasional Ubaya Law Fair Tahun 2021*, 2021.

Nawawi, J. "LEGAL PROTECTION OF PERSONAL DATA BASED ON REGULATION IN INDONESIA." *Jurnal Al-Dustur* 5, no. 1 (2022): 96–106. https://doi.org/10.30863/jad.v5i1.2581.

Nayak, R., A. Jain, M. Saxena, and R. Kumar. "Cyber Security for Personal Data." In *Developing AI, IoT and Cloud Computing-Based Tools and Applications for Women's Safety*, 123–41. 2024. https://doi.org/10.1201/9781003538172-9.

Nufus, Hayatun, and Moh Soleh. "Tinjauan Yuridis Dalam Kasus Memotret Orang Tanpa Izin Untuk Kepentingan Komersial." *Jurnal Cakrawala Akademika* 2, no. 1 (2025): 1–19. https://doi.org/10.70182/JCA.

Nurzihad, M.I., M. Ichsan, and F. Fitriyanti. "Personal Data Protection in Indonesian E-Commerce Platforms: The Maqasid Sharia Perspective." 693 LNNS (2023): 1077–86. https://doi.org/10.1007/978-981-99-3243-6_88.

Pakpahan, Jonathan Matthew. "Kesadaran Urgensi Peran Pengendali Dan Prosesor Data Pribadi Dalam Rangka Pelindungan Data Pribadi Individu Berdasarkan Undang-Undang Nomor 27 Tahun 2022 Tentang Pelindungan Data Pribadi." *Jurnal Hukum To-Ra : Hukum Untuk Mengatur Dan Melindungi Masyarakat* 10, no. 1 (2024): 119–37. https://doi.org/10.55809/tora.v10i1.331.

Puluhulawa, F.U., J. Puluhulawa, and M.G. Katili. “Legal Weak Protection of Personal Data in the 4.0 Industrial Revolution Era.” *Jambura Law Review* 2, no. 2 (2020): 182–200. https://doi.org/10.33756/jlr.v2i2.6847.

Rahmatullah, I. “FINANCIAL TECHNOLOGY AND THE LEGAL PROTECTION OF PERSONAL DATA: The Case of Malaysia and Indonesia.” *Al-Risalah: Forum Kajian Hukum Dan Sosial Kemasyarakatan* 20, no. 2 (2020): 197–214. https://doi.org/10.30631/alrisalah.v20i2.602.

Rambe, Rahmat, and Lukman Abdurrahman. “Implikasi Etika Dan Hukum Dalam Penggunaan Teknologi Pengenalan Wajah: Perlindungan Privasi Versus Keamanan Publik.” *Jurnal Hukum Caraka Justitia* 4, no. 2 (2024): 90–104. https://doi.org/10.30588/jhcj.v4i2.1828.

Rendreana, N.A., S. Cahyono, and R.A. Wijayanti. “Implementation of Gamification to Enhance Understanding of Personal Data Protection Based on Republic of Indonesia Law Number 27 of 2022.” 2023, 246–51. https://doi.org/10.1109/ICIMCIS60089.2023.10349080.

Rinjani, Muhamad Adri, and Ricky Firmansyah. “Hambatan Implementasi UU 27/2022 Dan Strategi Penguatan Perlindungan Data Pribadi Di Indonesia.” *Jurnal Analisis Hukum* 8, no. 1 (2025): 70–83. https://doi.org/10.38043/jah.v8i1.6793.

Rizal Amril Yahya. “Pudarnya Privasi Kita Di Hadapan Kamera Liar.” Tirto.Id, 2025. https://tirto.id/pudarnya-privasi-kita-di-hadapan-kamera-liar-hdcD#google_vignette.

Rumlus, Muhamad Hasan, and Hanif Hartadi. “Kebijakan Penanggulangan Pencurian Data Pribadi Dalam Media Elektronik.” *Jurnal HAM* 11, no. 2 (2020): 285. https://doi.org/10.30641/ham.2020.11.285-299.

Rusyda, Nabiha Khansa. “Perlindungan Hukum Erhadap Subjek Data Kebocoran Data Oleh Badan Publik Menurut UU Nomor 27 Tahun 2022.” *Desentralisasi : Jurnal Hukum, Kebijakan Publik, Dan Pemerintahan* 2, no. 3 (2025): 247–62. https://doi.org/10.62383/desentralisasi.v2i3.940.

Simatupang, Aldi Pebrian. *Penerapan Algoritma Deep Learning Dalam Pengenalan Wajah Untuk Sistem Keamanan*. 01 (2025): 7–12.

Soekanto, Soerjono. *Kesadaran Hukum Dan Kepatuhan Hukum*. Jakarta: CV. Rajawali, 1982.

Soerjono Soekanto. *Penegakan Hukum*. Jakarta: Bina Citra, 1983.

Tulay, M.A., and S. Olatunbosun. "Cybersecurity Techniques, Emerging Threats, and Industry Responses." 2262 (2025): 336–53. https://doi.org/10.1007/978-3-031-85933-5_25.

Utama, F.S., D.E. Purwoleksono, and T. Rachman. "Data Leakage of the Indonesian Elections Commission in Legal Aspects of Personal Data Protection." *Media Iuris* 7, no. 3 (2024): 479–98. https://doi.org/10.20473/mi.v7i3.55931.

Widjaja, Gunawan, and Fransiska Milenia Cesarianti. "Urgensi Pembentukan Lembaga Pengawas Pelindungan Data Pribadi Di Indonesia Berdasarkan Pasal 58 Juncto Pasal 59 Dan Pasal 60 Undang – Undang Nomor 27 Tahun 2022 Tentang Pelindungan Data Pribadi." *SINERGI : Jurnal Riset Ilmiah* 1, no. 4 (2024): 234–42. https://doi.org/10.62335/8qf44b59.

Xanthidis, D., F. Alsuwaidi, M. Al Ali, A. Alolama, and M. Albaloushi. "Information Privacy and Emerging Technologies in the U.A.E.: Current Standing and Research Directions." 2019, 314–18. https://doi.org/10.1109/ITT48889.2019.9075076.

Yeovandi, Felix, and Eko Prasetyo. "Evaluasi Keamanan Sistem Autentikasi Biometrik Pada Smartphone Dan Rekomendasi Implementasi Optimal." *JTIM : Jurnal Teknologi Informasi Dan Multimedia Evaluasi Keamanan Sistem Autentikasi Biometrik* 7, no. 1 (2025): 133–48. https://doi.org/10.35746/jtim.v7i1.653.

Yopi Prayitno. "Pertanggungjawaban Perdata Perusahaan Nodeflux Atas Kerugian Pengguna Akibat Kesalahan Output Teknologi Artificial Intelligence (Face Recognition)." Universitas Sriwijaya, 2024.

Zorluoğlu Yilmaz, Ayça. "Joint Controllership Under the GDPR - Concept, Responsibilities, and Liability." *Juridical Tribune - Review of Comparative and International Law* 15, no. 1 (2025): 93–107. https://doi.org/10.62768/TBJ/2025/15/1/06.