BIS HUMANITIES AND SOCIAL SCIENCE

Volume 2 2025 | DOI: 10.31603/bishss.331
6th Borobudur International Symposium on Humanities and Social Science (BIS-HSS) 2024

UNIMMA PRESS
Universitas Muhammadiyah Magelang

Urgency of face recognition technology in criminal investigation process: A formal legal perspective

Kurnia Dewi Anggraeny[1*], Bima Nurfauzi[1], Atqo Darmawan Aji[1]

[1] Universitas Ahmad Dahlan, Yogyakarta, Indonesia
[*]Corresponding author email: kurniadewi@law.uad.ac.id

Abstract

Face recognition technology is a system that utilizes face images from photos or videos to identify an individual. This system works by comparing face data obtained from images with a database sourced from the Civil Registration Office and internal police databases. The problem in this research is how urgent and how to implement facial recognition technology in the criminal investigation process in a formal legal perspective. This research aims to determine the urgency and implementation of face recognition technology in the criminal investigation process in a formal legal perspective. In this study, the author reviews and analyzes the development of face recognition technology as an artificial intelligence technology that is used to facilitate the tasks of law enforcement. Using a normative-empirical research type and a qualitative approach, this study is expected to reveal the challenges, benefits, and legal implications of using this technology. The results of this study show that face recognition technology has great potential in improving the efficiency of investigations and enhancing security in Indonesia. This technology plays a role in accelerating the identification process, increasing the accuracy of investigation results, expanding the scope of investigations, and supporting other investigative methods. This research contributes to identifying current knowledge gaps and is expected to provide practical solutions to existing problems and boost the efficiency and effectiveness of implementing face recognition technology in Indonesia.

Keywords

Urgency, Face recognition technology, Criminal investigation

Published:
May 30, 2025

Selection and Peer-review under the responsibility of the 6th BIS-HSS 2024 Committee

Introduction

Face recognition technology has been studied by researchers and developed as a method to identify human faces through images. As technology advances, face recognition systems have become increasingly sophisticated, utilizing powerful computers and machine learning algorithms. This technology has found widespread application in various sectors, including advertising and marketing, retail, insurance, banking, transportation, entertainment, aviation, and education.

Face recognition technology has also been employed in the fields of security and law enforcement by numerous countries. It has been used to enhance security measures, such as screening individuals entering airports through e-passport data, facilitating access to public services, and aiding in law enforcement investigations. The utilization of face recognition technology within the Indonesian legal and industrial contexts has indirect legal implications that pose potential threats to citizens' rights, including the right to data privacy and privacy as guaranteed by Article 28G paragraph (1) of the 1945 Constitution.

In the Indonesian legal system, face recognition technology can be implemented during the investigative process of criminal cases. This technology has been employed in several investigations, such as the Ade Armando case. Face recognition technology used to uncover such incidents can subsequently be classified as electronic evidence, as defined in Article 5 section (1) of Law No. 1 of 2024 concerning Electronic Information and Transactions.

The advent of face recognition technology has stolen the spotlight in recent years. This technological advancement allows computers to recognize human faces with a high level of accuracy. The use of face recognition technology is increasingly widespread, not only used by developed countries but also in developing countries such as Indonesia. Indonesia has implemented face recognition technology in various sectors, from security to public services. This system is used for quick and accurate identification of individuals, for example this technology can be used for identity verification when making banking transactions or entering important buildings.

The concept of face recognition has long been researched. One of the pioneers in this field is Takeo Kanade, who in his thesis entitled "Picture Processing System by Computer Complex and Recognition of Human Faces" discusses image processing systems and human face recognition. Face recognition technology works by analyzing various face features, such as the shape of the eyes, nose, and mouth. These features are then processed by a computer to produce a digital representation of a person's face. This digital representation is then used to compare with an existing face database [1].

Face recognition technology in Indonesia began its development in the 1970s. However, its practical application by the Indonesian National Police only started in 2012. Initially, the technology was relatively simple, relying on manual face sketches. These sketches were created based on witness descriptions and served as a foundational tool for identification purposes [2].

As computer technology advanced, the manual sketching method was gradually replaced by more sophisticated computer-based systems. These systems were designed to enhance security and were also used for search purposes. They utilized images, particularly photos or videos, to identify individuals.

According to experts like IPTU M. Indra Ardiawan, S.Kom., and Bapak Hery Cahyono, S.Pd., face recognition systems function by comparing an input image (like a photo or

video) against a database of stored face images. This database typically contains personal information obtained from electronic ID cards (e-KTP), such as names, birthdates, genders, and addresses. In addition to e-KTP data, the system may also access police databases containing criminal records, case histories, and other relevant information.

In the early stages of face recognition technology in Indonesia, manual sketches were commonly used to identify suspects in criminal cases. These sketches, created based on witness descriptions, were often crude and imprecise. However, as technology advanced, the accuracy of face sketches improved significantly. Modern face recognition systems can generate highly detailed visual representations of a suspect's face based on witness descriptions. These detailed sketches can be disseminated to the public through various media channels, such as television and social media, to solicit information [2].

Face recognition technology has significantly streamlined the process of identifying suspects. By comparing input images against vast databases, law enforcement agencies can quickly identify potential matches. This technology has also improved the accuracy of investigations and expanded the scope of law enforcement efforts.

In the expansion of the scope of investigation, this technology plays a role in tracking and capturing suspects who flee or hide by comparing the perpetrator's photo with the existing face recognition database. Criminals whose data has been obtained will be monitored by surveillance camera mechanisms with face recognition features installed in public spaces, such as train stations, airports, and shopping centers, to assist in real-time identification. This technology will also assist in analyzing CCTV footage to identify criminals from various angles, even when the perpetrator's face is partially covered. The initial processing results of face recognition technology can be used as preliminary clues regarding the identity of the perpetrator to facilitate the subsequent investigation process, and the presented processing results can also be used as additional evidence in the investigation process to strengthen the charges against the perpetrator.

Face recognition technology has become an integral part of modern life, especially in the 5.0 revolution era marked by rapid digital technology development. The use of this technology has also expanded widely and penetrated various sectors, from security to banking services. A study titled "Face Recognition Vendor Test (FRVT)" conducted by the National Institute of Standards and Technology (NIST) from the United States shows that face recognition systems have achieved a high level of accuracy in identifying individuals [3].

Face recognition technology has great potential to enhance security and efficiency across various sectors. The use of this technology must be carried out with consideration of the existing ethical and legal implications. During the demonstration event some time ago, face recognition technology was used to identify the perpetrators of the assault on Ade Armando. This case highlights the potential and challenges of

using this technology in law enforcement, although it was initially caused by an identification error. This case highlights the importance of data accuracy and algorithms in face recognition systems, as identification errors can seriously impact a person's reputation [4].

The case of misidentification by face recognition technology is a concrete example of privacy issues that are directly or indirectly related to the use of this technology. The errors in identification by face recognition technology pose a threat to the public regarding the risk of privacy violations, which can be considered quite serious. This technology should be able to identify individuals with a high level of accuracy, but in this case, the technology was not accurate in distinguishing between individuals who were involved in the incident and others who only had physical similarities. This incident can result in losses, such as false accusations against the wrong individuals and the potential misuse of face data [5].

This incident raises significant concerns regarding the privacy of face data obtained from this technology. The public does not know for sure how the face data will be managed and used by certain parties. The accuracy of face recognition technology, which is considered still inadequate, becomes a particular concern because there is a risk of face data being misused. This makes individual privacy very vulnerable and can damage public trust in face recognition technology.

The errors from face recognition technology results that occurred in Indonesia should be taken quite seriously. This incident highlights the importance of having regulations with a strong fundamental standing in the use of such technology. In order to ensure that face recognition technology is used responsibly and does not violate individual privacy rights, comprehensive regulations governing the use of this technology are necessary. The existence of good regulations is expected to minimize and even prevent the misuse of technology in the future.

In the regulations that will be formed later, one of the main priorities is the protection of privacy for individuals who are indirectly involved in the development and implementation of face recognition technology. There needs to be a balance between technological advancement and the fundamental rights of individuals residing in the territory of the Unitary State of the Republic of Indonesia. The use of face recognition technology with extensive coverage can threaten individual freedom and create a society full of surveillance. Comprehensive regulations regarding the use of data resulting from face recognition technology and how that data is protected by the authorities.

The cases that have occurred in Indonesia following the implementation of face recognition technology show that privacy issues are not just local problems, but also global challenges that must be faced together. Countries around the world also need to work together to formulate international standards and regulations governing the use of face recognition technology. The general public can also monitor that this technology

is used ethically and benefits all citizens. Currently, face recognition technology still faces challenges, as the recognition algorithms still have a relatively high error rate. Face recognition technology also has a weakness where it can contain biases that lead to discrimination against certain groups. The specific groups referred to are such as minority groups or individuals with certain face conditions. This can happen due to unrepresentative training data or unfair algorithm design.

In developments that can certainly be seen in a tangible way, Indonesia must also issue regulations specifically governing the use of face recognition technology itself. Law No. 1 of 2024 on Information and Electronic Transactions is legislation in force in Indonesia and relates to face recognition technology. This law contains articles relevant to face recognition technology, namely Article 26 paragraph (1) of Law No. 1 of 2024 on Information and Electronic Transactions. This article emphasizes the importance of individual consent in the use of their personal data through electronic media, including biometric data such as face recognition. This technology must establish a legal foundation to provide privacy protection in the context of face recognition technology [5].

Considering the great potential and challenges faced, in addition to the existing regulations, there is a need to further develop clear regulations regarding the use of face recognition technology. Mr. Hery Cahyono, S.Pd., (Polda Metro Jaya, Jakarta) stated that within the scope of police duties and technical assistance, the use of face recognition technology has been regulated by a guideline book in the form of Standard Operating Procedures (SOP). Based on the SOP, special training is then conducted for operators who will use face recognition technology. The SOP is a written guideline that is confidential, as its general dissemination would trigger the emergence of new methods by criminal actors to evade the application of this technology. That modus operandi can become a point of difficulty in the process of identifying images captured by security cameras.

Currently, the Indonesian National Police (Polri) has developed face recognition technology using the latest methods, achieving a high accuracy percentage. The development of face recognition technology is currently comparing one method with another or collaborating several methods to achieve a high level of accuracy. Through proper management and attention to ethical aspects, face recognition technology can become a highly beneficial tool in various fields, including law enforcement. It is important to remember that this technology is merely an auxiliary tool, and its use must always be balanced with considerations of humanity and justice.

Method

The type of research used by the author in this article is normative-empirical research type and qualitative approach, this study is expected to reveal the challenges, benefits, and legal implications of using this technology. The approach used by the author in this research is a sociological legal approach, especially using statute approach, case

approach, and structural approach. Data collection methods in this study include literature studies and interviews.

Results and Discussion

The advent of face recognition technology has stolen the spotlight in recent years. This technological advancement allows computers to recognize human faces with a high level of accuracy. The use of face recognition technology is increasingly widespread, not only used by developed countries but also in developing countries such as Indonesia. Indonesia has implemented face recognition technology in various sectors, from security to public services. This system is used for quick and accurate identification of individuals, for example this technology can be used for identity verification when making banking transactions or entering important buildings.

The concept of face recognition has long been researched. One of the pioneers in this field is Takeo Kanade, who in his thesis entitled "Picture Processing System by Computer Complex and Recognition of Human Faces" discusses image processing systems and human face recognition. Face recognition technology works by analyzing various face features, such as the shape of the eyes, nose, and mouth. These features are then processed by a computer to produce a digital representation of a person's face. This digital representation is then used to compare with an existing face database [1].

Face recognition technology in Indonesia has been implemented quite well. At several national-international events, this face recognition technology has also been employed to ensure the security and continuity of the event. Quoted from the online media Tempo.co, the 42nd ASEAN Summit in Labuan Bajo, Manggarai Barat, East Nusa Tenggara in 2023, the National Police Headquarters deployed 2,627 personnel along with face recognition technology installed to secure the event [6]. As stated by Mr. Hary Cahyono, S.Pd., in addition to that event, face recognition technology was also used during the U-17 World Cup in Solo and Surabaya.

In the field of crime prevention and investigation, face recognition technology has proven to be very valuable. Law enforcement agencies in Indonesia have successfully used it to identify and apprehend suspects, as well as to prevent and investigate criminal activities. The contribution of technology in these fields is clear in its track record of enhancing the efficiency and effectiveness of law enforcement efforts. The capabilities of this technology have made the monitoring process more effective and, in turn, also contributed to public safety and crime prevention. Its role in monitoring public spaces ensures a higher level of vigilance and security [1].

Indonesia, as a country that implements face recognition technology, has faced challenges in the application of this technology. Initially, Indonesia adopted this technology through cooperation with foreign police forces such as Australia and the United States. The adopted technology is designed to recognize the faces of foreign nationals. According to Mr. Hery Cahyono, S.Pd. (Polda Metro Jaya, Jakarta), the data

used in the technology is more suitable for recognizing the faces of foreign nationals. The data resulted in the application of this technology being less effective in recognizing the faces of Indonesian citizens. This incident is clearly caused by the differences in face characteristics between the two groups. Seeing the obstacles, the Indonesian National Police then decided to develop their own face recognition technology. The development of this technology is certainly aimed at creating a system with high accuracy in recognizing the faces of Indonesian citizens. The development of this technology is expected to enable face recognition technology to be used more effectively.

Face recognition technology can currently be referred to as one of the artificial intelligence technologies that is becoming increasingly sophisticated. The emergence of this technology has attracted the attention of countries around the world, including Indonesia. Its application, which is useful for various sectors, cannot be denied because it will provide benefits to the sectors that implement this technology. As a country with a large and diverse population, many questions inevitably arise regarding the regulation and ethics of its use.

Results

Face recognition technology, as explained, can currently be integrated in real-time during an event, so that every person passing in front of the camera will automatically have their identity detected. The detected identities are sourced from civil registry data as well as the internal police database. The application of real-time face recognition technology at an event can significantly enhance security levels. This system is expected to be able to verify identities quickly and accurately, thereby preventing unauthorized access and detecting individuals on the watchlist, thus minimizing the risk of criminal acts or security breaches.

This technology, which offers various benefits, also needs to be carefully considered regarding its implementation process. Some of the challenges that need to be addressed include the system's accuracy in poor lighting conditions or dynamic face expressions. The potential for misidentification, which could also lead to legal consequences. The legal consequences of this technology are certainly the responsibility of the relevant parties to minimize or even prevent from occurring.

Currently, face recognition technology has brought a breath of fresh air to the realm of law enforcement. The existence of this technology has helped the process of identifying a case to become more efficient and accurate. Especially within the environment of the National Police Headquarters, face recognition technology has been applied in various activities. One of the general applications is at the entrance access of the Mabes Polri building on Jalan Trunojoyo No.3, RT.2/RW.1, Selong, Kebayoran Baru District, South Jakarta City, Special Capital Region of Jakarta. Specifically, the surveillance cameras at the entrance of the Mabes Polri area will capture visuals of people passing through that area.

According to IPTU M. Indra Ardiawan S.Kom. (Polda Metro Jaya, Jakarta), another application is also carried out by the field that is the focus of this thesis research, namely the Police Photography Field (Bidtopol) Pusinafis Bareskrim Polri. The field already has the necessary equipment in the form of special tools designed to recognize a person's face. Mr. Hery Cahyono, S.Pd added that there is also web-based technology that can be accessed by the operators of this technology through computers, laptops, or smartphones. The operation of this face recognition technology is carried out by specially appointed police officers. These officers have access to the system and are responsible for the use of the technology. The officer must maintain the security and confidentiality of the data by being obligated to sign a data confidentiality agreement.

Conveyed by Mr. Hery Cahyono, S.Pd. (Polda Metro Jaya, Jakarta), the Bidtopol Pusinafis Bareskrim Polri, as a technical police assistance, will process evidence in the form of photos and videos provided by the investigator based on the approval of the leadership, namely the Kapusinafis Bareskrim Polri. The results obtained by Bidtopol will be returned for further consideration by the investigator. In practice, Bidtopol Pusinafis Bareskrim Polri, through designated operators, will input the suspect's photos or videos into the system, allowing the operator to quickly identify the criminal's identity. Before the data is processed, standardization will first be carried out to ensure the quality of the images, including cropping the face area and adjusting the size and orientation of the images to achieve good result accuracy. The data that has been obtained will then be processed using a face recognition technology algorithm based on facenet.

This technology serves as a bridge between visual data and individual identity information, or in other words, face recognition technology functions as an additional "eye" for investigators in searching for clues and solving cases. In the process of criminal investigation, the implementation of face recognition technology will significantly contribute to increasing efficiency and accuracy, as well as enhancing the success in solving cases. The surveillance camera system in public spaces that has been integrated with face recognition technology can also be used to detect someone who is on the Wanted List (DPO). This technology works by processing data in the form of photos of the perpetrators, witnesses, and victims, as well as CCTV footage from the crime scene, and will match the obtained data with the database held by the police. The integrated face recognition system under Pusinafis Bareskrim Polri allows for data exchange with the police management information system to enhance the role of technology in the criminal investigation process.

The face recognition technology possessed by the police is not only used internally. Other institutions that require face recognition services can submit a request to the Bareskrim Polri, which will be forwarded to the Bidtopol through the Kapusinafis. This open access allows various parties to utilize this advanced technology to enhance security and efficiency in various sectors. IPTU M. Indra Ardiawan, S.Kom. added that the open access to face recognition technology that has been implemented certainly raises questions about the success rate of this artificial intelligence technology. He also

explained that it is not yet possible to determine the percentage of the role of this technology, because there are cases that must be resolved with face recognition technology, and there are also cases that can be resolved without using it. In general, this technology can work optimally when the photo/video evidence provided by the investigator is of good quality (not blurry, high resolution, good angle), resulting in high accuracy in the processing. In contrast, if the photo/video evidence provided by the investigator is of low quality, the results will also show low accuracy, such as a large number of suspected perpetrators.

IPTU M. Indra Ardiawan, S.Kom. also provided an example regarding the possible percentage of success of face recognition technology. The data obtained from the face recognition process consists of suspected perpetrators who will be detained and then questioned like witnesses, so they cannot yet be referred to as Suspects or Defendants. The suspected perpetrators' data will be displayed by the face recognition technology team as candidates 1-10, sorted by accuracy level. The result of the identification does not always indicate that the actual perpetrator is in the first position; they could be in another position. This occurrence arises due to several aspects, including changes in face conditions, low image resolution, and others, making this technology require complex methods to analyze the suspect's photo/video with the emerging candidates.

Mr. Hery Cahyono, S.Pd. in another point stated that the Pusinafis Bareskrim Polri has established a strategic synergy with the Population and Civil Registration Office (Dukcapil) as an effort to optimize case handling. Accurate and up-to-date access to population data will expedite the process of identifying criminal offenders, tracking the whereabouts of suspects, and reconstructing the events of the case. Pusinafis also plans to collaborate with the Directorate General of Immigration to facilitate the resolution of cases involving Foreign Nationals (WNA), particularly those frequently occurring in tourist destinations like Bali. Based on data from the Directorate General of Immigration website, at the beginning of 2023 during the Indonesia-Indonesia period, 620 WNA were deported from Indonesia. These 620 WNA were expelled during that period for immigration violations such as visa and residence permit abuse, overstaying, disturbing public order, and not complying with regulations in Indonesia. In addition to imposing deportation sanctions, the immigration authorities also impose administrative sanctions in the form of a ban on re-entering Indonesian territory for a certain period [1].

Mr. Hery Cahyono S.Pd. and IPTU M. Indra Ardiawan, S.Kom., (Polda Metro Jaya, Jakarta) conveyed several points regarding what will be done if a perpetrator's identity is not integrated with Dukcapil, as follows:

1. If the perpetrator is not recorded in Dukcapil, the obtained data will be compared manually. Data in the form of fingerprints at the crime scene, whether belonging to the perpetrator or the victim, will be compared with individuals suspected of being the perpetrator or the victim.
2. If the fingerprint identification does not yield results, another step that can be taken is DNA identification conducted by the DVI Team of Pusdokes Mabes Polri.

3. In cases involving child perpetrators who do not yet have an eKTP, Pusinafis conducts the "Inafis Goes to School" activity to obtain more complete data and prevent incidents involving child perpetrators.

Pusinafis Bareskrim Polri hopes that after integrating with Dukcapil and the Directorate General of Immigration, law enforcement will become more effective and efficient. It is also hoped that after the data integration, the processes of identifying criminals, searching for witnesses, and checking someone's background will be faster and more accurate. This data integration will also enable investigators to perform real-time data cross-checks, allowing for a more comprehensive analysis of a case. This will then facilitate the resolution of various cases, ranging from conventional crimes to transnational crimes.

The implementation of recognition technology, with its myriad benefits, also has the potential to violate several human rights, such as the right to privacy, personal data protection, and freedom of expression. The implications for existing legal regulations must also be considered in the implementation of this technology. The research conducted by Fredi Syahlulus Tarigan highlights several issues related to the use of this technology. The potential violation of individual privacy has become one of the main issues. The use of face recognition technology without the individual's consent or knowledge can be considered a serious violation of privacy. Automatic face recognition can be done without individual consent, allowing for unauthorized monitoring and tracking. This can raise concerns about the misuse of personal data and excessive surveillance.

Discussion

The collection and processing of biometric data such as face data should comply with applicable laws and regulations. Individuals have rights over their personal data, and they have the right to know how their data is used. It is important to ensure that the collection and use of face data is done in an accountable and transparent manner, and in accordance with the principles of personal data protection [2].

The crucial issue that arises from the use of face recognition technology is data security. The database in Indonesia, which is still very vulnerable to hacking and data theft, must be addressed through strict regulations and maximum protection. Face recognition technology can also have serious impacts on human rights. The misuse of this technology can also pose a threat to civil liberties and individual rights, therefore, to protect human rights, strong legal safeguards and oversight of its use are necessary.

The emergence of legal issues that must be addressed becomes a benchmark for the importance of regulations that can effectively, ethically, and clearly govern this technology. The regulation must balance the benefits of face recognition technology and the protection of individual rights. International cooperation in developing uniform global regulations on face recognition technology with the same objectives is also important. The development and impact of face recognition technology on society need

to be accompanied by continuous monitoring and evaluation. Regulations and regulatory frameworks must keep pace with technological developments and emerging issues.

This research shows that the legal issues related to the use of face recognition technology are important and complex. Regulations must ensure that this technology is beneficial to society without sacrificing individual privacy. A strong legal framework will be essential to ensure that this technology develops responsibly, so it can become a key determinant of the future of face recognition technology.

The implementation of new technology in various sectors is certain to have a significant impact, whether it is perceived as an advantage or a disadvantage. This technology has the advantage that the implementation of biometric identification systems offers a number of significant benefits in various sectors, especially in the field of security. The utilization of unique physical characteristics of each individual, such as fingerprints, face features, or iris patterns, can significantly enhance security levels. Accurate and rapid identification allows authorities to track individuals more easily, thereby narrowing the movements of criminals. The biometric-based identity verification process can also expedite public services, such as airport security checks or access to government buildings.

The resource person, Mr. Hery Cahyono, S.Pd., also stated that face recognition technology supported by advanced equipment is considered safer. The safety referred to is because there is no need to come into direct contact with the perpetrator of the crime. The speed of technology in identifying perpetrators is also considered quite optimal, as it will immediately display the identity data of the suspected perpetrator. This result will then be utilized to carry out arrests and close off the perpetrator's escape routes through access that includes face recognition technology.

In addition to its advantages, this technology has weaknesses, as its implementation of biometric identification systems brings a number of challenges related to privacy and data accuracy. The main concern is the potential misuse of biometric data, which is unique and permanent. Face data, fingerprints, or iris patterns falling into the wrong hands can be used for unethical purposes, such as identity theft or mass surveillance. The quality of the biometric data used is crucial in determining the accuracy of the identification results. Poor image quality, inadequate lighting, or sensor damage can cause identification errors that potentially lead to legal issues.

Misidentification is another risk that needs to be considered in the implementation of biometric systems. This system is not always perfect because it can yield false negatives. The negative result referred to is when the system fails to recognize someone who should be recognized. This can have serious consequences, especially in the context of law enforcement.

In the integration of biometric identification systems with other systems, such as immigration systems, it also presents its own challenges. Differences in standards and

data formats between various systems can hinder the interoperability process and slow down case handling. From another perspective, the mass use of biometric data can raise concerns related to government surveillance and human rights violations, necessitating clear and comprehensive regulations. These regulations will be used to govern the use of biometric data, ensure privacy protection, and prevent technology misuse.

Technology advancements significantly impact various aspects of life, including law enforcement. Facial recognition technology has revolutionized criminal investigations, offering enhanced efficiency and accuracy. Amidst increasingly complex crimes with digital dimensions, this innovation is crucial. Although Indonesia's Criminal Procedure Code (KUHAP) doesn't regulate facial recognition, its benefits are evident. Most notably, it enhances identification processes. By facilitating swift and accurate identification, facial recognition reduces identity fraud risks and strengthens overall security measures [3].

Facial recognition is crucial in criminal law enforcement, enabling authorities to easily identify and apprehend suspects. This technology streamlines suspect identification and prevents future crimes. According to Article 5 of Indonesia's Personal Data Protection Law (UU No. 27/2022), individuals have the right to information regarding their personal data usage. Article 26 (1) of the Electronic Information and Transactions Law (UU 11/2008) regulates electronic personal data usage, requiring consent from the concerned individual. These regulations pose challenges for leveraging facial recognition in Indonesia's criminal justice system.

Comprehensive legal framework regulating facial recognition technology in criminal proceedings is essential. Governments play a pivotal role in ensuring public order and prosperity through effective criminal law [4]. Facial recognition can significantly facilitate law enforcement; thus, clear guidelines are necessary. Establishing procedural regulations for facial recognition will streamline criminal justice. Criminal law must adapt to evolving technologies. Clear regulations will expedite criminal proceedings, enhancing overall efficiency [5].

Indonesia requires comprehensive legislation governing facial recognition in criminal proceedings. This regulation will ensure public order, prosperity and efficient law enforcement. Clear guidelines are necessary to facilitate criminal justice [5]. Although Indonesian police utilize facial recognition technology to identify traffic offenders, supporting regulations are lacking. Since 1981, Indonesia's criminal procedure code has remained unchanged, becoming outdated [6]. Reforms are essential to modernize criminal law, aligning it with technological advancements. Updates will provide legal certainty for facial recognition in investigations, enhancing criminal justice efficiency.

Conclusion

Face recognition technology is a system that utilizes face images in the form of photos or videos to identify a person. This system works by comparing the face data obtained

from the images with the stored database. Face recognition technology in Indonesia is currently used as a preventive measure against criminal activities. In the security sector, surveillance cameras with face recognition features have been installed in public places to assist in the real-time identification of criminals. With the increase in accuracy and speed, this technology is expected to become increasingly integrated into various aspects of every individual's life. This also requires us to continuously develop adequate regulations and standards to ensure that the use of this technology aligns with humanitarian values.

The increased use of face recognition technology in Indonesia should serve as a momentum for the government to promptly formulate comprehensive regulations to prevent the misuse of this technology and protect the privacy rights of the public. The implementation, which is an interesting development, needs to be balanced with mature legal and ethical considerations. The existence of a clear and comprehensive legal framework is essential so that this technology can be utilized responsibly and provide benefits to society without sacrificing human rights. After the implementation of this regulation, it is hoped that issues regarding individual privacy, the right to personal data, data security, and discrimination from algorithmic bias can also be resolved.

Acknowledgement

I would like to express my gratitude to the Chancellor of Ahmad Dahlan University for the permission given to the author and also to the Dean of the Faculty of Law and the Head of the Legal Studies Program of Ahmad Dahlan University for their trust in the author so that funding can be provided to attend the international seminar and call for papers 6th BIS 2024 organized by University of Muhammadiyah Magelang.

References

[1] D. J. Imigrasi, "Dirjen Imigrasi: 620 WNA Nakal Dideportasi, Termasuk yang Viral di Bali."
[2] F. S. Tarigan, "Implikasi Hukum Terhadap Penggunaan Teknologi Pengenalan Wajah: Kajian Literatur," Judge J. Huk., vol. 4, no. 01, pp. 16–20, Apr. 2023, doi: 10.54209/judge.v4i01.375.
[3] S. A. Kusnadi, "Perlindungan Hukum Data Pribadi Sebagai Hak Privasi," AL WASATH J. Ilmu Huk., 2021, doi: 10.47776/alwasath.v2i1.127.
[4] I. R. Gulo, S. Sunarmi, and M. Mulyadi, "Perlindungan Hukum Terhadap Korban Tindak Pidana Pencucian Uang Dengan Predicat Crime Tindak Pidana Penipuan Yang Hartanya Dirampas Untuk Negara Studi Putusan Mahkamah Agung NO. 3096 K/PID.SUS/2018," J. RECTUM Tinj. Yuridis Penanganan Tindak Pidana, 2023, doi: 10.46930/jurnalrectum.v5i3.3496.
[5] C. T. Noerman and R. D. Agustanti, "Pertanggungjawaban Artificial Intelligence Sebagai Subjek Hukum Yang Melakukan Tindak Pidana Korupsi," J. Huk. Samudra Keadilan, 2023, doi: 10.33059/jhsk.v18i2.8722.
[6] D. Samosir, "Berbagai Permasalahan Yang Muncul Sehubungan Dengan Perumusan KUHAP," J. Huk. Pro Justitia, 2006.