THE FUTURE IMPLEMENTATION OF FACE RECOGNITION IN INDONESIA IN THE PERSPECTIVE OF HUMAN RIGHTS

Hilmi Ardani Nasution

The National Research and Innovation Agency of Indonesia

Keywords:
Face Recognition, Human Rights, Right to Privacy, Right to Personal Identity

***Correspondence Address:**
hilmikumham@gmail.com

Abstract: This normative legal research critically examines the prospective implementation of face recognition technology in Indonesia within the context of human rights. Utilizing normative legal analysis, the study seeks to unravel the perspective of human rights law regarding the integration of face recognition systems. The central question addressed is how human rights law perceives and evaluates the implications of adopting face recognition technology in Indonesia. The study reveals a potential contradiction between adopting face recognition and fundamental human rights principles. Primary concerns include the right to privacy and the right to personal identity. A nuanced exploration of existing legal frameworks exposes the need to assess the compatibility between face recognition practices thoroughly and established human rights norms. In conclusion, the implementation of face recognition in Indonesia holds the risk of violating human rights. The study advocates for consideration of human rights implications while integrating face recognition systems. A Precise legal framework that aligns with human rights principles is a must, safeguarding against potential abuses and ensuring an ethically sound deployment of face recognition technology in Indonesia.

INTRODUCTION

In cutting-edge technology, face recognition has emerged as a groundbreaking application that harnesses artificial intelligence and computer vision prowess. At its core, this technology utilizes sophisticated algorithms to analyze and identify unique facial features, creating a distinct biometric profile for each individual. The process involves mapping key facial landmarks, such as the arrangement of eyes, nose, and mouth, and translating these features into data that can be used for precise identification. The technical underpinnings of face recognition systems are rooted in machine learning, a subset of artificial intelligence. These systems are trained on vast datasets of facial images, allowing them to discern patterns and variations in facial features. As a person interacts with the system, their unique facial characteristics are captured, processed, and compared against the stored data. The advancements in deep learning algorithms have significantly improved the accuracy and efficiency of face recognition, enabling real-time identification with remarkable precision. The integration of neural networks has further enhanced the ability of

these systems to adapt and recognize faces across diverse conditions, such as varying lighting or facial expressions. The versatility of face recognition technology is reflected in its varied range of applications. One prominent domain is security, crucial in access control and surveillance.

In security, face recognition technology stands as a formidable force, reshaping the landscape of access control and surveillance systems; compared to the conventional Closed-Circuit Television (CCTV), it is common that CCTV footage is often deemed inconclusive or insufficient to substantiate any claims. Face recognition is pivotal in access control systems, surveillance, and monitoring environments where strict authentication is crucial. Airports, government facilities, and private organizations harness its capabilities to bolster security measures. The real-time processing of facial data allows for rapid identity verification, preventing unauthorized access and providing a proactive stance against potential threats. Integrating face recognition into security systems helps streamline operations, reduce the reliance on traditional identification methods, and mitigate the risks associated with stolen credentials or unauthorized access.

However, the intensified use of this technology raises questions about the fine line between security enhancement and the potential erosion of individual privacy. The widespread adoption of face recognition technology may cause controversy. Privacy concerns loom large as the technology raises questions about the collection, storage, and potential misuse of facial data. The mass deployment of these systems has prompted a delicate balance between security imperatives and safeguarding personal information, requiring ethical considerations and responsible implementation to address these contentious issues.

The continuous monitoring and storage of facial data raise alarms about the potential misuse or unauthorized access to sensitive information. The ethical dimensions of deploying face recognition systems in public spaces and the potential for discriminatory practices warrant careful consideration. Striking a balance between the benefits of enhanced security and the protection of individual privacy is crucial for the responsible development and widespread acceptance of face recognition technology in our increasingly interconnected and digitized world. Stringent regulations and safeguards are necessary to protect individuals from unwarranted intrusions into their private lives. This underscores the importance of ethical development and implementation to ensure the responsible use of face recognition technology in the digital age.

Indonesia's future government will likely implement face recognition, especially for security reasons. The National Police of Indonesia executed face recognition during The G20 Bali Summit 2022. The state-owned railway Kereta Api Indonesia has also implemented face recognition technology for passengers to ease the boarding service. The adoption of face recognition technology has sparked controversy in Indonesia due to growing concerns over privacy, civil liberties, and potential misuse. The purpose of data collection through face recognition must be cleared, the data collection procedure must be explained, and the most important thing is the consent of the individuals.

The potential contradictions of face recognition technology to human rights add a layer of complexity to its narrative. Issues such as the right to privacy and personal identity prompt the need for careful consideration and regulation. Striking an equilibrium between the advantages of enhanced security and the potential risks to privacy and human rights becomes imperative in navigating the ethical terrain of face recognition technology.

Based on the possible contradiction of face recognition technology and human rights, this research raises a problem statement about the perspective of human rights law concerning face recognition technology. This research aims to increase the alarm among the people and the government of Indonesia about the implementation of face recognition technology and the possible contradiction to the basic values of human rights.

RESEARCH METHODS

Using normative legal research, this research is a systematic approach and particular reasoning to study one or several specific legal phenomena using analysis. It is a process of discovering legal rules, principles, and doctrines to address legal issues faced by the nature of legal science. Legal research aims to develop Law and legal science by and in harmony with the advancements in science and technology, especially global information technology.

RESULTS AND DISCUSSION

Face recognition is one of the technological innovations that may improve various sectors of human life. One of the sectors related to security concerns is explored in a research study that shows people feel safe and comfortable with the implementation of face recognition technology. This is attributed to its advanced monitoring and surveillance capabilities, surpassing common CCTV systems today. The deployment of facial recognition technology creates substantial concerns vis-à-vis the right to privacy and personal identity.

The integration of facial recognition systems demands the acquisition, processing, and retention of individuals' biometric data, notably their facial features. This encroachment upon personal attributes threatens privacy rights, as it facilitates the tracking and monitoring individuals without explicit, informed consent. Furthermore, the precision and latent biases inherent in facial recognition algorithms contribute to the prospect of misidentifications, thereby impacting the divine right to personal identity. A judicious equilibrium between technological advancements and safeguarding these foundational rights becomes imperative to ensure facial recognition systems' conscientious and ethical implementation.

Indonesia has taken a significant step in safeguarding the privacy of its citizens by enacting Law Number 27 of 2022 concerning The Protection of Personal Data. This legislation reflects the nation's commitment to establishing a robust legal framework that governs the responsible use of personal information in the digital age. According to the Law, any information through electronic media, particularly concerning an individual's data, must be carried out with the explicit consent of the individual involved unless specified otherwise by regulations. The enactment of this Law underscores Indonesia's dedication to upholding privacy rights, recognizing the importance of balancing technological advancements with the protection of personal information in the modern era.

The personal data from the face recognition process is categorized as biometric data based on Law Number 27 of 2022, mentioned in Article 4. The face is biometric data because it is data related to an individual's physical, physiological, or behavioral characteristics that allow for unique identification, such as facial images or fingerprint data.

Even, there is an exception for the right to personal identity as mentioned in article 15 of Law Number 27 of 2022, namely for national defense and security interests, the interests of law enforcement processes, public interests in the framework of state administration, supervision of the financial services, monetary, payment systems, and economic system stability conducted in the framework of state administration; and statistical and scientific research interests. Article 15 also mentioned that the exceptions, as referred to, are implemented only in the context of the provisions of the Law. Consequently, every exception mentioned in Article 15 must be supported by the proper legal frameworks to ensure the legal certainty related to the implementation of face recognition.

The Law related to personal identity protection is coherent with the provisions in Law Number 11 of 2008 concerning Electronic Information and Transactions. Law Number

11 of 2008 also strongly assures personal data protection as part of privacy rights. As mentioned in Article 26:

Article 26

1) *Unless otherwise specified by legislation, the use of any information concerning an individual's data through electronic media must be done with the consent of the individual involved.*
2) *Anyone whose rights are violated, as referred to in paragraph (1), may file a lawsuit for the resulting damages based on this Law.*

In the utilization of Information Technology, the protection of personal data is one part of privacy rights. Based on Law Number 11 of 2008, privacy rights encompass the following meanings:

a. Privacy rights are the right to enjoy a personal life and be free from interference.
b. Privacy rights are the right to communicate with others without eavesdropping.
c. Privacy rights are the right to oversee access to information about one's personal life and data. The use of facial recognition technology has the potential to threaten individual privacy. Unauthorized or unnoticed identification can endanger their privacy rights. Therefore, strong privacy protection within a legal framework is necessary to safeguard individual rights.

Furthermore, Indonesia places a paramount emphasis on safeguarding privacy and personal data as enshrined in its human rights legislation, especially in the Constitution of Indonesia of 1945 Article 28G:

(1) Everyone has the right to protect their self, family, honor, dignity, and possessions under their control, as well as the right to security and protection from threats of fear to do or not to do something that constitutes a human right.

The legal framework protects these fundamental aspects and establishes a broader commitment to upholding individual rights and dignity. With a foundation rooted in human rights principles, Indonesia seeks to create a secure and respectful environment where privacy is regarded as an inviolable right, fostering trust and confidence among its citizens. This commitment reflects the nation's dedication to harmonizing technological advancements with ethical considerations, ensuring a balanced, rights-respecting approach in the evolving landscape of privacy and personal data protection. It is coherent with the Law Number 39 of 1999 concerning Human Rights:

Article 21:

Everyone is entitled to spiritual and physical personal integrity and should not be subjected to research without consent.

In addition to national regulations concerning privacy rights and personal identity protection, it is crucial to consider international human rights instruments to comprehensively describe facial recognition technology within the context of fundamental human rights values. This research draws upon various international human rights instruments, such as the Universal Declaration of Human Rights (UDHR) and the International Covenant on Civil and Political Rights (ICCPR), to provide a thorough examination and interpretation of the implications of facial recognition technology on core human rights principles. This broader perspective, encompassing national and international frameworks, ensures a stronger and globally informed understanding of the intersection between facial recognition technology and human rights.

Article 12 of the Universal Declaration of Human Rights (UDHR) explicitly articulates the fundamental right to privacy; it is mentioned:

"No one shall be subjected to arbitrary interference with his privacy, family, home or correspondence, nor to attacks upon his honour and reputation. Everyone has the right to the protection of the Law against such interference or attacks."

Article 17 of the International Covenant on Civil and Political Rights (ICCPR)

"1. No one shall be subjected to arbitrary or unlawful interference with his privacy, family, home or correspondence, nor illegal attacks on his honor and reputation.

2. Everyone has the right to the protection of the Law against such interference or attacks."

Face recognition may be implemented in Indonesia in line with the human rights principles related to the limitation and derogation of human rights; one of the most applicable principles of face recognition is The Siracusa Principle. The Siracusa Principles on the Limitation and Derogation Provisions in ICCPR are guidelines established by the International Commission of Jurists (ICJ) in Siracusa, Italy, in 1984. These principles provide authoritative guidance on interpreting and applying the ICCPR, particularly regarding the permissible limitations on human rights during states of emergency. The Siracusa Principles aim to clarify the circumstances under which a government may derogate certain rights during emergencies, balancing the need to protect public safety and order with preserving fundamental human rights. Key principles include the necessity of limitations

being prescribed by Law, proportionate to the threat, and non-discriminatory. A detailed explanation of facial recognition and the principles outlined in Siracusa is provided in the table below:

Siracusa Principle	Justification of Face Recognition Implementation
Prescribed by Law	Face recognition is implemented by clear and specific laws explicitly authorizing it for particular purposes, such as law enforcement, security, and public safety. This ensures a legal basis for the technology's deployment.
In a democratic society	Face recognition is implemented with transparency, public engagement, and accountability measures, aligning with democratic values. Policies governing its use are shaped through democratic processes, fostering a balance between security needs and individual rights.
Public order (ordre public)	Face recognition contributes to maintaining public order by swiftly identifying potential threats or criminal activities, thus enhancing overall societal stability and functioning. It is a tool to ensure the safety and security of the public.
Public health	Face recognition is employed for public health purposes, aiding in contact tracing during pandemics and swiftly identifying and isolating individuals with potential health risks to curb the spread of diseases.
Public morals	Face recognition is justified in upholding public morals by assisting in identifying and preventing activities that may be considered morally objectionable or illegal, contributing to societal values.
National security	Face recognition is implemented to address national security concerns, facilitating the rapid and accurate identification of potential threats and protecting the nation and its citizens.
Public safety	Face recognition enhances public safety by swiftly identifying individuals involved in criminal activities, preventing potential threats to general well-being, and providing a tool for law enforcement to maintain order.
Rights and freedoms of others, or rights and reputations of others	Face recognition is used with a focus on respecting the rights and reputations of others by swiftly identifying and addressing potential threats or criminal activities that may infringe on the rights of individuals, striking a balance between public safety and individual rights.
Restrictions on public trial	Face recognition may be employed with restrictions on public trials to protect the identity of witnesses, ensuring their safety and willingness to come forward and thereby contributing to the fairness and effectiveness of the judicial process.

The prospect of harmonizing the implementation of face recognition technology with human rights values becomes a plausible reality when guided by the principles outlined in the Siracusa Principles. This esteemed framework offers a strong foundation for ensuring that the deployment of face recognition technology is lawful and respects the fundamental rights and freedoms of individuals.

By adhering to the Siracusa Principles, policymakers and stakeholders can navigate the intricate balance between technological advancements and human rights concerns.

Through thoughtful consideration, transparent regulation, and a commitment to accountability, the implementation of face recognition can be a transformative force that upholds, rather than undermines, the core principles of human rights in Indonesia and beyond.

In the foreseeable future, face recognition technology's continued evolution and implementation necessitate significant enhancements coupled with a heightened focus on human rights values. As this technology becomes increasingly integrated into various aspects of our lives, from security systems to personal devices, addressing the inherent challenges to privacy and individual freedoms is imperative. To ensure responsible and ethical development, improvements in face recognition algorithms and systems must be pursued with careful consideration of human rights principles.

The Balance between technological innovation and the protection of the right to privacy and the right to personal identity is paramount, requiring strong legal frameworks, transparent policies, and ethical guidelines. The future trajectory of face recognition should be shaped by a commitment to upholding the values of privacy, dignity, and security, aligning its advancements with the broader spectrum of human rights to create a technologically empowered yet ethically sound landscape.

CONCLUSIONS AND RECOMMENDATIONS

Implementing face recognition technology may spark concerns about its potential contradiction with fundamental human rights law and existing legal frameworks in Indonesia. The capabilities of facial recognition systems raise significant privacy issues, as the technology often involves collecting, storing, and analyzing personal biometric data without explicit consent. The government should make sure the legal frameworks support the implementation of face recognition to avoid any possible human rights abuse related to the right to privacy and the right to personal identity. The formulation of legal frameworks to support face recognition must be based on the Siracusa Principle concerning the limitation and derogation of rights. The formulation of legal frameworks must be precise and concrete. For instance, in implementing face recognition for national security purposes, it is imperative to have implementing regulations (e.g., Peraturan Pemerintah/Government Regulation) dedicated to national security, and the rules must be aligned with the principles of human rights.

This research suggests the government make a comprehensive legal framework to cover the implementation of face recognition technology for national defense and security interests, the interests of law enforcement processes, public interests in the framework of state administration, supervision of the financial services, monetary, payment systems, and economic system stability conducted in the framework of state administration; and statistical and scientific research interests. Each purpose must be covered by proper legal frameworks, with their respective implementation or implementation of regulations that possess the characteristics of *the Omnibus Law*.

REFERENCES

Bestari, Novina Putri. "Heboh Kasus Face Recognition, KAI Bisa Langgar Hukum." CNBC Indonesia. Last modified 2023. Accessed December 14, 2023. https://cnbcindonesia.com/tech/20231121125452-37-490720/heboh-kasus-face-recognition-kai-bisa-langgar-hukum.

Fadillah, Dani, Zalik Nuryana, and Sularso. "Public Opinion of the Facial Recognition Policy in China by Indonesian Student in Nanjing City." OFS Preprints 24, no. 4 (2020): 1645–1652.

Kereta Api Indonesia. "Terapkan Face Recognition, Boarding Kini Cukup Pindai Wajah." Kai. Id. Last modified 2022. Accessed December 14, 2023. https://www.kai.id/information/full_news/5452-terapkan-face-recognition-boarding-kini-cukup-pindai-wajah.

Kumaran, Ivano, Muhamad Ramdhani Firmansyah, Eva Fauziah, Yosep B. Hutahaean, Anang Suryana, Aryo De Wibowo Muhammad Sidik, Marina Artiyasa, Anggy Pradiftha Junfithrana, and Ilman Himawan Kusumah. "Pengenalan Wajah Menggunakan Pendekatan Berbasis Pengukuran Dan Metode Segmentasi Dalam Berbagai Posisi Dan Pencahayaan." Jurnal Teknik Elektro 3, no. 1 (2022): 5–8.

Marzuki, Peter Mahmud. Penelitian Hukum. Jakarta: Kencana Prenada, 2010.

Maulana, Muhammad Dimas, Achmad Setiyo Prabowo, and Totok Warsito. "RANCANGAN PENDETEKSI WAJAH DENGAN MENGGUNAKAN KOMPUTASI MATLAB SEBAGAI ALAT BANTU KEAMANAN DI BANDAR UDARA." Proceedings of The SEMINAR NASIONAL INOVASI TEKNOLOGI PENERBANGAN (SNITP) TAHUN 2020 (2020).

Muhaimin. Metode Penelitian Hukum. Mataram: Mataram university Press, 2020.

Nasution, Hilmi Ardani, and Marwandianto. "Hak Atas Kebebasan Berpendapat Dan Berekspresi Dalam Koridor Penerapan Pasal 310 Dan 311 KUHP." Jurnal HAM Balitbangkumham 11, no. 1 (2020): 1–25.

Nugem, Duke. "Kemendagri Dan Polri Terapkan Teknologi Pengenalan Wajah Di KTT G20." TB NEWS. Last modified 2022. Accessed December 14, 2023. https://tribratanews.babel.polri.go.id/2022/11/14/kemendagri-dan-polri-terapkan-teknologi-pengenalan-wajah-di-ktt-g20/.

Rachmaniar, Adelia, Aris Mustriadi, Hasyimi Pradana, and Aditya Prastian Supriyadi. "Regulating Facial Recognition Technology under the Indonesian Privacy and Data Protection Frameworks: The Pacing Problem?" 1st International Conference on Law Studies "Law Policy on Transnational Issues" Jakarta 1, no. 1 (2020): 23–44.

Warong, Kristian Megahputra, Caecilia J. J. Waha, and Cornelius Tangkere. "Kajian Hukum Hak Asasi Manusia Terhadap Kebebasan Berpendapat Oleh Organisasi Kemasyarakatan Di Media Sosial." Lex Administratum VIII, no. 5 (2020): 44–53.