Volume 2 Issue 2 (2025) 91-106
E-ISSN 2988-6740| © Authors. CC BY-SA
https://doi.org/10.59261/iclr.v2i2.34
https://iclr.polteksci.ac.id/

Indonesian Cyber Law Review

Legal Compliance And Regulatory Challenges To The Use Of AI Algorithms In Facial Recognition Systems In The Public Sector

Anom Sutrisno
Universitas Swadaya Gunung Jati Cirebon, Indonesia
Corresponding Author : anom_sutrisno@ugj.ac.id

ABSTRACT

This study aims to analyze the level of legal compliance and regulatory challenges in the use of artificial intelligence algorithms in facial recognition systems in the Indonesian public sector. The study focuses on the clarity of the legal basis, biometric data protection, the risks of discrimination and algorithmic bias, and the weakness of transparency, oversight, and accountability mechanisms. The study uses a normative juridical method with a legislative, conceptual, and comparative legal approach. Data were obtained through a literature review of primary, secondary, and tertiary legal materials, including national regulations, international regulations such as the GDPR and the EU Artificial Intelligence Act, and current legal literature. The results show that although there are general regulations regarding personal data protection and human rights, there is no specific legal framework that explicitly and operationally regulates the use of facial recognition by state institutions. This condition has implications for low legal certainty, potential violations of privacy rights, and an increased risk of algorithmic discrimination. This study concludes that the establishment of specific regulations based on the principles of the rule of law and AI governance is necessary to ensure the legal, proportional, and accountable use of facial recognition technology in the public sector.

Keywords: facial recognition, artificial intelligence, legal compliance, biometric data protection, public sector

Article received on 20-07-2025 — Final revised on 11-11-2025 — Approved on 11-12-2025

Introduction

The development of artificial intelligence (AI) technology has brought fundamental changes to governance and public sector operations. One of the most significant applications of AI is the use of facial recognition systems, which utilize biometric data to identify and verify individual identities. This technology has been widely used in various countries in the context of law enforcement, public security control, immigration management, population administration services, and public space surveillance. A report by the European Union

Agency for Fundamental Rights (FRA) shows that more than 60% of EU member states have tested or used facial recognition technology in some form in the public sector, primarily by security forces and police (Capasso et al., 2023).

From a legal perspective, the use of facial recognition systems by states raises serious issues because this technology works by processing biometric data, which is categorized as sensitive personal data under international and regional law. Article 9 of the General Data Protection Regulation (GDPR) explicitly states that biometric data is a special category of personal data that can only be processed under very limited circumstances. Legal literature confirms that the use of biometric data by public institutions has the potential to directly impact privacy rights, civil liberties, and protection against abuse of state power, thus requiring stricter legal compliance standards than conventional information technology (Elmi, 2025).

Furthermore, the complex, adaptive, and often opaque (black-box) nature of AI algorithms increases the legal challenges in ensuring state accountability and responsibility. Legal studies published in the Harvard Journal of Law & Technology and the Computer Law & Security Review show that algorithm-based decisions are difficult to legally test due to the lack of transparency in the decision-making logic. This situation potentially contradicts the principle of the rule of law, which demands legal certainty, predictability, and a corrective mechanism for every government action (Gültekin-Várkonyi, 2024).

The specific legal issues that are the focus of this research are legal compliance and regulatory challenges in the use of AI algorithms in facial recognition systems in the public sector. These issues include: (1) clarity of the legal basis for the use of facial recognition by state institutions; (2) protection of biometric data as part of the right to privacy and the right to personal data; (3) the risk of discrimination and algorithmic bias in the identification process; and (4) weak mechanisms for transparency, oversight, and legal accountability. Several academic reports and court decisions in Europe and the United States indicate that the use of facial recognition without a clear legal framework often results in human rights violations and lawsuits against the state.

International legal literature consistently positions facial recognition technology as a high-risk technology. An article by Garvie, Bedoya, and Frankle, published in the Georgetown Law Center on Privacy & Technology, shows that the error rate of facial recognition systems used by police in the United States can reach 28% among certain racial groups. This research is frequently cited in legal journals as empirical evidence that the use of facial recognition has the potential to violate the principles of non-discrimination and equality before the law (Rangari, 2025).

At the regulatory level, the European Journal of Risk Regulation and International Data Privacy Law note that the European Union responds to these risks through a risk-based regulatory approach, which requires algorithmic impact assessments, audits of AI systems, and human oversight mechanisms. In contrast, many developing countries lack specific AI regulations and rely on general data protection or electronic systems laws. The legal literature describes this as a regulatory gap that has the potential to weaken the protection of citizens' rights in the context of AI use by the public sector (H Patel & Gera, 2024).

Previous research has extensively examined the use of facial recognition systems from the perspective of data protection law and privacy rights. For example, Edwards and Veale's study in Computer Law & Security Review (2018) examined automated decision-making and its implications for individual rights under the GDPR. Another study by Wachter, Mittelstadt, and Floridi in International Data Privacy Law focused on the limitations of the right to explanation in the context of AI algorithms. Furthermore, several

normative legal studies have examined facial recognition as an instrument of state surveillance and its threats to civil liberties in democratic societies (Kurniawan & Kurniawan, 2025).

While these studies are important, there is a significant research gap. Most studies still focus on developed country jurisdictions and address facial recognition issues only partially, from the perspective of data protection, algorithmic bias, and AI ethics. Research that comprehensively examines legal compliance and regulatory challenges in the use of AI algorithms in the public sector, particularly using the rule of law and AI governance approaches, is still relatively limited. Furthermore, studies that integrate national regulatory analysis with developments in international law are also scarce, providing a suitable opportunity for this research (Stepanov & Basangov, 2025).

This research employs a normative juridical approach grounded in the rule of law theory, which asserts that every state action must have a clear, proportional, and legally testable legal basis. This theory is used to assess the legitimacy of the use of facial recognition by the public sector within the applicable legal framework (Prasad Adhhikari, 2025).

Furthermore, this research adopts a human rights-based approach, which places the right to privacy, personal data protection, and the principle of non-discrimination as the primary parameters of analysis. This approach is widely used in international law journals to assess surveillance technology and the state's obligations to protect fundamental rights (Amaka Justina Obinna & Azeez Jason Kess-Momoh, 2024).

This research also utilizes the theories of AI governance and algorithmic accountability, which are emerging in technology law and policy studies. This approach emphasizes the importance of algorithm transparency, independent audits, and the legal responsibility of public institutions as users of AI, making it relevant to analyzing the regulatory challenges of facial recognition in the public sector (Tshipota et al., 2025).

This research aims to analyze the level of legal compliance and identify regulatory challenges in the use of AI algorithms in facial recognition systems in the public sector. Theoretically, this research is expected to enrich the study of technology law and AI governance. Practically, this research is expected to provide legal policy recommendations for lawmakers and public institutions to ensure the use of facial recognition is legal, transparent, accountable, and in line with human rights protections (Malladhi, 2023).

Research Method

This research is a normative legal research (doctrinal legal research), focusing on positive legal norms, legal principles, and applicable legal doctrines related to the use of artificial intelligence algorithms in facial recognition systems in the public sector. This approach is used because the object of the study does not examine empirical public behavior, but rather analyzes the suitability of the use of facial recognition technology with the legal framework, the principles of the rule of law, and the protection of human rights (Rezende, 2020).

This research adopts a comprehensive legal approach by combining several analytical methods. A legislative approach is used to systematically examine various regulations related to the use of facial recognition systems, including provisions on personal data protection, human rights, and the governance of electronic systems in the public sector, to assess the extent to which these practices comply with applicable legal norms. Furthermore, a conceptual approach is applied to examine and interpret several key concepts in technology law, such as legal compliance, data protection, algorithmic

accountability, the characterization of high-risk artificial intelligence, and the importance of human oversight, as widely discussed in international legal literature and journals. This research also uses a comparative legal approach by comparing national regulatory frameworks related to facial recognition with international legal regimes, particularly the General Data Protection Regulation (GDPR) and the European Union Artificial Intelligence Act, which are widely recognized in academic studies as references for best practices in regulating the use of facial recognition technology in the public sector (Chalakov et al., 2025).

This research relies on secondary data as the primary source of analysis. This data includes primary legal materials in the form of laws and regulations governing personal data protection and human rights, relevant international regulations such as the General Data Protection Regulation (GDPR) and the European Union Artificial Intelligence Act, as well as court decisions and official reports related to the implementation of facial recognition technology by public sector institutions. Furthermore, this research also utilizes secondary legal materials obtained from scholarly articles published in reputable legal journals, including Computer Law & Security Review, International Data Privacy Law, Harvard Journal of Law & Technology, and European Journal of Risk Regulation, as well as books and academic reports specifically discussing artificial intelligence governance, the use of facial recognition systems, and human rights protection. To complement and clarify understanding of the legal terms and concepts used, tertiary legal materials such as legal encyclopedias, legal dictionaries, and other supporting documents are also used as references in this research (Frimpong, 2025).

Data collection in this study was conducted through library research, exploring and reviewing various relevant written sources. The steps taken included an inventory of legal provisions, both at the national and international levels, that regulate the use of artificial intelligence, facial recognition technology, and biometric data protection. Furthermore, this study examined scientific articles published in reputable law journals that specifically discuss the application of facial recognition in the public sector. To enrich the analysis, a review of academic reports and policy papers frequently used as references in legal studies related to artificial intelligence was also conducted (Della Giustina & De Gioia Carabellese, 2024).

The obtained materials and data were analyzed using a qualitative, normative approach, carried out in a systematic manner. The analysis began with grouping legal materials based on key issues related to compliance with legal provisions, data protection, and various regulatory challenges arising from the use of facial recognition technology. The next stage was legal interpretation to understand and explain the application of applicable legal norms to the use of artificial intelligence algorithms in the system. A normative evaluation was then conducted by comparing the practice of facial recognition in the public sector with the principles of the rule of law, human rights protection, and responsible artificial intelligence governance. The analysis process concluded with the formulation of prescriptive conclusions, in the form of legal recommendations and regulatory directions needed to strengthen compliance and legal protection in the application of this technology (Hennocq et al., 2024).

To ensure the validity and validity of the data, this study implemented several testing steps relevant to the nature of normative legal research. One such step was source triangulation, which involved comparing statutory provisions, legal journal articles, and academic reports to ensure the consistency and accuracy of the analysis. Furthermore, this study prioritized the authority of the sources by selecting references from reputable legal

journals and official regulations with academic and legal authority and recognition. The validity of the analysis was also maintained through normative consistency, ensuring that the legal interpretations and arguments used remained in line with legal principles and principles recognized in doctrine and jurisprudence (Velinova et al., 2025).

Result and Discussion

Table 1. Clarity of the Legal Basis for the Use of Facial Recognition by State Institutions

No	Legal Approach	Legal Basis Analyzed	Research Findings
1	Statute Approach	1945 Constitution, Personal Data Protection Law, Human Rights Law, ITE Law	There is no explicit legal basis that clearly grants authority to state institutions to use facial recognition systems
2	Conceptual Approach	Principle of legality, rule of law, legal compliance	The use of facial recognition by the state has not yet fulfilled the principles of legal certainty and limitation of power
3	Comparative Approach	GDPR and the EU Artificial Intelligence Act	International standards require a specific legal basis that has not yet been equivalently adopted in national law

Based on an inventory and analysis of the 1945 Constitution of the Republic of Indonesia, specifically Article 28G paragraph (1) concerning personal protection, and Article 28H paragraph (4) concerning the right to legal certainty and protection of private property rights, the study found that the constitution provides general protection for citizens' privacy rights. However, this protection has not been specifically enshrined in sectoral regulations regarding the use of facial recognition technology by state institutions.

Furthermore, the Personal Data Protection Law (Law No. 27 of 2022) does classify biometric data as specific personal data, but it does not regulate in detail the use of facial recognition technology by government agencies, particularly regarding the basis of authority, purpose limitations, and oversight mechanisms. Similarly, Law No. 39 of 1999 concerning Human Rights and Law No. 11 of 2008 in conjunction with Law No. 19 of 2016 concerning Electronic Information and Transactions (ITE) only regulate the protection of rights and electronic systems in general. These findings indicate that, normatively, there is no explicit legal basis that firmly and specifically legitimizes the use of facial recognition by state institutions.

Through a conceptual analysis referring to legal literature from the Computer Law & Security Review and the Harvard Journal of Law & Technology, the study found that facial recognition is categorized as a form of high-risk AI because it involves processing biometric data and has direct implications for privacy rights and civil liberties. Under the principle of legality, any state action that restricts citizens' rights must be based on clear, written, and foreseeable law.

However, the use of facial recognition by state institutions based solely on administrative discretion or internal policies fails to meet the principles of legal compliance, algorithmic accountability, and human oversight. Conceptually, this practice has the potential to violate the rule of law, as it expands state authority without clear normative limitations. These findings confirm that, from a legal theory perspective, the legitimacy of state use of facial recognition remains problematic.

Based on a comparative study of the General Data Protection Regulation (GDPR), specifically Article 9, the study found that biometric data for identification purposes is treated as a special category of personal data, which, in principle, is prohibited from being

processed except on a specific legal basis. Furthermore, the EU Artificial Intelligence Act explicitly classifies real-time remote biometric identification in public spaces as a highly restricted practice and is generally prohibited, except for certain interests specifically regulated by law.

Compared to national legal frameworks, there are no laws or statutory regulations that explicitly regulate facial recognition as a high-risk AI technology. This finding indicates a significant gap between international regulatory standards and national laws regarding the clarity of the legal basis and restrictions on the use of facial recognition technology by state institutions.

Table 2. Biometric Data Protection as Part of the Right to Privacy and the Right to Personal Data

No	Legal Approach	Legal Basis Analyzed	Research Findings
1	Statute Approach	1945 Constitution; Law No. 27 of 2022 on Personal Data Protection; Law No. 39 of 1999 on Human Rights; ITE Law	Biometric data are recognized as sensitive data, but there are no specific operational regulations governing facial recognition in the public sector
2	Conceptual Approach	Privacy rights doctrine, data protection, and high-risk AI	Facial biometric data require enhanced protection standards due to their permanent nature and high risk of misuse
3	Comparative Approach	GDPR and the EU Artificial Intelligence Act	International standards provide significantly stricter protection for biometric data compared to the national legal framework

Based on an examination of Article 28G paragraph (1) of the 1945 Constitution, the state is obliged to protect citizens' right to security and personal protection, which doctrinally includes the right to privacy. This protection is reinforced by Law No. 39 of 1999 concerning Human Rights, which recognizes the right of every person to protect their personal and private life. Furthermore, Law No. 27 of 2022 concerning Personal Data Protection (PDP Law) explicitly classifies biometric data as specific personal data, thus requiring stricter legal protection.

However, the results of the regulatory inventory indicate that although biometric data has been recognized as sensitive data, there are no provisions specifically governing the processing of biometric data through facial recognition technology in the public sector. No norms were found that detailedly regulate the legal requirements for processing, limitations on purposes, retention periods, or mandatory deletion of facial recognition data. These findings indicate that biometric data protection in the context of facial recognition remains a general normative matter and is not yet operational.

Through a conceptual review referring to legal literature from the International Data Privacy Law and the Computer Law & Security Review, the study found that facial biometric data is immutable and permanently linked to an individual's identity. Because of this nature, biometric data leaks or misuse cannot be recovered like other types of personal data. In the context of the use of AI algorithms, biometric data is not only used for identification but also has the potential for profiling, mass surveillance, and the creation of covert population databases.

Conceptually, the use of facial recognition by state institutions must comply with the principles of legal compliance, data minimization, purpose limitation, and human oversight.

However, practices based solely on general regulations and internal administrative policies do not reflect adequate algorithmic accountability. These findings emphasize that biometric data protection cannot be treated the same as regular personal data and require a stricter and more specific legal framework.

Based on a comparative study with the General Data Protection Regulation (GDPR), specifically Article 9, biometric data for identification purposes is categorized as a special category of personal data, which is, in principle, prohibited from being processed, except under very limited exceptions expressly regulated by law. Furthermore, the EU Artificial Intelligence Act classifies facial recognition systems as high-risk AI, even prohibiting the use of real-time remote biometric identification in public spaces in general, except for very specific and proportionate legal interests.

Compared to national legal frameworks, there are no regulations that explicitly designate facial recognition as a high-risk technology or impose strict prohibitions and restrictions on the processing of biometric data by the state. This gap indicates that national laws still lag behind in providing a level of protection equivalent to international standards for the right to privacy and personal data.

Table 3. Risks of Discrimination and Algorithmic Bias in Facial Recognition Identification Processes

No	Legal Approach	Legal Basis Analyzed	Research Findings
1	Statute Approach	1945 Constitution; Human Rights Law; Personal Data Protection Law; ITE Law	National regulations do not specifically address the prevention of algorithmic bias and discrimination in facial recognition systems
2	Conceptual Approach	Non-discrimination principle, algorithmic accountability, high-risk AI	Facial recognition systems pose a risk of generating systemic bias that conflicts with principles of equality and justice
3	Comparative Approach	GDPR and the EU Artificial Intelligence Act	International regulations explicitly acknowledge and impose limits on algorithmic discrimination risks

Based on a review of Article 28I paragraph (2) of the 1945 Constitution of the Republic of Indonesia, the state is obliged to guarantee that every person is free from discriminatory treatment on any basis. This principle is reinforced in Law No. 39 of 1999 concerning Human Rights, which expressly prohibits all forms of discrimination in treatment by the state. However, the inventory results indicate that this provision remains general and does not specifically address the potential for discrimination arising from algorithmic systems.

Furthermore, Law No. 27 of 2022 concerning Personal Data Protection emphasizes the principles of fairness, transparency, and accuracy of data processing, but does not explicitly regulate the obligation to control algorithmic bias in AI systems. Similarly, the ITE Law and regulations on the implementation of electronic systems do not yet contain technical standards or legal obligations for state institutions to conduct algorithm audits to prevent discriminatory misidentification. These findings confirm that national law still does not provide an adequate normative basis for controlling the risk of algorithmic bias in the use of facial recognition in the public sector.

According to a literature review by the Harvard Journal of Law & Technology and the Computer Law & Security Review, facial recognition is widely categorized as high-risk AI because its error rate is unevenly distributed. Various academic studies have shown that facial recognition technology tends to have a higher rate of misidentification of certain

groups, such as women, ethnic minorities, and certain ages. This situation raises the risk of algorithmic discrimination, namely discrimination that arises not from the direct intent of policymakers, but rather from the design, training data, and implementation of the algorithm.

Conceptually, the use of AI algorithms by the state must comply with the principles of equality before the law, algorithmic accountability, and human oversight. If facial recognition identification results are used as the basis for public decision-making—such as law enforcement or security surveillance—without adequate human oversight, the state potentially violates the principle of substantive justice. These findings demonstrate that the risk of algorithmic bias is not merely a technical issue, but a serious legal and human rights issue.

Based on a review of the General Data Protection Regulation (GDPR), specifically Articles 5 and 22, the processing of personal data through automated systems must be fair, accurate, and not result in a discriminatory impact on the data subject. The GDPR also provides individuals with the right not to be subject to decisions based solely on automated processing, including profiling. Furthermore, the EU Artificial Intelligence Act explicitly classifies facial recognition as a high-risk AI system and requires bias mitigation, dataset testing, and algorithm documentation.

Furthermore, the AI Act even prohibits the use of real-time remote biometric identification in public spaces if it has the potential to lead to mass discrimination. Compared with national legal frameworks, there are no equivalent legal obligations regarding bias audits, dataset testing, or citizens' rights to challenge facial recognition-based decisions. These findings indicate a significant gap between international standards and national laws in addressing the risks of algorithmic discrimination in the public sector.

Table 4. Weak Transparency, Oversight, and Legal Accountability Mechanisms in the Use of Facial Recognition by State Institutions

No	Legal Approach	Legal Basis Analyzed	Research Findings
1	Statute Approach	1945 Constitution; Human Rights Law; Personal Data Protection Law; ITE Law	There are no explicit regulations governing algorithmic transparency, mandatory AI audits, or independent oversight mechanisms
2	Conceptual Approach	Principles of algorithmic accountability, human oversight, good governance	The use of facial recognition in the public sector risks producing opaque ("black box") decision-making without clear legal accountability
3	Comparative Approach	GDPR and the EU Artificial Intelligence Act	International regulations impose significantly stricter requirements on transparency, auditing, and oversight compared to national law

The results of the inventory of laws and regulations indicate that the principles of accountability and transparency are normatively recognized in the 1945 Constitution of the Republic of Indonesia, specifically Article 28D paragraph (1), which guarantees fair legal certainty, and Article 28F, which guarantees the right to information. This principle is reinforced by Law No. 39 of 1999 concerning Human Rights, which requires the state to act openly and responsibly in restricting citizens' rights.

However, in Law No. 27 of 2022 concerning Personal Data Protection, although data controllers are required to ensure transparency and accuracy of processing, there are no explicit provisions requiring state institutions to disclose the working logic of facial

recognition algorithms, conduct independent audits, or provide a dedicated complaint mechanism for citizens harmed by system errors. The ITE Law and regulations on the implementation of electronic systems also do not regulate algorithmic transparency obligations or legal accountability procedures if AI systems produce erroneous decisions. These findings indicate a lack of norms regarding oversight and accountability mechanisms for the use of facial recognition in the public sector.

Based on a literature review from the Harvard Journal of Law & Technology and the European Journal of Risk Regulation, facial recognition is understood as an AI technology that tends to operate opaquely or in a black box, making it difficult for users and affected communities to understand. In a legal context, this contradicts the principle of algorithmic accountability, which requires that every algorithm-based decision be explainable, monitored, and legally accountable.

The concept of human oversight also emphasizes that the use of AI in the public sector should not completely replace human judgment, especially when it impacts citizens' fundamental rights. However, the findings suggest that without legal obligations governing the involvement of human oversight, facial recognition has the potential to be used as the basis for administrative decisions or law enforcement without effective room for correction. This weak accountability mechanism places citizens in a vulnerable position, as it is difficult to determine who is responsible in the event of misidentification or misuse of the system.

Unlike national legal frameworks, the General Data Protection Regulation (GDPR) explicitly stipulates the principles of transparency, accountability, and explainability in the processing of personal data by automated systems. Articles 13 and 14 of the GDPR require data controllers to provide clear information regarding the logic of algorithmic processing, while Article 22 provides individuals with the right to obtain human intervention and challenge automated decisions.

Furthermore, the EU Artificial Intelligence Act explicitly requires high-risk AI systems, including facial recognition, to undergo ex-ante conformity assessments, regular audits, technical documentation, and oversight by an independent authority. These provisions demonstrate that transparency and accountability are not viewed as policy options, but rather as legal obligations. This comparison confirms that Indonesia still lags behind in developing oversight mechanisms and legal accountability for the use of AI by state institutions.

Clarity of the Legal Basis for the Use of Facial Recognition by State Institutions

A clear legal basis is a fundamental prerequisite for the use of facial recognition technology by state institutions, especially when the technology operates in the realm of restricting human rights and collecting citizens' biometric data. Based on research findings, the use of facial recognition systems in the Indonesian public sector remains within a general regulatory framework, without a legal mandate specifically regulating the purpose, limitations, and conditions of use of such technology. From a rule of law perspective, this condition raises issues of legitimacy, because any state action that has the potential to restrict citizens' constitutional rights must have a clear, accessible, and predictable legal basis (legal certainty).

Several previous studies have emphasized that the absence of an explicit legal basis for the use of facial recognition has the potential to lead to the practice of function creep, namely the expansion of the use of technology beyond its original purpose (Veale, M., & Edwards, 2018). An empirical study conducted by (Garvie, C., Bedoya, A., & Frankle, 2016) in the United States showed that police officers used facial recognition without a transparent

legal framework, thus triggering privacy violations and unaccountable mass surveillance. This finding is conceptually relevant to the Indonesian context, as it shows that the absence of a specific legal basis opens up excessive discretion for state institutions in determining when and how this technology is used.

When linked to the principle of legal compliance, Indonesian national regulations—despite recognizing the right to privacy and personal data protection—have not explicitly classified facial recognition as a high-risk technology (high-risk AI) requiring special regulation. However, technology law literature confirms that AI systems used for biometric identification in public spaces are highly intrusive and require stricter legal legitimacy than information technology in general (Binns, 2020). Without a specific legal basis, the use of facial recognition has the potential to violate the principles of legality and the principle of limiting state power.

A comparative legal approach reinforces these findings. The GDPR explicitly classifies biometric data as a special category of data whose processing is prohibited unless based on a clear and proportionate legal basis (Article 9 GDPR). Furthermore, the EU Artificial Intelligence Act normatively positions facial recognition for remote biometric identification in public spaces as a practice that is prohibited in principle, except in very limited situations with a specific legal basis, judicial oversight, and a strict necessity-proportionality principle. Research by (Lynskey, 2019) confirms that a clear legal basis is not merely an administrative issue, but a mechanism for protecting human rights against state surveillance technology.

Thus, this discussion demonstrates that the primary challenge in the Indonesian context is not simply weak technical regulations, but rather the absence of a substantive legal basis that explicitly grants, limits, and oversees state authority in the use of facial recognition. This situation has implications for low legal compliance, as state institutions operate high-risk technology without adequate normative legitimacy. Therefore, prescriptively, this study emphasizes the need for specific regulations or sectoral arrangements that explicitly govern facial recognition in the public sector, with reference to human rights principles, the rule of law, and international AI governance standards.

Biometric Data Protection as Part of the Right to Privacy and the Right to Personal Data

Biometric data protection occupies a central position in the legal discourse surrounding the use of AI algorithms in facial recognition systems in the public sector, given the unique, permanent, and unchangeable nature of biometric data. Unlike other types of personal data, the leakage or misuse of biometric data has long-term implications for individuals, making it doctrinally viewed as a core element of the right to privacy and the right to personal data protection. Research findings indicate that although national legal frameworks recognize biometric data as sensitive data, there are still inadequate regulations regarding protection standards and limitations on the processing of biometric data in the context of facial recognition by state institutions.

This finding aligns with previous research suggesting that normative recognition of biometric data does not necessarily guarantee effective protection without strict operational regulations. (Kuner, C., Bygrave, L. A., Docksey, C., & Drechsler, 2017) emphasize that modern personal data protection must incorporate the principles of purpose limitation, data minimization, and strict controls on the processing of high-risk data, including biometric data. Without clear parameters regarding the purpose, duration, and under whose supervision facial data is processed, state use of facial recognition has the potential to blur the line between administrative necessity and excessive surveillance practices.

From a human rights perspective, facial biometric data is directly linked to the right to privacy as recognized in international human rights instruments. Research by (Mantelero, 2018) shows that AI-based technologies using biometric data can create new forms of privacy violations, not only through data collection but also through inference and tracking of individual behavior without meaningful consent. This emphasizes that biometric data protection should not be understood solely as a technical issue of data management, but rather as part of the protection of human dignity and civil liberties.

A comparative legal analysis reveals a significant gap between national and international standards for protecting biometric data. The GDPR explicitly classifies biometric data as a special category of personal data, the processing of which is, in principle, prohibited unless it meets a very strict legal basis (Article 9 of the GDPR). Empirical research by (Tzanou, 2021) confirms that the European Union's approach places biometric data within the highest protection regime due to its potential for misuse by states and corporations. Meanwhile, the EU Artificial Intelligence Act reinforces this position by categorizing facial recognition as a high-risk AI system, requiring the implementation of multiple legal, technical, and institutional safeguards.

Compared to these standards, the research findings indicate that biometric data protection within the national legal framework remains fragmented and tends to be reactive. The absence of specific regulations regarding facial recognition in the public sector means that basic data protection principles—such as accountability, proportionality, and protection of data subjects' rights—have not been optimally internalized in practice. This situation has the potential to undermine legal compliance by state institutions, as the use of technology that touches on citizens' private spheres is not supported by protection mechanisms commensurate with the level of risk.

Based on this normative evaluation, this research prescriptively emphasizes the urgency of establishing a regulatory framework that specifically governs biometric data protection in the use of facial recognition by the public sector. Such regulations need to define the intended limits of use, strengthen data subjects' rights, and require effective oversight and accountability to ensure that the use of AI technology aligns with the principles of the right to privacy, the right to personal data, and internationally recognized AI governance standards.

Risks of Discrimination and Algorithmic Bias in Facial Recognition Identification Processes

The risk of discrimination and algorithmic bias is one of the most crucial challenges in the use of AI algorithms in facial recognition systems in the public sector, particularly when this technology is used in the context of law enforcement, population administration services, and public oversight. Based on research findings, the national legal framework does not explicitly regulate the prevention of algorithmic bias or legal accountability mechanisms for the discriminatory impacts of facial recognition systems. This situation raises serious concerns from the perspective of the principles of non-discrimination and equality before the law.

These findings align with various previous studies showing that facial recognition algorithms are not socially or legally neutral. An empirical study conducted by (Buolamwini, J., & Gebru, 2018) showed a significantly higher error rate in identifying the faces of women and racial minorities compared to light-skinned men. The study revealed that facial recognition accuracy for dark-skinned women can reach an error rate of over 30%, while for light-skinned men the error rate is below 1%. This data provides strong evidence

that bias in training datasets and algorithm design can result in systemic discrimination that potentially violates human rights.

From a legal perspective, algorithmic bias in facial recognition challenges the principles of equality and the prohibition of discrimination as recognized in national and international human rights law. (Crawford, 2021) asserts that AI systems often reproduce and reinforce existing social inequalities, particularly when used by the state in decision-making that directly impacts citizens' rights. In this context, the use of facial recognition by public institutions risks creating a form of indirect discrimination, where the detrimental impact on certain groups stems not from discriminatory intent but from the design of the technology itself.

This research is also relevant to a National Institute of Standards and Technology (NIST) report that found significant variation in the accuracy of facial recognition systems across demographic groups. The NIST report (2019; updated 2022) indicates that some commercial algorithms have higher false positive rates for certain ethnic groups, which in the public sector context can lead to misidentification, mistaken arrests, or restrictions on access to public services. This fact emphasizes that algorithmic bias is not simply a technical issue but has serious legal implications when the technology is used by the state.

From a normative evaluation perspective, the absence of mandatory bias audits, human rights impact tests, and error correction mechanisms in national law indicates a failure to fulfill the principles of the rule of law and algorithmic accountability. Unlike the European Union's approach, the EU Artificial Intelligence Act explicitly classifies facial recognition as a high-risk AI system and requires discrimination risk mitigation, dataset quality, and human oversight. As (Veale, M., & Borgesius, 2021) argue, effective regulation must bridge the gap between the technical complexity of AI and the normative demands of human rights protection.

Based on a prescriptive analysis, this study asserts that the regulation of facial recognition in the public sector must explicitly recognize the risk of algorithmic discrimination as a legal issue, not simply a technological one. Legal obligations to conduct regular bias audits, transparency of system parameters, and redress mechanisms for individuals harmed by misidentification are required. Without these normative measures, the use of AI algorithms has the potential to undermine the principle of substantive justice and undermine public trust in state institutions.

Weak Transparency, Oversight, and Legal Accountability Mechanisms in the Use of Facial Recognition by State Institutions

The lack of transparency, oversight, and legal accountability mechanisms in the use of facial recognition systems by state institutions constitutes a structural issue that places AI technology in a position beyond public legal control. Based on research findings, the primary problem lies not in the absence of general norms, but rather in the absence of legal instruments that operationally require algorithm transparency, independent audits, and accountability accessible to affected communities. This situation reflects the imbalance between the rapid adoption of technology and the readiness of the legal system to ensure responsible technology management.

These findings are consistent with research by (Davenport, T. H., & Mittal, 2020), which states that most public sector AI systems are developed and operated as black boxes, where the decision-making logic cannot be traced by either users or affected parties. In the context of facial recognition, this opacity increases the risk of misidentification but also hinders efforts to seek legal accountability. This is reinforced by (Pasquale, 2015), who

explains that the lack of transparency in automated state systems has the potential to undermine the principle of due process of law because individuals lack sufficient information to challenge algorithm-based administrative decisions.

From an oversight perspective, previous research has shown that internal control mechanisms alone are insufficient to ensure the use of AI in accordance with good governance principles. A report by the European Union Agency for Fundamental Rights (FRA, 2019) emphasized that the use of facial recognition by public authorities must be subject to independent oversight, particularly as this technology directly impacts the rights to privacy, freedom of movement, and protection from mass surveillance. When oversight is internal and opaque, the potential for abuse of power increases, particularly in the context of security and law enforcement.

Within the framework of accountability, research by (Edwards, L., & Veale, 2018) highlights the gap between classical legal accountability concepts and modern AI systems. They explain that without a legal obligation to explain the system's workings and the basis for decision-making, accountability for algorithmic errors becomes unclear: it is unclear whether responsibility rests with the developer, the operator, or state institutions as users. This situation creates what is known as an accountability gap, where citizens' rights to justice are not balanced by effective mechanisms for tracking responsibility.

When evaluated normatively, the lack of transparency and accountability in the use of facial recognition in the public sector indicates a suboptimal implementation of the rule of law, particularly the principles of openness and limited power. Unlike the European Union's approach, which mandates algorithmic transparency, risk assessment, and human oversight in the EU Artificial Intelligence Act, national legal frameworks do not explicitly establish these obligations as minimum standards. As stated by (Leenes, 2020), AI regulations that lack transparency obligations and independent oversight risk transforming the technology into an instrument of power that is difficult to democratically control.

Based on prescriptive analysis, this study asserts that strengthening legal accountability for the use of facial recognition must be directed at establishing clear legal obligations regarding system transparency, regular algorithm audits by independent institutions, and complaint and redress mechanisms for individuals who suffer losses. Without these regulatory reforms, the use of AI in the public sector has the potential to conflict with the principles of good governance and erode the legal legitimacy of the state in carrying out its service functions and protecting citizens' rights.

Conclusions

This study demonstrates that the use of artificial intelligence algorithms in facial recognition systems in the public sector has significant strategic value in improving the effectiveness of public services, security, and government administration, but at the same time presents complex legal challenges that have not been fully addressed within the national regulatory framework. The main strength of this study lies in its normative-comparative approach that is able to systematically reveal the gap between the practice of implementing facial recognition by state institutions and fundamental legal principles, particularly the principles of legality, human rights protection, personal data protection, and responsible AI governance. The research findings confirm that although there are general norms governing data protection, human rights, and the implementation of electronic systems, there is no explicit, integrated, and operational legal basis that specifically regulates

the use of facial recognition in the public sector, including mechanisms for limiting authority, preventing algorithmic discrimination, system transparency, independent oversight, and legal accountability. On the other hand, this study's limitations lie in its normative scope and reliance on secondary data, thus not yet empirically describing the variations in the practice of implementing this technology in the field or the perceptions of the public and officials who use the system. Nevertheless, the results of this study have the potential for broad application, particularly as a conceptual and normative reference for policymakers in formulating specific regulations related to high-risk AI, as a basis for strengthening technology governance in the public sector, and as a framework for evaluating legal compliance for state institutions that have or will implement facial recognition systems. By expanding this study through empirical and interdisciplinary research, the resulting findings have the potential to enrich the development of national legal policies that are responsive to technological advances while still ensuring the protection of citizens' constitutional rights and the principles of the rule of law.

Acknowledgement

The author would like to express sincere appreciation to all individuals and institutions who contributed to the completion of this study. Gratitude is extended to legal experts, technology practitioners, and policymakers who provided valuable insights regarding the use of AI algorithms in public-sector facial recognition systems. The author also thanks academic advisors and colleagues for their guidance and constructive feedback. It is hoped that this research contributes to a deeper understanding of legal compliance and regulatory challenges in this evolving field.

References

Amaka Justina Obinna, & Azeez Jason Kess-Momoh. (2024). Developing a conceptual technical framework for ethical AI in procurement with emphasis on legal oversight. *GSC Advanced Research and Reviews*, *19*(1), 146–160. https://doi.org/10.30574/gscarr.2024.19.1.0149

Binns, R. (2020). Human Judgement in Algorithmic Loops: Individual Justice and Automated Decision-Making. *Regulation & Governance*, *14(2)*, 311–329.

Buolamwini, J., & Gebru, T. (2018). Gender Shades: Intersectional Accuracy Disparities in Commercial Gender Classification. *Proceedings of Machine Learning Research*, *81*, 1–15.

Capasso, C., Zingoni, A., Calabro, G., & Sterpa, A. (2023). Legal and Technical Answers to Privacy Issues raised by AI-based Facial Recognition Algorithms. *2023 IEEE International Conference on Metrology for EXtended Reality, Artificial Intelligence and Neural Engineering (MetroXRAINE)*, 575–580. https://doi.org/10.1109/MetroXRAINE58569.2023.10405669

Chalakov, R., Andonov, A., & Jekova, V. (2025). Artificial intelligence and biometric technologies in defense algorithms and challenges. *Proceeding of 34th International Scientific and Technical Conference Automation of Discrete Production Engineering 2025*, 173–181. https://doi.org/10.53656/adpe-2025.15

Crawford, K. (2021). Atlas of AI: Power, Politics, and the Planetary Costs of Artificial Intelligence. *Yale University Press*.

Davenport, T. H., & Mittal, N. (2020). Creating Trust in Artificial Intelligence. *MIT Sloan Management Review*, *61(4)*, 1–6.

Della Giustina, C., & De Gioia Carabellese, P. (2024). Article: AI, Facial Recognition, and Policing: Business Opportunities and Legal Challenges: A UK Analysis with Glimpses of EU Law. *Global Privacy Law Review*, *5*(Issue 1), 23–30. https://doi.org/10.54648/GPLR2024008

Edwards, L., & Veale, M. (2018). Slave to the Algorithm? Why a Right to an Explanation Is Probably Not the Remedy You Are Looking For. *Duke Law & Technology Review*, *16(1)*, 18–84.

Elmi, M. (2025). Faces and places: navigating the cross-border legal challenges of AI facial recognition technologies. *AI and Ethics*, *5*(5), 5453–5466. https://doi.org/10.1007/s43681-025-00787-5

Frimpong, V. (2025). Rules for Radical AI: A Counter-Framework for Algorithmic Contestation. *Annals of Social Sciences & Management Studies*, *11*(5). https://doi.org/10.19080/ASM.2025.11.555823

Garvie, C., Bedoya, A., & Frankle, J. (2016). The Perpetual Line-Up: Unregulated Police Face Recognition in America. *Georgetown Law Center on Privacy & Technology*.

Gültekin-Várkonyi, G. (2024). Navigating data governance risks: Facial recognition in law enforcement under EU legislation. *Internet Policy Review*, *13*(3). https://doi.org/10.14763/2024.3.1798

H Patel, U., & Gera, K. (2024). Biometric Security Systems Enhanced by AI: Exploring Concerns with AI Advancements in Facial Recognition and Other Biometric Systems have Security Implications and Vulnerabilities. *International Journal of Innovative Science and Research Technology (IJISRT)*, 2078–2082. https://doi.org/10.38124/ijisrt/IJISRT24JUN1510

Hennocq, Q., Bongibault, T., Garcelon, N., & Khonsari, R. H. (2024). Humanitarian Facial Recognition for Rare Craniofacial Malformations. *Plastic and Reconstructive Surgery - Global Open*, *12*(5), e5780. https://doi.org/10.1097/GOX.0000000000005780

Kuner, C., Bygrave, L. A., Docksey, C., & Drechsler, L. (2017). The General Data Protection Regulation: A Commentary. *Oxford University Press*.

Kurniawan, K. S., & Kurniawan, I. G. A. (2025). The Limitations of Lex Generalis: Analyzing the Readiness of the GDPR and PDP Law for AI-Based Facial Recognition Technology. *SIGn Jurnal Hukum*, *7*(2), 838–852. https://doi.org/10.37276/sjh.v7i2.533

Leenes, R. (2020). Governing Algorithms: The Normative Challenges of Automated Decision-Making. *Oxford University Press*.

Lynskey, O. (2019). Criminal Justice Profiling and EU Data Protection Law: Pre-empting the Presumption of Innocence? *International Data Privacy Law*, *9(2)*, 82–102.

Malladhi, A. (2023). Transforming Information Extraction: AI and Machine Learning in Optical Character Recognition Systems and Applications Across Industries. *International Journal of Computer Trends and Technology*, *71*(4), 81–90. https://doi.org/10.14445/22312803/IJCTT-V71I4P110

Mantelero, A. (2018). AI and Big Data: A Blueprint for a Human Rights, Social and Ethical Impact Assessment. *Computer Law & Security Review*, *34(4)*, 754–772.

Pasquale, F. (2015). The Black Box Society: The Secret Algorithms That Control Money and Information. *Harvard University Press*.

Prasad Adhhikari, A. (2025). Artificial Intelligence in Governance: The State of Facial Recognition Technology in Canada. *Policy & Governance Review*, *9*(3), 334. https://doi.org/10.30589/pgr.v9i3.1275

Rangari, J. (2025). Balancing AI Innovation and Privacy: A Study of Facial Recognition Technologies under the DPDPA. *Revista Review Index Journal of Multidisciplinary*, *5*(1), 30–38. https://doi.org/10.31305/rrijm2025.v05.n01.004

Rezende, I. N. (2020). Facial recognition in police hands: Assessing the 'Clearview case' from a European perspective. *New Journal of European Criminal Law*, *11*(3), 375–389. https://doi.org/10.1177/2032284420948161

Stepanov, O., & Basangov, D. (2025). Smart Digital Facial Recognition Systems in the Context of Individual Rights and Freedoms. *Legal Issues in the Digital Age*, *6*(2), 118–133. https://doi.org/10.17323/2713-2749.2025.2.118.133

Tshipota, T. C., Du, C., Nawej, C. M., & Leholo, S. T. (2025). A Systematic review on AI-based object recognition in unfavorable weather condition: Curacy and GDPR compliance. *Edelweiss Applied Science and Technology*, *9*(8), 641–651. https://doi.org/10.55214/2576-8484.v9i8.9394

Tzanou, M. (2021). Data Protection as a Fundamental Right Next to Privacy? "Reconstructing" a Not So New Right. *International Data Privacy Law*, *11(1)*, 1–14.

Veale, M., & Borgesius, F. Z. (2021). Demystifying the Draft EU Artificial Intelligence Act. *Computer Law & Security Review*, *22(4)*, 1–15.

Veale, M., & Edwards, L. (2018). Clarity, Surprises, and Further Questions in the GDPR's "Right to Explanation. *Computer Law & Security Review*, *34(2)*, 398–404.

Velinova, E., Cvetanoski, V., Chakarovski, K., Mechkaroska, D., & Domazet, E. (2025). Cloud-Based AI Surveillance for Motion Detection and Facial Recognition. *2025 3rd Cognitive Models and Artificial Intelligence Conference (AICCONF)*, 1–6. https://doi.org/10.1109/AICCONF64766.2025.11064180