Vol 2 No 1 2025 || E-ISSN 2997-7258

The Journal of Academic Science

journal homepage:
https://thejoas.com/index.php/

Facial Recognition Technology in Indonesia: Opportunities and Ethical Challenges

Dendy K Pramudito
Universitas Pelita Bangsa
Email: doktor.haji.dendy@pelitabangsa.ac.id

KEYWORDS
Facial Recognition Technology, Indonesia, Ethical Challenges, Privacy and Regulation, Emerging Technologies

ABSTRACT
Facial Recognition Technology (FRT) has emerged as a powerful tool in various sectors, ranging from security to personalized services. In Indonesia, its adoption is gaining momentum, offering significant opportunities for enhancing public safety, streamlining administrative processes, and improving customer experiences. This study employs a qualitative research methodology to explore the implementation of FRT in Indonesia, focusing on its potential applications and the ethical challenges it presents. Data were collected through document analysis, interviews with key stakeholders, and observations of relevant cases. The findings reveal that FRT is being utilized in diverse fields, such as law enforcement, border control, and financial services, where it offers efficiency and accuracy benefits. However, its rapid deployment also raises critical ethical concerns, including privacy violations, data security risks, biases in algorithm design, and potential misuse for surveillance purposes. Furthermore, the lack of comprehensive regulations governing FRT usage in Indonesia exacerbates these challenges. This study underscores the urgent need for a balanced approach that maximizes the opportunities provided by FRT while addressing its ethical and regulatory shortcomings. By fostering transparent policies, public awareness, and inclusive technology development, Indonesia can harness FRT as a transformative tool without compromising ethical standards. The insights from this research contribute to the global discourse on the responsible implementation of emerging technologies in diverse socio-cultural contexts.

1. INTRODUCTION

The emergence of Facial Recognition Technology (FRT) has become a transformative force across various industries, offering innovative solutions in security, public administration, financial services, healthcare, and more(Rosenbloom et al., 2022). Globally, FRT has been adopted as a tool to enhance public safety, streamline operational efficiency, and provide personalized services(Krishnan et al., 2024). In Indonesia, this technology is gaining momentum, particularly in sectors such as law enforcement, immigration control, and digital financial platforms, where the ability to accurately and efficiently identify individuals is critical (Latonero & Kift, 2018). FRT's potential to address issues like identity verification and crime prevention has positioned it as an essential component of Indonesia's efforts to modernize and digitize its infrastructure(Pribadi et al., 2021).

Despite its potential, the implementation of FRT is fraught with significant ethical challenges and risks, particularly concerning privacy, data security, algorithmic bias, and surveillance misuse(Mosa et al., 2024). These

challenges are further exacerbated by Indonesia's evolving legal and regulatory framework, which has yet to adequately address the governance of advanced technologies like FRT(Ardiansyah et al., 2015). Unlike more mature technology ecosystems in developed countries, where regulatory oversight and ethical standards are more established, Indonesia faces the dual challenge of integrating FRT into its socio-economic systems while simultaneously building the legal and ethical infrastructure to mitigate risks(Radyati & Tjahjono, 2021).

A research gap exists in the current body of knowledge regarding FRT, especially in the Indonesian context. Most studies on FRT focus on its technical capabilities or its application in Western or highly industrialized nations(West & Bogers, 2014). While these studies provide valuable insights, they fail to account for the unique socio-cultural, legal, and economic dynamics of Indonesia as a developing nation. For instance, there is limited research on how FRT interacts with Indonesia's pluralistic society, decentralized governance structures, and nascent data protection laws (Testriono, 2022). Moreover, studies often neglect the perspectives of local stakeholders, such as policymakers, technologists, and civil society organizations, who play a crucial role in shaping the ethical and practical outcomes of FRT deployment. This lack of context-specific research creates an urgent need to fill the void with localized, qualitative insights (Lastikova, 2023).

The urgency of this research stems from the rapid deployment of FRT in Indonesia without sufficient safeguards or comprehensive regulatory mechanisms(Wahyuningtyas & Singgalen, 2023). As the technology becomes more integrated into critical sectors, such as public security and financial services, the risks associated with its misuse ranging from privacy violations to discriminatory practices become increasingly significant(Citron & Solove, 2022). Without a clear framework for responsible implementation, there is a danger of FRT being misused for mass surveillance or other unethical purposes, potentially undermining public trust and infringing on individual freedoms(Bilal et al., 2020). Additionally, the lack of awareness among the general public and stakeholders about the ethical challenges of FRT further heightens the need for research that not only identifies risks but also proposes actionable solutions.

While previous research has primarily focused on the global adoption of FRT and its implications, few studies have examined its deployment in Indonesia, particularly from an ethical and regulatory perspective(Wahyuningtyas & Singgalen, 2023). This study seeks to address this gap by exploring how FRT is being used in Indonesia, the opportunities it presents, and the ethical challenges it introduces. The novelty of this research lies in its qualitative approach, which includes the perspectives of multiple stakeholders policymakers, technology developers, and civil society representatives to provide a holistic understanding of the opportunities and challenges of FRT. By focusing on the Indonesian context, this study contributes to a growing body of literature that emphasizes the need for localized approaches to technology adoption and governance.

The objective of this research is twofold: first, to investigate the opportunities presented by FRT in Indonesia across various sectors, including public safety, financial services, and administration; and second, to identify the ethical and regulatory challenges that arise from

its implementation. Through a qualitative analysis of stakeholder perspectives and case studies, this research aims to provide actionable recommendations for policymakers, technologists, and other stakeholders to foster the responsible use of FRT.

The benefits of this study are significant. By raising awareness about the ethical implications of FRT, the research seeks to empower stakeholders to make informed decisions regarding its adoption and governance. Furthermore, the study aims to guide the development of robust legal and regulatory frameworks that can balance the benefits of FRT with the protection of individual rights and societal values. Ultimately, this research aspires to contribute to Indonesia's technological advancement by ensuring that the deployment of FRT is both innovative and ethical, setting a precedent for responsible technology adoption in other developing economies.

2. METHOD

This study adopts a qualitative research methodology to explore the opportunities and ethical challenges associated with the implementation of Facial Recognition Technology (FRT) in Indonesia(Wahyuningtyas & Singgalen, 2023). A qualitative approach is deemed appropriate for this study as it allows for an in-depth understanding of the contextual and multi-dimensional aspects of FRT deployment, particularly within Indonesia's socio-cultural and regulatory frameworks. By analyzing data from multiple sources and perspectives, this research seeks to provide a comprehensive view of how FRT is utilized, perceived, and governed in Indonesia.

Type of Research

This study is descriptive and exploratory in nature. The descriptive component focuses on mapping the applications and opportunities of FRT in various sectors in Indonesia, such as law enforcement, financial services, and public administration. The exploratory component aims to identify and analyze the ethical challenges associated with FRT, including issues of privacy, data security, algorithmic bias, and regulatory gaps. This dual focus enables the study to address both the benefits and potential risks of FRT deployment in Indonesia.

Sources of Data

The research relies on two primary sources of data:

1. Primary Data: Collected through semi-structured interviews with key stakeholders, including policymakers, technology developers, civil society organizations, and academic experts in technology and ethics. These interviews provide firsthand insights into the opportunities, challenges, and perspectives surrounding FRT in Indonesia.
2. Secondary Data: Sourced from academic journals, government reports, policy briefs, news articles, and case studies on FRT deployment globally and within Indonesia. These documents serve as a foundation for understanding the broader context and informing the analysis.

Data Collection Techniques

The study employs a combination of the following data collection techniques:

1. Semi-Structured Interviews: Conducted with 15–20 key informants, selected purposively based on their relevance and expertise in FRT-related fields. The semi-structured format allows for flexibility in exploring new themes while maintaining focus on the research objectives.
2. Document Analysis: Involves reviewing policy documents, research articles, media reports, and industry publications to understand the current state of FRT implementation and its ethical implications.
3. Observations: Observational data are collected through case studies of FRT

applications in Indonesia, such as in smart city projects, law enforcement, and customer identification systems. Observations focus on how FRT is used, perceived, and regulated in practice.

Data Analysis Methods

The study utilizes a thematic analysis approach to analyze the collected data. Thematic analysis is particularly suitable for qualitative research as it helps identify, analyze, and interpret patterns or themes within the data. The following steps are involved in the data analysis process:

1. Data Familiarization: Reading and re-reading interview transcripts, observation notes, and documents to gain a deep understanding of the content.
2. Coding: Systematically assigning codes to segments of data that reflect specific ideas, opportunities, or ethical concerns related to FRT.
3. Theme Development: Grouping related codes into broader themes, such as privacy concerns, regulatory gaps, or technological opportunities.
4. Interpretation: Interpreting the themes within the context of Indonesia's socio-cultural and regulatory landscape to draw meaningful conclusions.
    1. Validation: Cross-checking findings with key informants and secondary data to ensure the reliability and accuracy of the interpretations.

3. RESULT AND DISCUSSION

The findings of this study reveal a dynamic interplay between the opportunities presented by Facial Recognition Technology (FRT) in Indonesia and the ethical challenges it poses. The implementation of FRT in various sectors demonstrates its transformative potential, particularly in enhancing efficiency, security, and service delivery(Gomber et al., 2018). However, the study also highlights significant ethical and regulatory concerns that require immediate attention to ensure its responsible deployment.

FRT in Indonesia is being adopted across several domains, including law enforcement, financial services, and public administration. For law enforcement, the technology is primarily utilized to identify suspects, track individuals in real-time, and prevent crimes. Police forces in major cities have integrated FRT into surveillance systems, leveraging its ability to match facial data against criminal databases with remarkable accuracy and speed(Bilal et al., 2020). Similarly, in financial services, FRT is used to authenticate user identities, ensuring seamless and secure transactions in the growing digital economy. Moreover, public administration has begun to incorporate FRT into programs such as smart city initiatives, where it plays a critical role in traffic management, citizen identification, and access control to public facilities.

These advancements underscore the opportunities FRT offers for addressing persistent challenges in governance, security, and service delivery. It has the potential to reduce fraud, enhance public safety, and streamline administrative processes, making it an essential tool in Indonesia's journey toward digital transformation. The technology's ability to improve operational efficiency and minimize human error is particularly valuable in a developing country with resource constraints and vast geographical challenges.

However, the study also identifies several ethical challenges associated with the rapid adoption of FRT. One of the most pressing concerns is the issue of privacy. FRT inherently involves the collection and processing of biometric data, raising concerns about the extent to which individuals' rights to privacy are protected. In Indonesia, where comprehensive data protection laws are still in their infancy, there is a significant risk of misuse or unauthorized access to sensitive personal information. The absence of stringent legal frameworks exacerbates this issue, leaving individuals vulnerable to potential surveillance abuses and data breaches.

Another critical concern is algorithmic bias. FRT systems, often trained on datasets

that do not adequately represent the diversity of Indonesia's population, are prone to inaccuracies in identifying individuals from certain ethnic or demographic groups. This bias not only undermines the reliability of FRT but also raises questions about its fairness and inclusivity. In a pluralistic society like Indonesia, where ethnic and cultural diversity is a cornerstone of national identity, such biases can exacerbate social inequalities and erode public trust in the technology.

The potential misuse of FRT for mass surveillance also emerged as a significant concern. While the technology's application in public safety is justified, the lack of transparency and accountability in its deployment raises fears of authoritarian practices. Without clear guidelines on its usage, FRT could be weaponized for purposes such as political surveillance or the suppression of dissent, undermining democratic values and human rights. These concerns are compounded by the limited public awareness about the ethical implications of FRT, which prevents meaningful societal engagement in discussions about its deployment.

The findings further highlight the regulatory gaps in Indonesia's approach to FRT. While there are some policies addressing digital technologies, they are often fragmented and insufficient to address the specific challenges posed by FRT. This lack of a cohesive regulatory framework hampers efforts to ensure the ethical and responsible use of the technology. Moreover, it places an undue burden on individual organizations to develop their own governance mechanisms, leading to inconsistencies and potential exploitation.

Despite these challenges, the study identifies opportunities for addressing these ethical dilemmas through a multi-stakeholder approach. Policymakers, technology developers, and civil society organizations must work collaboratively to establish robust legal and ethical frameworks that prioritize transparency, accountability, and inclusivity. Public education campaigns can play a crucial role in raising awareness about the implications of FRT and empowering individuals to advocate for their rights. Additionally, the development of localized datasets that reflect Indonesia's diversity can mitigate algorithmic bias and improve the reliability of FRT systems.

This discussion underscores the dual nature of FRT as both an enabler of progress and a source of ethical dilemmas. Its potential to drive digital transformation and enhance public services is undeniable, but its deployment must be guided by a strong commitment to ethical principles and human rights. By addressing the identified challenges and fostering a culture of responsible innovation, Indonesia can leverage FRT as a transformative tool while safeguarding the values of privacy, equity, and democracy. These findings contribute to the broader discourse on the responsible implementation of emerging technologies, offering valuable insights for policymakers and stakeholders both within Indonesia and globally.

Discussion:

The Opportunities of Facial Recognition Technology in Indonesia

Facial Recognition Technology (FRT) is emerging as a key enabler of digital transformation across various sectors in Indonesia. Its integration into law enforcement, financial services, and public administration illustrates its capacity to enhance efficiency and address longstanding challenges. In law enforcement, FRT has proven invaluable in improving public safety by enabling faster identification of suspects and missing persons. By utilizing real-time surveillance systems integrated with facial recognition capabilities, law enforcement agencies in Indonesia have been able to enhance crime prevention strategies. The technology's ability to match individuals against criminal databases with high accuracy minimizes manual errors and accelerates investigative processes.

In financial services, FRT is widely utilized for user authentication and fraud prevention, particularly in the growing landscape of digital banking and e-commerce. The adoption of FRT-based Know Your Customer (KYC) processes ensures seamless and secure onboarding of

users, reducing the risks of identity theft and financial fraud. As the digital economy in Indonesia continues to expand, the integration of FRT is becoming indispensable for fostering trust and security in online transactions.

Public administration in Indonesia has also benefited significantly from FRT, particularly in initiatives such as smart city programs. Cities like Jakarta and Surabaya are implementing facial recognition for traffic management, public transportation access, and administrative services. These applications streamline citizen identification, reduce bureaucratic inefficiencies, and improve service delivery, aligning with the government's broader goals of digitalizing public services.

Additionally, FRT holds significant potential for healthcare. The technology can be utilized for patient identification, ensuring accurate medical records and efficient healthcare delivery. This is particularly crucial in rural and underdeveloped areas, where documentation issues often impede access to quality healthcare services.

Despite these promising opportunities, FRT's adoption in Indonesia is still in its nascent stages, with varying levels of integration across sectors. However, as investments in digital infrastructure continue to grow, the potential for FRT to revolutionize the efficiency and effectiveness of public and private services is substantial. Harnessing this potential requires addressing the ethical and regulatory challenges that accompany its deployment.

Figure 1, Face Recognition

Face recognition is one of the AI technologies that is increasingly being utilized across various fields, ranging from security and surveillance to entertainment and customer service management. This technology leverages advanced algorithms to recognize and identify human faces, opening up significant opportunities in many sectors(Dwivedi et al., 2021). The development of face recognition is supported by advancements in machine learning, image processing, and deep learning, enabling computers to recognize faces with high precision. Broadly speaking, face recognition works by capturing facial images, extracting unique features, and comparing them with an existing database of faces.

Comparison Between CNN and GAN in Facial Recognition Technology

- **CNN (Convolutional Neural Networks)**:
  - Primarily used for feature extraction and classification.
  - More structured and deterministic.
  - High accuracy in controlled environments but struggles with variations in lighting, pose, and occlusion.
  - Widely used in commercial facial recognition applications.
- **GAN (Generative Adversarial Networks)**:
  - Used for generating realistic images and enhancing dataset augmentation.
  - Can improve recognition under challenging conditions by creating variations in training data.
  - More robust against adversarial attacks.
  - Used in deepfake technology, posing ethical concerns.

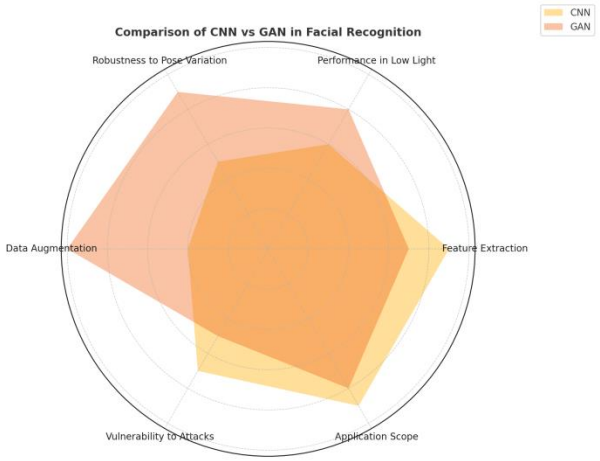

Figure 2, Comparison Between CNN and GAN in Facial Recognition Technology

Explanation of the Radar Chart:

This chart compares **CNN-based** and **GAN-based** facial recognition technologies across six key parameters:

1. **Feature Extraction**: CNN excels in structured feature extraction, while GANs focus on generating realistic synthetic images.
2. **Performance in Low Light**: GANs perform better due to their ability to generate enhanced images.
3. **Robustness to Pose Variation**: GANs are more adaptable as they can generate diverse face angles for training.
4. **Data Augmentation**: GANs outperform CNNs by generating synthetic training data.
5. **Vulnerability to Attacks**: CNN is more structured, making it harder to manipulate, while GANs can be exploited for deepfake-like attacks.
6. **Application Scope**: CNN is dominant in commercial applications, but GANs are advancing in security and media.

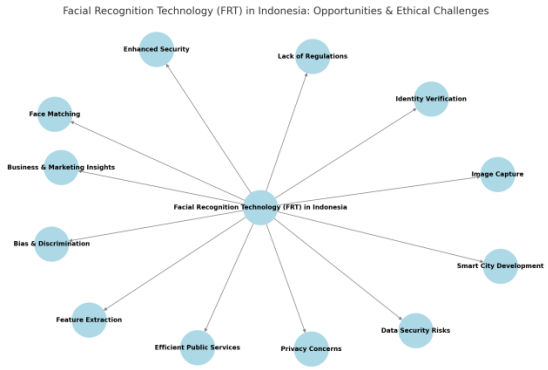

Figure 3, Facial Recognition Technology (FRT) in Indonesia

The diagram illustrates the Facial Recognition Technology (FRT) in Indonesia, focusing on how FRT recognizes faces, its opportunities, and the ethical challenges associated with its implementation.

How FRT Recognizes Faces:

1. Image Capture – The system captures a person's face through surveillance cameras, smartphones, or biometric devices.
2. Feature Extraction – Key facial features such as eyes, nose, and mouth are analyzed and converted into digital data.
3. Face Matching – The extracted data is compared with an existing database of images for identification.
4. Identity Verification – If a match is found, the system confirms the person's identity for security, access control, or other applications.

Opportunities of FRT in Indonesia:

- Enhanced Security – Used for crime prevention, law enforcement, and border control.
- Smart City Development – Integrated into traffic control, surveillance, and urban planning.
- Efficient Public Services – Helps in digital identity verification for banking, healthcare, and government services.
- Business & Marketing Insights – Retailers and marketers use FRT for customer behavior analysis and targeted advertising.

Ethical Challenges of FRT in Indonesia:

- Privacy Concerns – Citizens may not always consent to being monitored, raising data privacy issues.
- Data Security Risks – Risk of biometric data breaches, leading to identity theft and misuse.
- Bias & Discrimination – Some FRT systems may have racial or gender biases, leading to unfair treatment.
- Lack of Regulations – Indonesia still lacks comprehensive laws to regulate FRT usage and data protection.

Privacy Concerns and Data Protection Challenges

One of the most significant ethical challenges of FRT implementation in Indonesia is the issue of privacy. FRT inherently relies on the collection and processing of biometric data, which includes unique and sensitive information about individuals. In Indonesia, the legal framework governing data protection remains underdeveloped, leaving significant gaps in the regulation of biometric data (Wahyuningtyas & Singgalen, 2023). The recently enacted Personal Data Protection Law (PDP Law) is a step forward, but it lacks specific provisions addressing the complexities of FRT, such as consent mechanisms for facial data collection and storage.

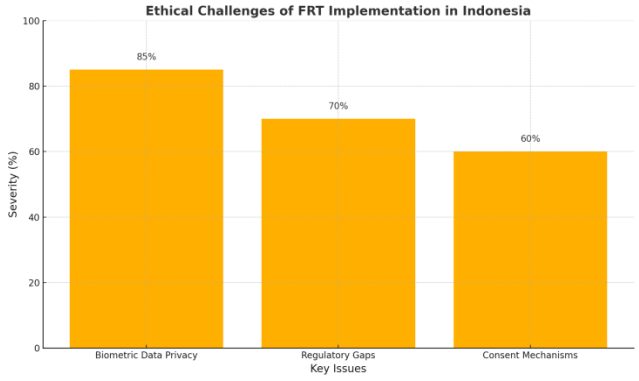

Figure 4, Ethical challenges of FRT implementation in Indonesia

The bar chart above highlights the significant ethical challenges associated with the implementation of Facial Recognition Technology (FRT) in Indonesia(Sitinjak et al., 2023). These challenges revolve around three key areas: biometric data privacy, regulatory gaps, and consent mechanisms. Each of these areas presents critical issues that must be addressed to ensure the ethical deployment of FRT while safeguarding individual rights.

1. Biometric Data Privacy (85%)

Biometric data privacy is the most pressing ethical concern, as reflected by its high severity rating. FRT relies heavily on the collection and processing of sensitive biometric data, such as facial features, which are unique to each individual. Unlike other forms of personal data, biometric data cannot be easily changed or replaced if compromised. This inherent sensitivity makes it particularly vulnerable to misuse, such as unauthorized data sharing, identity theft, or mass surveillance.

In Indonesia, the protection of biometric data is further complicated by the absence of robust data governance practices. Many organizations that collect and store facial data lack the necessary infrastructure and protocols to ensure its security. Data breaches, which have become increasingly common in the country, highlight the vulnerability of such sensitive information. Without adequate safeguards, the widespread adoption of FRT could lead to significant violations of individual privacy.

2. Regulatory Gaps (70%)

Regulatory gaps present another critical challenge. Although Indonesia recently enacted the Personal Data Protection Law (PDP Law), it falls short of addressing the specific complexities of FRT. For example, the law does not provide clear guidelines on how biometric data should be collected, processed, stored, or deleted. This lack of specificity leaves room for inconsistent practices and potential abuses by both public and private entities.

Furthermore, the PDP Law does not adequately define the boundaries of permissible FRT usage, such as its application in surveillance or law enforcement. In the absence of clear legal restrictions, there is a risk of FRT being used for mass surveillance or other purposes that infringe on individual freedoms and democratic principles. The lack of independent oversight mechanisms exacerbates this issue, making it difficult to hold organizations accountable for unethical practices.

3. Consent Mechanisms (60%)

Consent mechanisms are another area where the ethical deployment of FRT in Indonesia faces significant hurdles. In any data-driven technology, obtaining informed consent from individuals is a cornerstone of ethical practice. However, Indonesia's current regulatory framework does not provide clear guidance on how consent should be obtained, managed, or withdrawn in the context of biometric data.

In many cases, individuals are unaware that their facial data is being collected or how it will be used. This lack of transparency undermines their ability to make informed decisions about their personal information. Additionally, there are no standardized protocols for ensuring that consent is meaningful and not coerced. For example, in public spaces where FRT is deployed for surveillance, it is often unclear whether individuals can opt out of having their data collected.

The absence of robust consent mechanisms not only erodes trust in FRT but also raises broader ethical questions about autonomy and control over personal information. Addressing this issue will require the development of detailed policies and practices that prioritize transparency, user empowerment, and accountability.

Broader Implications

These three challenges are interconnected and have broader implications for the ethical and legal landscape of FRT in Indonesia. Without adequate safeguards, the deployment of FRT could lead to widespread violations of privacy, reinforce existing social inequalities, and undermine public trust in technology. Moreover, the unregulated use of FRT could pave the way for authoritarian practices, such as mass surveillance or political monitoring, which threaten democratic values and human rights.

At the same time, addressing these challenges presents an opportunity for Indonesia to position itself as a leader in responsible technology adoption. By strengthening its legal and regulatory frameworks, fostering public awareness, and promoting ethical innovation, the country can harness the benefits of FRT while mitigating its risks. For example, tailored regulations that reflect Indonesia's socio-cultural context can ensure that FRT is deployed in a manner that aligns with national values and priorities.

The Way Forward

To address these challenges, a multi-stakeholder approach is essential. Policymakers, technology developers, and civil society organizations must collaborate to develop comprehensive frameworks that balance innovation with ethical considerations. Public education campaigns can play a crucial role in raising awareness about the implications of FRT and empowering individuals to advocate for their rights. Additionally, regular audits and impact assessments can help ensure that FRT systems are inclusive, transparent, and accountable.

Ultimately, the ethical deployment of FRT in Indonesia will depend on the country’s ability to navigate these challenges effectively. By adopting a proactive and inclusive approach, Indonesia can demonstrate that technology can be a force for good, driving progress while upholding the principles of privacy, equity, and

democracy. The insights gained from addressing these issues can also serve as a valuable model for other countries grappling with the ethical complexities of FRT(Pramudito, 2024).

Public awareness about privacy implications is also low in Indonesia. Many individuals are unaware of how their biometric data is collected, stored, and used. This lack of transparency exacerbates concerns about unauthorized data usage, including surveillance or third-party sharing of facial data. Without robust mechanisms to ensure informed consent and data ownership, individuals remain vulnerable to privacy breaches and misuse of their personal information.

The risk of data breaches is another critical concern. Indonesia has experienced several high-profile cases of data leaks in recent years, raising questions about the country's cybersecurity infrastructure. The collection of facial data by both public and private entities introduces additional vulnerabilities, as breaches of such sensitive data can have far-reaching consequences, including identity theft and unauthorized surveillance.

Moreover, questions arise regarding the storage and retention of facial data. The lack of clarity on how long data can be retained and the purposes for which it can be used creates opportunities for misuse. For instance, if facial data is stored indefinitely, it could be repurposed for activities beyond the scope of the original consent, violating individual privacy rights.

The intersection of FRT and privacy concerns also raises broader ethical questions about the balance between public safety and individual freedoms. While FRT is justified in certain contexts, such as criminal investigations, its unregulated use for surveillance undermines the principles of privacy and autonomy. Addressing these issues requires a comprehensive review of Indonesia's legal framework to ensure that privacy rights are protected without compromising technological innovation.

Algorithmic Bias and Its Implications for Social Equity

Algorithmic bias is a critical issue in FRT, particularly in a diverse country like Indonesia. FRT systems are often trained on datasets that do not adequately represent the ethnic, cultural, and demographic diversity of Indonesia's population. As a result, the technology is prone to inaccuracies, disproportionately affecting certain groups, such as ethnic minorities or individuals with non-standard facial features.

This bias undermines the reliability and fairness of FRT systems, particularly in high-stakes applications such as law enforcement. For example, misidentifications due to algorithmic bias can lead to wrongful arrests, reinforcing systemic inequalities and eroding public trust in the technology. Such outcomes are particularly concerning in Indonesia, where ethnic and social disparities remain a sensitive issue.

The implications of algorithmic bias extend beyond law enforcement. In financial services, biased FRT systems can lead to unequal access to banking or loan approvals, disproportionately excluding individuals from marginalized communities(Pantin, 2023). Similarly, in public administration, biased algorithms can hinder access to essential services for underrepresented groups, perpetuating social inequalities.

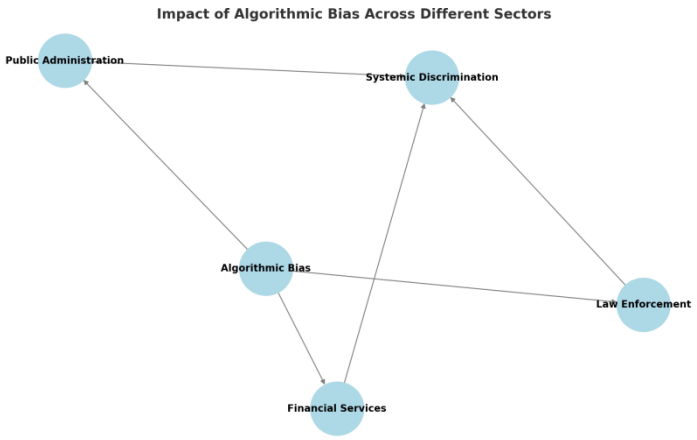

Figure 5, Impact of algorithmic bias across different sectors

The diagram above visually represents the impact of algorithmic bias across different sectors and its broader implications for systemic discrimination and social inequalities(Kordzadeh & Ghasemaghaei, 2022). The relationships between the key elements illustrate how biases embedded in Facial Recognition Technology (FRT) extend beyond law enforcement and influence financial services and public administration, ultimately leading to long-term disparities.

Algorithmic Bias as the Root Cause

At the core of the issue is algorithmic bias, which arises when facial recognition systems are trained on datasets that lack adequate representation of diverse demographic groups. This bias can manifest in various ways, including higher error rates for individuals from marginalized communities, leading to incorrect identifications and discriminatory outcomes. The consequences of algorithmic bias differ across sectors, but they share a common theme exclusion and systemic inequality.

Impact on Law Enforcement

One of the most widely discussed consequences of algorithmic bias is its effect on law enforcement. Biased facial recognition systems have been shown to misidentify individuals from racial and ethnic minorities at disproportionately high rates, leading to wrongful arrests and surveillance injustices. When law enforcement agencies rely heavily on flawed FRT, innocent individuals are more likely to be falsely accused or monitored unfairly. This contributes to racial profiling, distrust in policing, and over-policing of specific communities, deepening the divide between law enforcement and the public(Pramudito & Fatchan, 2025).

Furthermore, automated surveillance systems powered by biased algorithms reinforce existing prejudices within the criminal justice system. If historical data used to train FRT systems reflects past discriminatory policing practices, the bias becomes self-perpetuating, increasing the likelihood of marginalized groups being overrepresented in law enforcement databases.

Impact on Financial Services

Algorithmic bias in financial services is another growing concern. Many financial institutions have adopted AI-driven FRT systems for identity verification, loan approvals, and fraud prevention. However, biased algorithms can disproportionately exclude individuals from marginalized communities from accessing critical financial services. This occurs when facial recognition systems fail to recognize individuals accurately, leading to higher rejection rates for identity verification and loan approvals.

One of the most problematic aspects of this bias is its reinforcement of economic disparities. If individuals from underrepresented groups are systematically denied banking services or loans due to biased FRT, they are denied opportunities for financial stability and wealth accumulation. Moreover, AI models trained on historical loan approval data may inherit biases from past financial exclusion patterns, further exacerbating economic inequalities. As a result, access to credit, housing, and business opportunities becomes more restricted for marginalized groups, perpetuating financial insecurity.

Impact on Public Administration

Public administration is increasingly reliant on AI and facial recognition technology for various services, including social welfare programs, voter registration, and public assistance verification. However, biased algorithms can create significant barriers to accessing essential government services. When individuals from underrepresented groups struggle to authenticate their identities due to algorithmic inaccuracies, they may be wrongfully denied benefits such as healthcare, unemployment support, or housing assistance.

Moreover, biased FRT in voter registration systems can lead to voter disenfranchisement, disproportionately affecting minority communities. Errors in facial recognition databases might prevent individuals from casting their votes, leading to concerns about democratic fairness and representation. Similarly, digital government platforms that depend on facial recognition for security may inadvertently exclude those who do not fit the algorithm's trained dataset, leading to a digital divide that disproportionately affects already marginalized populations.

Systemic Discrimination and Social Inequality

As demonstrated in the diagram, the cumulative effect of algorithmic bias in these sectors leads to long-term systemic discrimination. Individuals affected by bias in law enforcement, financial services, or public administration experience reduced access to opportunities, economic hardship, and social exclusion. Over time, this exacerbates existing inequalities and entrenches cycles of disadvantage that are difficult to break.

The reinforcement of these biases on a structural level creates a feedback loop, where marginalized communities continue to face barriers in multiple aspects of life. These systemic issues are not merely technical challenges but ethical and social concerns that require urgent intervention from policymakers, technology developers, and civil rights advocates.

Addressing Algorithmic Bias

To mitigate these issues, several actions must be taken:

1. Diverse and Representative Training Data – AI models should be trained on datasets that accurately represent all demographic groups to reduce bias.
2. Transparent AI Auditing – Governments and organizations must establish independent auditing mechanisms to assess and correct bias in AI-driven FRT systems.
3. Stronger Regulations – Laws must be updated to prevent discrimination in AI-powered decision-making processes, particularly in high-stakes areas such as law enforcement, finance, and public services.
4. Human Oversight – AI-driven decisions should always involve human review processes to prevent unfair or erroneous outcomes.
5. Public Awareness and Advocacy – The public must be educated about the risks of biased FRT, empowering communities to demand accountability and fairness.

Addressing algorithmic bias requires the development of localized datasets that reflect Indonesia's demographic diversity. Collaborative efforts between government agencies, technology developers, and academic institutions are essential to ensure that FRT systems are inclusive and fair. Additionally, transparency in algorithm design and regular audits can help mitigate biases and improve the accuracy and reliability of FRT.

Mass Surveillance and the Threat to Democratic Values

The potential misuse of FRT for mass surveillance is one of the most controversial aspects of its adoption. While FRT can enhance public safety, its unregulated use for monitoring citizens poses significant risks to democratic values and human rights. In Indonesia, concerns about surveillance have grown as FRT is increasingly integrated into public spaces, such as transportation hubs, government offices, and urban centers.

The lack of transparency and accountability in how FRT is deployed exacerbates fears of misuse. Without clear guidelines on the scope and purpose of surveillance, there is a risk of the technology being weaponized for political purposes, such as monitoring activists, journalists, or opposition groups. Such practices undermine freedom of expression and the right to dissent, which are

fundamental to Indonesia's democratic framework.

Table 1. Potential Misuse of Facial Recognition Technology (FRT) for Mass Surveillance in Indonesia

Aspect	Description
Enhanced Public Safety	FRT can improve security by identifying criminals, preventing crimes, and ensuring safer public spaces.
Mass Surveillance Risks	Unregulated FRT deployment raises concerns about excessive citizen monitoring, infringing on privacy rights.
Democratic Threats	The use of FRT for monitoring activists, journalists, and opposition groups threatens freedom of expression.
Lack of Transparency	The absence of clear policies on how FRT data is collected, stored, and used increases fears of government abuse.
Legal and Ethical Gaps	Weak legal frameworks fail to regulate FRT usage, allowing unchecked mass surveillance practices.
Public Space Deployment	FRT is widely integrated into transportation hubs, government buildings, and urban areas, intensifying concerns.
Chilling Effect	Fear of constant surveillance may deter people from engaging in activism, protests, or expressing political views.
Need for Regulation	Robust laws and oversight mechanisms are required to ensure ethical and accountable FRT deployment.

This table highlights the dual nature of FRT deployment in Indonesia, where the technology can enhance public safety but also pose significant threats to democracy and human rights (Yilmaz et al., 2022). The lack of transparency in FRT implementation and the absence of clear legal safeguards create risks of misuse for political and authoritarian purposes. Without proper regulations, mass surveillance may erode civil liberties, discourage political dissent, and contribute to a chilling effect in society. Therefore, a balanced approach that promotes security while protecting democratic values and individual freedoms is essential to ensure the ethical use of FRT in Indonesia (Acharya, 2014).

Public trust in FRT is further eroded by the absence of oversight mechanisms. In Indonesia, the lack of independent regulatory bodies to monitor the use of surveillance technologies creates opportunities for abuse. The potential for FRT to be used for blanket surveillance, rather than targeted interventions, raises ethical questions about proportionality and necessity.
To address these concerns, Indonesia must establish robust regulatory frameworks that define the permissible use of FRT in public spaces. Transparency in surveillance practices, combined with independent oversight, can help restore public trust while ensuring that the technology is used responsibly and ethically.

4. CONCLUSION

Facial Recognition Technology (FRT) in Indonesia offers transformative opportunities in security, financial services, and public administration by enhancing efficiency, authentication accuracy, and crime prevention. However, its rapid adoption also introduces significant ethical challenges, including concerns over privacy violations, algorithmic bias, and the risk of mass surveillance without proper oversight. The absence of a comprehensive legal framework further exacerbates these issues, creating vulnerabilities in data protection and fairness in AI-driven decision-making. While advancements in FRT can contribute to Indonesia's digital transformation, its implementation must be

guided by transparent policies, ethical safeguards, and public accountability to ensure that it serves societal interests without undermining fundamental rights. Addressing these challenges through regulatory measures and inclusive AI development will be crucial in balancing technological innovation with ethical considerations.

5. REFERENCES

Acharya, A. (2014). Indonesia matters: Asia's emerging democratic power (Vol. 1). World Scientific.

Ardiansyah, F., Marthen, A. A., & Amalia, N. (2015). Forest and land-use governance in a decentralized Indonesia: A legal and policy review.

Bilal, M., Hakkala, A., & Isoaho, J. (2020). Utilitarian Analysis of Mass Surveillance: Panopticons and Privacy.

Citron, D. K., & Solove, D. J. (2022). Privacy harms. BUL Rev., 102, 793.

Dwivedi, Y. K., Hughes, L., Ismagilova, E., Aarts, G., Coombs, C., Crick, T., Duan, Y., Dwivedi, R., Edwards, J., & Eirug, A. (2021). Artificial Intelligence (AI): Multidisciplinary perspectives on emerging challenges, opportunities, and agenda for research, practice and policy. International Journal of Information Management, 57, 101994.

Gomber, P., Kauffman, R. J., Parker, C., & Weber, B. W. (2018). On the fintech revolution: Interpreting the forces of innovation, disruption, and transformation in financial services. Journal of Management Information Systems, 35(1), 220–265.

Kordzadeh, N., & Ghasemaghaei, M. (2022). Algorithmic bias: review, synthesis, and future research directions. European Journal of Information Systems, 31(3), 388–409.

Krishnan, R., Perumal, E., Govindaraj, M., & Kandasamy, L. (2024). Enhancing Logistics Operations Through Technological Advancements for Superior Service Efficiency. In Innovative Technologies for Increasing Service Productivity (pp. 61–82). IGI Global.

Lastikova, M. (2023). Context-Specific Peace Education Initiatives within local communities in Western Cape, South Africa: Lessons from Ubuntu.

Latonero, M., & Kift, P. (2018). On digital passages and borders: Refugees and the new infrastructure for movement and control. Social Media+ Society, 4(1), 2056305118764432.

Mosa, M. J., Barhoom, A. M., Alhabbash, M. I., Harara, F. E. S., Abu-Nasser, B. S., & Abu-Naser, S. S. (2024). AI and Ethics in Surveillance: Balancing Security and Privacy in a Digital World.

Pantin, L. P. (2023). Financial Inclusion, Cryptocurrency, and Afrofuturism. Nw. UL Rev., 118, 621.

Pramudito, D. K. (2024). Enhancing Real-Time Object Detection in Autonomous Systems Using Deep Learning and Computer Vision Techniques. The Journal of Academic Science, 1(6), 788–804.

Pramudito, D. K., & Fatchan, M. (2025). Optimizing Image Recognition in Low-Light Environments through Advanced Computer Vision Algorithms. The Journal of Academic Science, 2(1), 278–289.

Pribadi, K. S., Abduh, M., Wirahadikusumah, R. D., Hanifa, N. R., Irsyam, M., Kusumaningrum, P., & Puri, E. (2021). Learning from past earthquake disasters: The need for knowledge management system to enhance infrastructure resilience in Indonesia. International Journal of Disaster Risk Reduction, 64, 102424.

Radyati, M. R. N., & Tjahjono, B. (2021). the

new social economy in Indonesia: Features, Recent Development and Challenges. In The New Social and Impact Economy: An International Perspective (pp. 73–94). Springer.

Rosenbloom, D. H., Kravchuk, R. S., & Clerkin, R. M. (2022). Public administration: Understanding management, politics, and law in the public sector. Routledge.

Sitinjak, C., Tahir, Z., Toriman, M. E., Lyndon, N., Simic, V., Musselwhite, C., Simanullang, W. F., & Hamzah, F. M. (2023). Assessing public acceptance of autonomous vehicles for smart and sustainable public transportation in urban areas: a case study of Jakarta, Indonesia. Sustainability, 15(9), 7445.

Testriono, F. (2022). Persistence of Power and Subnational Democratic Performance: The Case of indonesia.

Wahyuningtyas, S. Y., & Singgalen, Y. A. (2023). Mapping Stakeholder Perceptions: Navigating Biometric Data Protection Initiative and Face Recognition Technology Support in Indonesia.

West, J., & Bogers, M. (2014). Leveraging external sources of innovation: A review of research on open innovation. Journal of Product Innovation Management, 31(4), 814–831.

Yilmaz, I., Saleem, R. M. A., Pargoo, M., Shukri, S., Ismail, I., & Shakil, K. (2022). Religious populism, cyberspace and digital authoritarianism in Asia: India, Indonesia, Malaysia, Pakistan, and Turkey.