Jurnal Kecerdasan Buatan dan Teknologi Informasi
Vol. 4, No. 3, September 2025, pp. 356-363
e-ISSN: 2964-2922, p-ISSN: 2963-6191
DOI : https://doi.org/10.69916/jkbti.v4i3.491

CONSTITUTIONAL LIMITS ON GOVERNMENT USE OF FACIAL RECOGNITION TECHNOLOGY IN PUBLIC SERVICES AND PUBLIC SECURITY

Wiredarme

Institut Pemerintahan Dalam Negeri, Indonesia
Email: wiredarme@ipdn.ac.id

(Received: July 5, 2025; Revised: September 12, 2025; Accepted: September 27, 2025)

Abstract

This study aims to examine the constitutional limits of government use of facial recognition technology in public services, public security, and citizen identification. The central issue addressed in this article is the tension between state interests in security and administrative efficiency on the one hand, and the protection of privacy, civil liberties, equality, due process, and constitutional rights on the other. This study employs a qualitative legal research method with a normative-doctrinal approach. The analysis is conducted through statutory, conceptual, and comparative approaches by examining constitutional principles, legal norms, regulatory frameworks, human rights standards, and recent academic literature on facial recognition, biometric governance, digital identity, and public-sector surveillance. The findings show that facial recognition is not merely a technical instrument, but a form of constitutional state action because it enables the government to collect, process, store, and act upon citizens' biometric identity. In public services, the technology may improve verification and administrative efficiency, but it may also create forced consent and exclusion from essential services. In public security, facial recognition may support lawful identification, but it may also enable mass surveillance, chilling effects, discriminatory outcomes, and unchallengeable decisions. This study contributes a constitutional boundary framework based on legality, legitimate aim, necessity, proportionality, transparency, accountability, non-discrimination, meaningful human review, and effective remedy. The study implies that facial recognition may only be constitutionally justified when technological capability remains subject to strict rights-based legal control.

Keywords: facial recognition, constitutional rights, public security, public services, biometric data, privacy.

1. INTRODUCTION

Facial recognition technology has become one of the most consequential instruments in contemporary digital government because it transforms the human face into a machine-readable identifier for authentication, verification, surveillance, and administrative decision-making. In public services, facial recognition is increasingly associated with digital identity systems, access to government portals, welfare distribution, immigration control, and citizen verification. In public security, the same technology is used to identify suspects, search for wanted persons, monitor public spaces, support border management, and assist criminal investigations. This dual function places facial recognition at the intersection of administrative efficiency and coercive state power. Its constitutional relevance emerges because the face is not merely technical data, but a bodily attribute that is permanent, visible, and closely connected to personal identity, autonomy, dignity, and freedom from arbitrary state interference [1], [2], [12].

The main problem is not only whether facial recognition can improve the accuracy or speed of public administration and security operations, but whether its use by government can remain compatible with constitutional rights. Facial recognition can create a form of pervasive identification in which individuals are recognized, classified, traced, or profiled without meaningful awareness or consent. In ordinary public service contexts, citizens may feel compelled to submit biometric data because access to essential services depends on compliance. In security contexts, the technology may expand surveillance capacity beyond traditional limits because cameras, databases, and algorithmic matching can operate continuously and invisibly. These features raise serious risks to privacy, equality, freedom of movement, freedom of assembly, freedom of expression, due process, and protection from discriminatory treatment [5], [6], [9], [18].

The constitutional dilemma becomes sharper because facial recognition is often justified through public interest arguments, especially national security, crime prevention, administrative modernization, and fraud control. These objectives are legitimate in a democratic state, yet constitutional government requires every restriction of rights to be based on clear law, a legitimate aim, necessity, proportionality, accountability, and effective remedies. Facial recognition is problematic when the legal basis is vague, the purpose is overly broad, the retention period is unclear, the database is interoperable without strict limits, or the individual has no effective mechanism to challenge false matches. Misidentification is not a merely technical error because it can lead to exclusion from services, wrongful

suspicion, unlawful arrest, reputational harm, or unequal treatment of vulnerable groups [3], [7], [17], [20]. For that reason, the use of facial recognition by the government must be examined not only as a matter of technological governance, but also as a constitutional question concerning the boundaries of state authority.

Recent scholarship has developed important analyses of facial recognition from legal, ethical, regulatory, and human rights perspectives. Qandeel argues that facial recognition must be assessed through the rule of law, legal certainty, and the state duty to regulate unacceptable-risk AI systems [1]. Wang et al. examine the ethical and regulatory implications of face recognition beyond surveillance, especially in relation to privacy, consent, and legal accountability [2]. Sarabdeen emphasizes that existing legal frameworks are often insufficient to protect individual rights when facial recognition is used by public and private actors [12]. Raposo's work provides a detailed analysis of facial recognition under European data protection law and law enforcement frameworks, including the need for stricter safeguards in government deployment [15], [16]. Simmler and Canova further show that facial recognition in law enforcement requires a specific legal basis because general data analysis rules cannot automatically justify biometric identification by police authorities [3]. Galič and Stevens demonstrate that criminal procedure law and data protection law often fail to interact effectively, creating gaps in supervision, necessity assessment, and proportionality control [7].

Other studies have expanded the debate toward democracy, public space, protest, and civil liberties. Lynch compares regulatory case studies in policing and security and shows that facial recognition regulation remains fragmented, reactive, and highly dependent on institutional context [8]. Fletcher analyzes government surveillance and facial recognition in Australia through a human rights lens, showing how public security arguments may normalize intrusive identification practices [4]. Mobilio discusses the surveillance power of real-time facial recognition in urban spaces and links it to risks of mass monitoring and fundamental rights violations [18]. Palmiotto and Menéndez González connect facial recognition with democracy and human rights, stressing that biometric surveillance can weaken democratic participation when citizens cannot appear in public without being identifiable by the state [9]. Gabrielli focuses on peaceful protest and argues that facial recognition may produce a chilling effect on freedom of assembly and expression [5]. Murray also warns that facial recognition may alter the practical meaning of human rights because it enables persistent visibility and continuous state recognition [6]. Dauvergne extends this critique to the Global South and argues that facial recognition for policing and surveillance may intensify authoritarian practices, social control, and unequal exposure to state power [13].

A second body of literature examines public acceptance, institutional trust, privacy perception, and implementation risks. Shore shows that public support for facial recognition is shaped by framing and context, meaning that citizens may react differently when the technology is presented as a security tool, convenience tool, or privacy threat [10]. Choung et al. find that acceptance of AI-powered facial recognition in surveillance scenarios depends strongly on trust in responsible authorities, perceived security benefits, and perceived privacy risks [11]. Liu et al. analyze face recognition and privacy in China through social cognition and cultural psychology, showing that perceived risk, trust, and cultural context influence public attitudes toward biometric technologies [14]. Zhang demonstrates that perceived privacy and perceived security affect behavioral intention to use face recognition through trust, perceived usefulness, and perceived ease of use [19]. Martin and Metzger connect facial recognition with digital identity acceptance and show that privacy, usability, data sovereignty, and technology affinity influence citizen acceptance of biometric identity systems [21]. Fussey et al. reveal that "assisted" facial recognition in policing does not remove human discretion, but reshapes suspicion through algorithmic outputs [22]. Urquhart and Miranda also show that intelligent facial surveillance creates future governance challenges because police use may become normalized before constitutional safeguards mature [23]. Raposo's analysis of erroneous identification strengthens this concern by showing that algorithmic failures may generate legal liability and rights violations when the system misrecognizes individuals [17].

Although these studies provide strong foundations, existing research is still fragmented across data protection, criminal procedure, ethics, public acceptance, democracy, and surveillance studies. Many studies focus on specific jurisdictions, regulatory models, public attitudes, or law enforcement contexts, while fewer studies formulate a constitutional boundary framework that applies across public services, public security, and citizen identification. This article fills that gap by examining the constitutional limits of government facial recognition as a rights-restricting public power. The novelty of this study lies in positioning facial recognition not merely as an administrative innovation or security technology, but as a constitutional object that must be controlled through legality, necessity, proportionality, due process, equality, transparency, independent oversight, and accessible remedies. The purpose of this study is to analyze how governments may use facial recognition in public service and public security without violating privacy, civil liberties, and constitutional protection of citizens.

2. RESEARCH METHODS

This study uses a qualitative legal research design with a normative-doctrinal approach. The research does not employ quantitative measurement, statistical testing, biometric experiments, machine-learning model evaluation, or a specific facial recognition algorithm. Instead, it examines facial recognition technology as an object of constitutional

analysis by interpreting legal norms, constitutional principles, regulatory instruments, court decisions, and academic literature. The qualitative design is appropriate because the main research problem concerns the constitutional limits of government power, rather than the technical performance of facial recognition systems. The study focuses on how facial recognition may be legally justified, restricted, supervised, and challenged when it is used by public authorities in public service delivery and public security operations.

The doctrinal method is combined with statutory, conceptual, and comparative approaches. The statutory approach is used to examine legal norms governing constitutional rights, privacy, personal data protection, administrative authority, public service delivery, public security, and the use of biometric data by the government. The conceptual approach is used to develop an analytical framework based on legality, necessity, proportionality, due process, equality, transparency, accountability, and effective remedy. The comparative approach is used to understand how different jurisdictions regulate facial recognition, especially in relation to biometric identification, law enforcement surveillance, automated decision-making, and public-sector digital governance. This combination enables the study to evaluate facial recognition not merely as a technological innovation, but as a form of state action that must remain within constitutional boundaries.

This study adopts a case-study orientation by focusing on government facial recognition in two main institutional contexts. The first context is public service delivery, particularly the use of facial recognition for citizen identification, digital identity verification, access to government platforms, distribution of welfare benefits, immigration services, and administrative authentication. This context is important because citizens may be required to submit biometric data in order to obtain essential public services. The second context is public security, particularly the use of facial recognition by police, immigration authorities, border agencies, and security institutions to identify suspects, monitor public spaces, support investigations, and manage security risks. These two contexts are selected because they represent the most visible tension between administrative efficiency, state security, privacy, civil liberties, and constitutional protection.

The data used in this study consist of legal materials and academic sources. Primary legal materials include constitutional provisions, statutory regulations, government regulations, public service rules, data protection laws, administrative law instruments, and legal norms related to security and law enforcement. Where relevant, the study also examines judicial decisions, constitutional court reasoning, human rights instruments, and official regulatory documents concerning biometric data and state surveillance. Secondary legal materials include peer-reviewed journal articles, academic books, research reports, and scholarly discussions on facial recognition, digital identity, biometric surveillance, data protection, public security, and constitutional rights. Tertiary materials, such as legal dictionaries, official institutional glossaries, and regulatory explanatory notes, are used only to clarify technical or legal terminology.

Data collection is conducted through library research and document analysis. The study collects journal articles published in recent years from reputable academic databases and publishers, especially literature that discusses facial recognition, biometric governance, human rights, public-sector AI, digital identity, surveillance, and constitutional law. The selection of literature is based on relevance to the research focus, academic credibility, recency, and the availability of identifiable DOI information. Legal documents are selected based on their normative authority and relevance to the regulation of state power, personal data, privacy, public service, and public security. The collected materials are then organized according to key themes, namely the legal basis of facial recognition, the purpose of government use, risks to constitutional rights, safeguards against abuse, oversight mechanisms, and remedies for affected citizens.

The analysis is conducted through qualitative content analysis and normative legal interpretation. First, the study identifies the legal and constitutional principles that should govern the use of facial recognition by public authorities. Second, it examines whether the use of facial recognition in public service and security contexts satisfies the requirements of legality, legitimate aim, necessity, proportionality, transparency, accountability, and non-discrimination. Third, it evaluates the risks created by unclear legal mandates, excessive data collection, database integration, algorithmic bias, false identification, lack of consent, and insufficient remedies. Fourth, the study formulates a constitutional boundary framework that can be used to determine when government facial recognition is permissible, restricted, or unconstitutional.

The validity of the analysis is strengthened through source triangulation. This is done by comparing legal norms, scholarly literature, regulatory debates, and relevant case examples across different public-sector contexts. The study does not treat technological efficiency as the only measure of legitimacy. Instead, it assesses facial recognition through constitutional standards that require public power to be legally grounded, rights-sensitive, accountable, and subject to independent supervision. Through this method, the study seeks to produce a legal argument that is conceptually rigorous, normatively grounded, and relevant for governments that are considering or already implementing facial recognition in public services and public security.

3. RESULTS AND DISCUSSION

3.1. Facial Recognition as a Form of Constitutional State Action in Public Services and Public Security

The findings of this study show that government use of facial recognition technology cannot be understood only as a technical instrument for identity verification or security enhancement. In constitutional terms, facial recognition constitutes a form of state action because it enables public authorities to collect, process, compare, store, and act upon biometric characteristics attached to citizens' physical identity. This finding is important because the human face is not ordinary administrative data. It is a permanent and highly identifiable biometric attribute that links the body, legal identity, public presence, and personal autonomy. When the state transforms facial features into digital templates, the relationship between citizen and government changes from conventional identification into continuous technological recognizability.

In the context of public services, facial recognition may support administrative efficiency by simplifying access to digital identity systems, welfare distribution, immigration services, licensing platforms, and electronic government portals. The technology can reduce document fraud, accelerate authentication, and improve service accessibility when it is governed by strict legal safeguards. Yet the study finds that public service facial recognition also produces a risk of forced consent. Citizens often do not have an equal bargaining position when access to essential services depends on biometric submission. In this situation, consent becomes formally present but substantively weak. This finding is consistent with Wang et al., who argue that facial recognition raises serious ethical and legal issues because biometric processing often occurs in contexts where privacy, consent, and institutional accountability are not sufficiently balanced [2].

In the context of public security, facial recognition creates a stronger constitutional concern because it is connected to the coercive functions of the state. Police, immigration authorities, border agencies, and security institutions may use facial recognition to identify suspects, monitor public areas, detect wanted persons, or support criminal investigations. These objectives may serve legitimate public interests, yet they also expand the capacity of the state to identify individuals in public spaces without direct interaction, prior suspicion, or meaningful notification. Simmler and Canova emphasize that facial recognition in law enforcement cannot be treated as ordinary data analysis because biometric matching changes the nature of police identification and requires a specific legal basis [3]. This study supports that position and adds that the constitutional character of facial recognition depends not only on who uses the technology, but also on the purpose, scale, legal basis, database connection, and consequences of the identification process.

The analysis also finds a fundamental difference between targeted facial recognition and mass facial recognition. Targeted use refers to limited biometric matching based on a specific legal purpose, such as identifying a missing person, confirming a person already subject to lawful investigation, or verifying identity in a clearly regulated service. Mass use refers to indiscriminate scanning of crowds, public spaces, protests, transport hubs, or administrative databases without individualized suspicion. Targeted use may be constitutionally justifiable when it satisfies legality, necessity, and proportionality. Mass use is more difficult to justify because it tends to transform public space into a zone of permanent identification. This finding is in line with Gabrielli, who argues that facial recognition in protest contexts may lead to mass surveillance and weaken the protection of peaceful assembly [5].

The study further finds that the constitutional issue is not eliminated by the existence of human operators. In practice, facial recognition systems may be described as "assisted" tools because the final decision remains in human hands. Yet algorithmic outputs can strongly influence human judgment, especially when officers or administrators treat system matches as reliable indicators of identity. Fussey et al. show that assisted facial recognition reshapes suspicion and discretion in digital policing because human operators may depend on algorithmic signals when making operational judgments [22]. This study confirms that constitutional safeguards must apply not only to fully automated decisions, but also to hybrid decision-making where human officials rely on biometric algorithmic outputs.

3.2. Constitutional Rights Affected by Government Facial Recognition

The second finding shows that facial recognition affects several constitutional rights at the same time. The first and most direct right is privacy. Facial recognition enables the state to identify individuals from images, cameras, databases, or digital platforms without requiring physical documents or active participation. Privacy is affected not only when data are disclosed, but also when individuals lose control over how their biometric identity is captured, stored, reused, and connected to other government databases. Sarabdeen argues that facial recognition creates legal vulnerability because existing legal frameworks often fail to provide sufficient protection for individual rights in biometric processing [12]. This study strengthens that argument by showing that privacy protection must include purpose limitation, storage limitation, database separation, prior authorization, and a right to challenge biometric processing.

The second affected right is freedom of movement and freedom from arbitrary surveillance. When facial recognition is installed in public areas, transport systems, border points, or government buildings, individuals may become continuously identifiable in spaces where anonymity previously existed. Public space is not a rights-free zone. Citizens should be able to move, gather, and participate in social life without being subjected to constant biometric recognition. Mobilio argues that facial recognition increases the surveillance power of the state because public

visibility can be converted into automated identifiability [18]. Murray also warns that facial recognition may change the practical meaning of human rights because the technology makes individuals permanently visible to state systems [6]. This study finds that such risks are constitutionally relevant because democratic citizenship requires a protected sphere of public anonymity.

The third affected right is freedom of assembly and expression. Facial recognition may discourage citizens from attending demonstrations, political meetings, religious gatherings, civil society events, or public protests if they believe their presence can be identified and recorded by the government. The chilling effect does not require direct punishment. It may arise from fear of future monitoring, profiling, investigation, or administrative consequences. Gabrielli's study on peaceful protest supports this finding by showing that facial recognition may facilitate mass surveillance practices and weaken the exercise of human rights in democratic societies [5]. Palmiotto and Menéndez González also argue that facial recognition can threaten democracy when biometric surveillance reduces citizens' ability to participate freely in public life [9]. This study adds that the constitutional assessment of facial recognition must consider not only actual misuse, but also the reasonable fear created by its possible use.

The fourth affected right is equality and non-discrimination. Facial recognition systems may produce unequal outcomes because of differences in training data, image quality, demographic representation, lighting, camera angle, age, gender, skin tone, disability, or other physical characteristics. A false match may expose an innocent person to questioning, exclusion, arrest, or administrative denial. A false non-match may prevent a citizen from accessing public services. Raposo's study on erroneous identification shows that facial recognition errors can create legal liability and serious rights consequences when systems fail to recognize individuals correctly [17]. This study finds that equality concerns are not secondary technical issues. They are constitutional issues because the state has a duty to prevent discriminatory impact in public services and security operations.

The fifth affected right is due process. Facial recognition may influence administrative or security decisions without giving citizens access to the reason, evidence, algorithmic basis, or review mechanism behind the decision. A person may be denied access to services, flagged for investigation, delayed at a border checkpoint, or wrongly identified as a suspect without knowing how the system produced the match. Galič and Stevens show that the interaction between criminal procedural law and data protection law may create regulatory gaps in police use of facial recognition [7]. This study reaches a similar finding in the broader context of constitutional governance. Due process requires that affected individuals have access to explanation, correction, appeal, independent review, and remedy when facial recognition contributes to adverse decisions.

The analysis also shows that public acceptance cannot replace constitutional legitimacy. Citizens may support facial recognition when it is framed as a tool for convenience or security, but acceptance does not automatically justify rights restriction. Shore finds that public support for facial recognition depends heavily on framing and context [10]. Choung et al. also show that trust, perceived security, and privacy perceptions affect acceptance of AI-powered facial recognition in surveillance settings [11]. These findings are useful, but constitutional analysis requires a stricter standard. Public trust may support implementation, yet it cannot replace clear law, proportionality review, independent oversight, and enforceable remedies.

3.3. Constitutional Boundary Framework for Government Use of Facial Recognition

The third finding of this study is the need for a constitutional boundary framework that determines when government facial recognition is permissible, restricted, or unconstitutional. The first boundary is legality. Facial recognition must be based on a clear, specific, accessible, and democratically legitimate legal basis. A general mandate to maintain public order, improve public services, or modernize administration is not sufficient. The law must define the authorized institution, permitted purpose, type of biometric processing, scope of database use, retention period, oversight mechanism, and rights of affected persons. Qandeel argues that facial recognition must be regulated through the rule of law because unclear legal mandates can create unacceptable risks for individual rights [1]. This study agrees and finds that legality is the first constitutional filter for any government deployment of facial recognition.

The second boundary is legitimate aim and necessity. Facial recognition may only be used for a specific and constitutionally acceptable purpose, such as preventing serious crime, protecting vulnerable persons, verifying identity in high-risk public services, or securing borders under strict conditions. The government must show that the technology is necessary because less intrusive alternatives are insufficient. Necessity cannot be presumed from technological efficiency alone. A faster system is not automatically a constitutionally necessary system. Raposo's analysis of European law enforcement use shows that biometric identification requires careful assessment because public security objectives must be balanced against privacy and data protection safeguards [15]. This study develops that argument by emphasizing that necessity must be proven before deployment, not after rights violations occur.

The third boundary is proportionality. Facial recognition must not impose excessive rights restrictions in relation to the public objective pursued. Proportionality requires limits on location, duration, database size, category of persons, access authority, data sharing, and retention period. Real-time facial recognition in public spaces should be treated as a high-risk or exceptional measure because it allows immediate biometric identification of people who have not individually triggered suspicion. Lynch's regulatory case studies show that facial recognition governance

remains fragmented and often reactive in policing and security contexts [8]. This study finds that proportionality can reduce such fragmentation by offering a structured test for assessing whether the scale and intensity of facial recognition are constitutionally acceptable.

The fourth boundary is transparency and explainability. Citizens must know when facial recognition is used, for what purpose, by which institution, and with what legal consequences. Transparency does not mean disclosing sensitive operational details that may endanger lawful investigations. It means ensuring that facial recognition does not operate as a hidden infrastructure of public power. In public services, transparency requires notice, clear consent mechanisms where appropriate, alternative access channels, and information about data retention and complaint procedures. In security contexts, transparency requires public rules, reporting duties, audit records, and independent review. Wang et al. emphasize that facial recognition requires stronger ethical and regulatory frameworks to address privacy and accountability problems [2]. This study confirms that transparency is a constitutional requirement because secret biometric governance weakens public control over state power.

The fifth boundary is accountability and independent oversight. Facial recognition should be subject to institutional responsibility before, during, and after deployment. Before deployment, the government should conduct human rights impact assessments, data protection impact assessments, bias testing, and necessity analysis. During deployment, the system should be monitored through audit logs, accuracy reports, access controls, and independent supervision. After deployment, affected citizens must have access to complaint mechanisms, correction procedures, judicial remedies, and compensation when harm occurs. Raposo's work on erroneous identification shows that liability becomes crucial when facial recognition produces false matches or wrongful consequences [17]. This study adds that accountability must be institutional, not merely technical. Public authorities cannot shift constitutional responsibility to vendors, algorithms, or software providers.

The sixth boundary is non-discrimination and human review. Government facial recognition must be tested for demographic bias, error rates, database quality, and unequal impact before being used in public decisions. Human review must be meaningful, not symbolic. Officials must be trained to question algorithmic outputs, examine supporting evidence, and avoid treating biometric matches as conclusive proof. This is especially important in policing, immigration, welfare distribution, and administrative sanctions. Fussey et al. show that assisted facial recognition can reshape police discretion even when human operators remain formally involved [22]. This study finds that meaningful human review must include competence, independence, documentation, and responsibility for the final decision.

Based on these findings, the study formulates a constitutional standard for government use of facial recognition. The technology may be permissible when it is based on specific law, pursues a legitimate aim, is necessary for a clearly defined purpose, is proportionate in scale, uses reliable and tested systems, provides transparency, includes independent oversight, prevents discrimination, and offers effective remedies. It should be restricted when the purpose is vague, the database is excessive, the retention period is unclear, the technology affects vulnerable groups disproportionately, or citizens lack alternatives in essential public services. It should be considered unconstitutional when it enables indiscriminate mass surveillance, operates without clear legal basis, suppresses civil liberties, produces unchallengeable decisions, or removes meaningful control over biometric identity. This framework positions facial recognition as a technology that may serve public interests only when constitutional limits remain stronger than technological capability.

4. CONCLUSION

This study concludes that government use of facial recognition technology in public services and public security must be understood as a constitutional issue, not merely as a technical instrument for administrative modernization or crime prevention. Facial recognition changes the relationship between citizens and the state because it allows public authorities to transform the human face into a permanent digital identifier. In public service contexts, this technology may support identity verification, reduce fraud, and accelerate access to digital government platforms. In public security contexts, it may assist law enforcement, border control, and the identification of persons in specific high-risk situations. Yet these benefits create serious constitutional risks when biometric identification is used without clear legal limits, independent oversight, meaningful remedies, and protection against arbitrary state action.

The main finding of this study is that facial recognition affects several constitutional rights simultaneously. It may interfere with privacy because biometric data are closely connected to bodily identity and personal autonomy. It may restrict freedom of movement, assembly, and expression when citizens become identifiable in public spaces, protests, religious activities, political meetings, or civic participation. It may also threaten equality and non-discrimination because false matches and false rejections can produce unequal impacts on certain demographic groups. In addition, facial recognition may weaken due process when citizens do not know why they are flagged, denied services, investigated, or subjected to administrative consequences. These findings confirm previous studies that identify facial recognition as a high-risk technology for privacy, democracy, and human rights [5], [6], [9], [12], while this study extends the discussion by placing those risks within a more explicit constitutional boundary framework.

The novelty of this study lies in its effort to formulate constitutional limits for the use of facial recognition across two government domains: public service delivery and public security. Previous studies have often focused on data protection, policing, public acceptance, technical bias, or regulatory gaps in particular jurisdictions. This study contributes a broader constitutional framework based on legality, legitimate aim, necessity, proportionality, transparency, accountability, non-discrimination, meaningful human review, and effective remedy. Through this framework, facial recognition may be considered permissible only when the state can prove that its use is legally authorized, strictly necessary, proportionate to a specific public purpose, independently supervised, and open to challenge by affected citizens. It should be restricted when the purpose is vague, the database is excessive, the retention period is unclear, or citizens have no alternative access to essential services. It becomes constitutionally unacceptable when it enables indiscriminate mass surveillance, suppresses civil liberties, or produces unchallengeable decisions.

The implication of this study for previous research is that debates on facial recognition should move beyond the binary question of whether the technology should be accepted or rejected. The more important constitutional question is under what conditions the state may use biometric recognition without transforming public power into permanent surveillance power. This study supports the concerns raised by scholars who argue that facial recognition can reshape police discretion, weaken democratic participation, and normalize biometric surveillance. At the same time, it adds that constitutional review must also cover public service settings, because biometric dependency in essential services can create forced consent and administrative exclusion. The lack of study addressed in this article is the limited integration between public service governance, public security governance, and constitutional rights analysis in facial recognition research.

This study has limitations because it is based on normative legal analysis and document-based interpretation. It does not measure the technical accuracy of facial recognition systems, test algorithmic bias empirically, or examine citizen experiences through field interviews. Future research should conduct empirical studies on how citizens experience facial recognition in public services, especially in welfare distribution, digital identity systems, immigration services, and local government platforms. Further studies should also compare constitutional court decisions, regulatory models, and oversight mechanisms across jurisdictions. In addition, interdisciplinary research involving law, public administration, computer science, and human rights studies is needed to evaluate whether legal safeguards are effective in practice, especially in preventing false identification, discriminatory impact, excessive data retention, and abuse of facial recognition in public security operations.

REFERENCES

[1] M. Qandeel, "Facial recognition technology: regulations, rights and the rule of law," *Frontiers in Big Data*, vol. 7, 2024, doi: 10.3389/fdata.2024.1354659.

[2] X. Wang, Y.-C. Wu, M. Zhou, and H. Fu, "Beyond surveillance: privacy, ethics, and regulations in face recognition technology," *Frontiers in Big Data*, vol. 7, 2024, doi: 10.3389/fdata.2024.1337465.

[3] M. Simmler and G. Canova, "Facial recognition technology in law enforcement: Regulating data analysis of another kind," *Computer Law & Security Review*, vol. 56, 2025, doi: 10.1016/j.clsr.2024.106092.

[4] A. Fletcher, "Government surveillance and facial recognition in Australia: A human rights analysis of recent developments," *Griffith Law Review*, vol. 32, no. 1, pp. 30–61, 2023, doi: 10.1080/10383441.2023.2170616.

[5] G. Gabrielli, "The use of facial recognition technologies in the context of peaceful protest: The risk of mass surveillance practices and the implications for the protection of human rights," *European Journal of Risk Regulation*, vol. 16, no. 2, pp. 514–541, 2025, doi: 10.1017/err.2025.26.

[6] D. Murray, "Facial recognition and the end of human rights as we know them?" *Netherlands Quarterly of Human Rights*, vol. 42, no. 2, 2024, doi: 10.1177/09240519241253061.

[7] M. Galič and L. Stevens, "Regulating police use of facial recognition technology in the Netherlands: The complex interplay between criminal procedural law and data protection law," *New Journal of European Criminal Law*, vol. 14, no. 4, pp. 459–478, 2023, doi: 10.1177/20322844231212834.

[8] N. Lynch, "Facial recognition technology in policing and security—Case studies in regulation," *Laws*, vol. 13, no. 3, 2024, doi: 10.3390/laws13030035.

[9] F. Palmiotto and N. Menéndez González, "Facial recognition technology, democracy and human rights," *Computer Law & Security Review*, vol. 50, 2023, doi: 10.1016/j.clsr.2023.105857.

[10] A. Shore, "Talking about facial recognition technology: How framing and context influence privacy concerns and support for prohibitive policy," *Telematics and Informatics*, vol. 70, 2022, doi: 10.1016/j.tele.2022.101815.

[11] H. Choung, P. David, and T.-W. Ling, "Acceptance of AI-powered facial recognition technology in surveillance scenarios: Role of trust, security, and privacy perceptions," *Technology in Society*, vol. 79, 2024, doi: 10.1016/j.techsoc.2024.102721.

[12] J. Sarabdeen, "Protection of the rights of the individual when using facial recognition technology," *Heliyon*, vol. 8, no. 3, 2022, doi: 10.1016/j.heliyon.2022.e09086.

[13] P. Dauvergne, "Facial recognition technology for policing and surveillance in the Global South: A call for bans," *Third World Quarterly*, vol. 43, no. 9, pp. 2325–2335, 2022, doi: 10.1080/01436597.2022.2080654.
[14] T. Liu, B. Yang, Y. Geng, and S. Du, "Research on face recognition and privacy in China—Based on social cognition and cultural psychology," *Frontiers in Psychology*, vol. 12, 2021, doi: 10.3389/fpsyg.2021.809736.
[15] V. L. Raposo, "The use of facial recognition technology by law enforcement in Europe: A non-Orwellian draft proposal," *European Journal on Criminal Policy and Research*, vol. 29, pp. 515–533, 2023, doi: 10.1007/s10610-022-09512-y.
[16] V. L. Raposo, "(Do not) remember my face: Uses of facial recognition technology in light of the General Data Protection Regulation," *Information & Communications Technology Law*, vol. 32, no. 1, pp. 45–63, 2023, doi: 10.1080/13600834.2022.2054076.
[17] V. L. Raposo, "When facial recognition does not 'recognise': Erroneous identifications and resulting liabilities," *AI & Society*, vol. 39, pp. 1857–1869, 2024, doi: 10.1007/s00146-023-01634-z.
[18] G. Mobilio, "Your face is not new to me—Regulating the surveillance power of facial recognition technologies," *Internet Policy Review*, vol. 12, no. 1, 2023, doi: 10.14763/2023.1.1699.
[19] Y. Zhang, "Impact of perceived privacy and security in the TAM model: The perceived trust as the mediated factors," *International Journal of Information Management Data Insights*, vol. 4, no. 2, 2024, doi: 10.1016/j.jjimei.2024.100270.
[20] A. Sagana, M. Zhang, and M. Sauerland, "Public attitudes towards police use of AI-driven face recognition technology," *Computers in Human Behavior*, 2026, doi: 10.1016/j.chb.2025.108821.
[21] N. Martin and F. M. Metzger, "What determines the acceptance of digital identity and facial recognition-based technologies? Evidence from an eID system and a multi-country survey," *Journal of Innovation Management*, vol. 13, no. 2, pp. 129–173, 2025, doi: 10.24840/2183-0606_013.002_0006.
[22] P. Fussey, B. Davies, and M. Innes, "'Assisted' facial recognition and the reinvention of suspicion and discretion in digital policing," *The British Journal of Criminology*, vol. 61, no. 2, pp. 325–344, 2021, doi: 10.1093/bjc/azaa068.
[23] L. Urquhart and D. Miranda, "Policing faces: The present and future of intelligent facial surveillance," *Information & Communications Technology Law*, vol. 31, no. 2, pp. 194–219, 2022, doi: 10.1080/13600834.2021.1994220.