Passagens. Revista Internacional de História Política e Cultura Jurídica
Rio de Janeiro: vol. 18, nº 3, September-December, 2026, p. 471-482.

https://doi.org/10.15175/dcmy3d24

Articles

Facial recognition technology in law enforcement: balancing security and the right to privacy

Hifajatali SAYYED*

Maharashtra National Law University, Chhatrapati Sambhajinagar, India

Abstract

Facial Recognition Technology has rapidly emerged as a powerful tool in modern law enforcement, enabling efficient identification, surveillance, and crime prevention. However, its widespread deployment raises significant concerns regarding the protection of the right to privacy and other fundamental human rights. This paper examines the tension between state interests in ensuring public safety and the individual's right to informational self-determination. It critically analyzes the legal and constitutional framework governing surveillance, with particular reference to the recognition of privacy as a fundamental right in Justice K.S. Puttaswamy v. Union of India. The study further explores issues of proportionality, necessity, and accountability in the use of FRT, highlighting risks such as mass surveillance, data misuse, and algorithmic bias. It argues for a robust regulatory framework that ensures transparency, safeguards civil liberties, and harmonizes technological advancement with human rights principles.

Keywords: right to privacy; human rights; facial recognition technology; surveillance; proportionality principle.

Tecnologia de reconhecimento facial na aplicação da lei: equilibrando segurança e o direito à privacidade

Resumo

A tecnologia de reconhecimento facial emergiu rapidamente como uma ferramenta poderosa na aplicação da lei moderna, permitindo identificação, vigilância e prevenção de crimes de forma eficiente. No entanto, sua ampla implantação suscita preocupações significativas quanto à proteção do direito à privacidade e de outros direitos humanos fundamentais. Este artigo examina a tensão entre os interesses do Estado em garantir a segurança pública e o direito do indivíduo à autodeterminação informacional. Ele analisa criticamente o marco jurídico e constitucional que rege a vigilância, com referência especial ao reconhecimento da privacidade como um direito fundamental no caso Juiz K.S. Puttaswamy contra União da Índia. O estudo explora ainda questões de proporcionalidade, necessidade e prestação de contas no uso da FRT, destacando riscos como vigilância em massa, uso indevido de dados e viés algorítmico. Defende um marco regulatório robusto que garanta transparência, proteja as liberdades civis e harmonize o avanço tecnológico com os princípios dos direitos humanos.

Palavras-chave: direito à privacidade; direitos humanos; tecnologia de reconhecimento facial; vigilância; princípio da proporcionalidade.

* PhD in Law from GD Goenka University, India. Assistant Professor, Maharashtra National Law University, Chhatrapati Sambhajinagar, India. E-mail: ali4823@gmail.com.
https://mnlua.ac.in/faculty/details?title=dr-hifajatali-sayyed https://orcid.org/0000-0001-9472-6950

Received on April 28, 2026, and accepted for publication on August 17, 2026.

Este trabalho está licenciado com uma Licença Creative Commons Attribution 4.0 International License.

La tecnología de reconocimiento facial en las fuerzas del orden: el equilibrio entre la seguridad y el derecho a la intimidad

Resumen

La tecnología de reconocimiento facial se ha convertido rápidamente en una potente herramienta en las fuerzas del orden modernas, ya que permite una identificación, vigilancia y prevención del delito eficaces. Sin embargo, su uso generalizado suscita importantes preocupaciones en relación con la protección del derecho a la intimidad y otros derechos humanos fundamentales. Este artículo examina la tensión entre los intereses del Estado por garantizar la seguridad pública y el derecho de la persona a la autodeterminación informativa. Analiza de forma crítica el marco jurídico y constitucional que regula la vigilancia, con especial referencia al reconocimiento de la privacidad como derecho fundamental en el caso K.S. Puttaswamy contra la Unión de la India. El estudio explora además cuestiones de proporcionalidad, necesidad y rendición de cuentas en el uso de la tecnología de reconocimiento facial, destacando riesgos como la vigilancia masiva, el uso indebido de datos y el sesgo algorítmico. Aboga por un marco regulador sólido que garantice la transparencia, proteja las libertades civiles y armonice el avance tecnológico con los principios de los derechos humanos.

Palabras clave: derecho a la intimidad; derechos humanos; tecnología de reconocimiento facial; vigilancia; princípio de proporcionalidad.

La technologie de reconnaissance faciale dans les forces de l'ordre : concilier sécurité et droit à la vie privée

Résumé

La technologie de reconnaissance faciale s'est rapidement imposée comme un outil puissant dans les forces de l'ordre modernes, permettant une identification, une surveillance et une prévention de la criminalité efficaces. Cependant, son déploiement à grande échelle soulève des préoccupations importantes concernant la protection du droit à la vie privée et d'autres droits humains fondamentaux. Cet article examine la tension entre les intérêts de l'État en matière de sécurité publique et le droit de l'individu à l'autodétermination informationnelle. Il analyse de manière critique le cadre juridique et constitutionnel régissant la surveillance, en se référant notamment à la reconnaissance de la vie privée comme droit fondamental dans l'affaire K.S. Puttaswamy c. Union indienne. L'étude explore en outre les questions de proportionnalité, de nécessité et de responsabilité dans l'utilisation de la reconnaissance faciale, en mettant en évidence des risques tels que la surveillance de masse, l'utilisation abusive des données et les biais algorithmiques. Elle plaide en faveur d'un cadre réglementaire solide qui garantisse la transparence, protège les libertés civiles et concilie le progrès technologique avec les principes des droits de l'homme.

Mots-clés : droit à la vie privée ; droits de l'homme ; technologie de reconnaissance faciale ; surveillance ; principe de proportionnalité.

执法领域的人脸识别技术：平衡安全与隐私权

摘要

人脸识别技术已迅速成为现代执法工作中的有力工具，实现了高效的身份识别、监控及犯罪预防。然而，该技术的广泛应用引发了关于隐私权及其他基本人权保护的重大关切。本文探讨了国家维护公共安全的利益与个人信息自决权之间的张力，并批判性地分析了规制监控活动的法律与宪法框架，特别参考了 “K.S. Puttaswamy 诉印度联邦案” 中关于将隐私权确立为基本权利的裁决。此外，本研究还探讨了人脸识别技术应用中的比例原则、必要性及问责机制问题，重点分析了大规模监控、数据滥用及算法偏见等风险。文章主张建立健全的监管框架，以确保透明度、保障公民自由，并实现技术进步与人权原则的协调统一。

关键词：隐私权；人权；人脸识别技术；监控；比例原则。

Gesichtserkennungstechnologie in der Strafverfolgung: Abwägung zwischen Sicherheit und dem Recht auf Privatsphäre

Zusammenfassung

Die Gesichtserkennungstechnologie hat sich rasch zu einem leistungsstarken Instrument in der modernen Strafverfolgung entwickelt, das eine effiziente Identifizierung, Überwachung und Kriminalprävention ermöglicht. Ihr flächendeckender Einsatz wirft jedoch erhebliche Bedenken hinsichtlich des Schutzes des Rechts auf Privatsphäre und anderer grundlegender Menschenrechte auf. Dieser Beitrag untersucht das Spannungsfeld zwischen staatlichen Interessen an der Gewährleistung der öffentlichen Sicherheit und dem Recht des Einzelnen auf informationelle Selbstbestimmung. Er analysiert kritisch den rechtlichen und verfassungsrechtlichen Rahmen für Überwachungsmaßnahmen, unter besonderer Berücksichtigung der Anerkennung der Privatsphäre als Grundrecht im Fall „Justice K.S. Puttaswamy gegen Union of India“. Die Studie befasst sich ferner mit Fragen der Verhältnismäßigkeit, der Notwendigkeit und der Rechenschaftspflicht beim Einsatz von Gesichtserkennungstechnologie und hebt dabei Risiken wie Massenüberwachung, Datenmissbrauch und algorithmische Verzerrungen hervor. Sie plädiert für einen soliden Rechtsrahmen, der Transparenz gewährleistet, bürgerliche Freiheiten schützt und den technologischen Fortschritt mit den Menschenrechtsgrundsätzen in Einklang bringt.

Schlüsselwörter: Recht auf Privatsphäre; Menschenrechte; Gesichtserkennungstechnologie; Überwachung; Grundsatz der Verhältnismäßigkeit.

Introduction

The rapid advancement of digital technologies has transformed the landscape of criminal justice, particularly in the domain of law enforcement. Among these innovations, Facial Recognition Technology (FRT) has emerged as a powerful tool capable of identifying individuals through biometric analysis of facial features (Gates, 2011). By enabling real-time surveillance, automated identification, and data-driven policing, FRT promises enhanced efficiency in crime prevention, investigation, and national security operations. Governments across the world are increasingly adopting this technology to strengthen public safety frameworks, manage large-scale events, and track criminal activity. However, the deployment of FRT has also generated profound legal and ethical concerns, particularly regarding its implications for the right to privacy and other fundamental human rights. At its core, FRT operates by capturing an image or video of an individual’s face, extracting unique biometric markers, and comparing them against databases for identification or verification. While this process appears technologically sophisticated and beneficial, it raises critical questions about consent, transparency, and the potential for misuse. Unlike traditional surveillance methods, FRT enables mass, continuous, and often invisible monitoring of individuals in public and private spaces. This capability significantly alters the relationship between the state and the individual, introducing the possibility of pervasive surveillance that may infringe upon civil liberties.

The right to privacy has been recognized as a fundamental human right under international legal frameworks, including the International Covenant on Civil and Political Rights, which protects individuals against arbitrary or unlawful interference with their

privacy. In the Indian context, the landmark judgment in Justice K.S. Puttaswamy v. Union of India (2018) firmly established privacy as an intrinsic part of the right to life and personal liberty under Article 21 of the Constitution. This recognition imposes a constitutional obligation on the state to ensure that any intrusion into privacy is lawful, necessary, and proportionate. The use of FRT by law enforcement agencies must therefore be evaluated against these constitutional standards to determine its legitimacy. Despite its potential advantages, FRT presents several challenges that complicate its integration into legal systems (Jensen; White; Cuomo, 2020). One of the primary concerns is the risk of mass surveillance, where individuals are monitored without their knowledge or consent, leading to a chilling effect on freedoms such as expression and assembly. The possibility that citizens may be constantly watched can deter participation in democratic activities, including protests and public gatherings. Additionally, the lack of clear and comprehensive regulatory frameworks governing the use of FRT exacerbates these concerns, as it creates opportunities for arbitrary or excessive state action.

Another significant issue is the question of accuracy and bias in facial recognition systems. Empirical studies have shown that such technologies may exhibit higher error rates when identifying individuals from certain demographic groups, particularly along lines of race, gender, and age (Paik *et al.*, 2025). These inaccuracies can result in wrongful identification, unjust arrests, and violations of due process rights. In a criminal justice system that relies on fairness and equality before the law, the integration of potentially biased technology raises serious human rights implications. The use of FRT raises concerns about data protection and security. The collection and storage of biometric data create risks of unauthorized access, data breaches, and misuse by both state and non-state actors. Unlike passwords or identification numbers, biometric identifiers such as facial features cannot be easily altered, making individuals particularly vulnerable in the event of a data compromise. This underscores the need for stringent data protection measures and accountability mechanisms to safeguard personal information.

In balancing the benefits and risks of FRT, the principle of proportionality assumes central importance. Any restriction on fundamental rights must be justified by a legitimate state aim, such as public safety, and must be the least restrictive means available to achieve that aim. The deployment of FRT must therefore be carefully calibrated to ensure that it does not result in excessive or unjustified intrusion into individual freedoms. This requires not only a robust legal framework but also effective oversight and transparency in its implementation. This paper seeks to critically examine the use of Facial Recognition Technology in law enforcement through the lens of human rights and constitutional law. It explores whether the

current legal frameworks are adequate to address the challenges posed by FRT and evaluates the extent to which its use can be justified within the boundaries of the right to privacy. By analyzing legal principles, judicial precedents, and comparative approaches, the study aims to contribute to the ongoing discourse on how to reconcile technological innovation with the protection of fundamental rights in a democratic society.

Methodology

This study adopts a doctrinal legal research methodology, a well-established and authoritative approach within legal scholarship. The doctrinal method is particularly suited to the systematic examination of legal principles, statutory provisions, judicial precedents, and academic commentary, thereby providing a strong analytical foundation for understanding the existing legal framework. In the present research, this methodology is employed to critically evaluate the legal foundations and policy implications of Facial Recognition Technology in law enforcement, with particular emphasis on the tension between public security and the right to privacy. The research involves a comprehensive analysis of both primary and secondary sources. Primary sources include constitutional provisions, statutory frameworks, and judicial decisions, most notably the recognition of privacy as a fundamental right in Justice K.S. Puttaswamy v. Union of India, as well as relevant international human rights instruments such as the International Covenant on Civil and Political Rights. Secondary sources, including peer-reviewed journal articles, scholarly books, and policy reports, are used to contextualize and critically assess the application of these legal principles. Through careful interpretation and synthesis of these materials, the study identifies key doctrinal developments, emerging trends, and regulatory gaps concerning the use of FRT. The doctrinal approach further facilitates a comparative analysis of legal frameworks across jurisdictions, enabling an evaluation of how different legal systems address the challenges posed by biometric surveillance technologies. It highlights how courts and legislatures attempt to balance individual rights with collective security concerns, and how these efforts align with international human rights standards. Proper citation practices are maintained throughout to ensure academic integrity and to acknowledge prior scholarship. Overall, this methodology enables a structured and nuanced exploration of the legal landscape surrounding FRT, offering insights into how its use can be regulated in a manner that upholds constitutional guarantees and human rights norms. The findings aim to contribute to ongoing debates on surveillance, privacy, and

criminal justice reform, while also informing future legal and policy development in this rapidly evolving area.

Results and Discussions

The Security Mandate

The argument for Facial Recognition Technology in law enforcement is built upon the premise that in an era of globalized crime and rapid urbanization, traditional policing methods are no longer sufficient. Law enforcement agencies characterize FRT as a “force multiplier”, a technological advancement that drastically enhances the speed, scale, and accuracy of human efforts. By automating the process of scanning thousands of faces against established databases, FRT allows a lean police force to monitor vast areas and process mountains of digital evidence that would otherwise take months of manual labor to review (Reedy, 2023). This efficiency is not merely a matter of convenience; proponents argue it is a vital necessity for maintaining the social contract of public safety. In the realm of criminal investigation, FRT has revolutionized the utility of “cold case” files and post-incident analysis. Before the widespread adoption of biometric software, investigators had to rely on eyewitness testimony, notoriously unreliable, or manually scrub through thousands of hours of grainy CCTV footage. Today, FRT can digitize a suspect's features from a single frame and cross-reference them against national criminal records or driver's license databases in seconds. This capability is particularly transformative for “cold cases” where physical evidence may have degraded but visual records remain. By identifying a suspect who was previously just a “blur on a screen,” FRT provides the breakthrough needed to bring closure to victims of violent crimes who have waited years for justice. The “Pro” case for FRT is perhaps most visible in the context of proactive public safety at high-risk events. Large-scale gatherings, such as the World Cup, political inaugurations, or major festivals, present “soft targets” for terrorism and organized violence. Law enforcement agencies utilize real-time FRT to scan crowds against “watchlists” of known violent offenders or individuals with active warrants. This allows for a “surgical” approach to security: instead of intrusive, blanket stop-and-search tactics that affect every citizen, police can discretely identify and intercept specific threats before an incident occurs. Proponents argue that this targeted surveillance actually preserves the liberty of the law-abiding majority by preventing mass-casualty events while minimizing the need for heavy-handed, visible policing (Levine, 2016).

Beyond the pursuit of criminals, FRT serves a humanitarian purpose in victim identification and emergency response. In cases of human trafficking, victims are often moved rapidly across borders and through transit hubs under aliases. FRT enables agencies to scan these hubs for missing persons reports, often identifying children or vulnerable adults who are unable to seek help themselves. Similarly, in medical emergencies involving non-responsive individuals or those suffering from dementia who have wandered away from home, FRT provides a non-invasive way to establish identity. When every minute counts in a trauma ward or a missing child case, the ability to instantly link a face to a medical history or a home address is a life-saving application that transcends the typical "police vs. privacy" debate. Furthermore, the integration of FRT into law enforcement is defended as an equalizer against the increasing sophistication of modern criminals. As bad actors utilize encrypted communications and deepfake technologies to obscure their identities, the state argues that it must be equipped with equally sophisticated biometric tools to maintain "deterrence equilibrium." The mere presence of FRT in high-security zones acts as a psychological deterrent, making it significantly harder for known fugitives to operate in the shadows of public life. For law enforcement, the "Security Mandate" is clear: FRT is an essential evolution of the fingerprint and the mugshot, modernized for a digital world where safety depends on the ability to identify a needle in a haystack of millions.

The Privacy and Human Rights Challenge

The widespread adoption of Facial Recognition Technology introduces a profound set of "human rights friction points" that challenge the very foundations of democratic societies. While privacy is the most immediate concern, the implications extend far deeper, threatening the fundamental tenets of liberty, equality, and personal security. Opponents of unregulated FRT argue that the technology transforms the nature of public space from a venue of free movement into a digital "panopticon," where every action is recorded, analyzed, and permanent. A primary concern is the "chilling effect" that ubiquitous FRT has on the Freedom of Assembly and Expression. When individuals know that their faces are being scanned and cross-referenced against government databases in real-time, their behavior changes. The anonymity historically afforded by a crowd, a crucial protection for whistleblowers, political dissidents, and marginalized groups, evaporates. If participation in a peaceful protest or a controversial political gathering carries the risk of being permanently tagged in a "police watchlist," many will choose to stay home. This invisible

barrier to civic engagement effectively suppresses dissent without the need for physical force, fundamentally altering the relationship between the state and the citizen.

Beyond the threat to expression, FRT is plagued by the systemic issue of Algorithmic Bias, which directly undermines the Right to Equality. Numerous studies, most notably from the National Institute of Standards and Technology (NIST), have demonstrated that many facial recognition algorithms exhibit significantly higher error rates when identifying women, youth, and people of color. These “demographic differentials” are often the result of biased training datasets or flawed mathematical modeling. In a law enforcement context, these technical failures translate into real-world harm: wrongful arrests, invasive interrogations, and the disproportionate targeting of minority communities. When a technology is inherently less accurate for certain groups, its use by the state becomes a form of systemic discrimination that violates the principle of equal protection under the law (Jones, 2022). Finally, the challenge of Data Permanence creates a unique and irreversible security risk that distinguishes biometrics from any other form of identification. Unlike a password or a credit card number, which can be changed or reset if compromised, a “face print” (the biometric template derived from your features) is a permanent part of your identity. If a centralized law enforcement database or a private vendor is breached, the affected individuals face a lifelong vulnerability. Their most intimate biological data becomes available on the dark web, potentially enabling identity theft or unauthorized tracking that can never be fully mitigated. This permanence transforms a temporary security breach into a permanent human rights liability, casting a long shadow over the future of personal autonomy in a digital world.

Legal & Regulatory Frameworks

The establishment of a robust legal and regulatory framework is essential to ensure that the deployment of Facial Recognition Technology does not outpace the protection of fundamental human rights. As of 2026, the global legal landscape has transitioned from a “wild west” of unregulated experimentation to a sophisticated, tiered system of governance. Central to this evolution is the European Union AI Act, which has become the global benchmark for biometric regulation. By categorizing “Real-time Remote Biometric Identification” in publicly accessible spaces as an inherently “High-Risk” or, in many cases, “Prohibited” activity, the Act sets a high bar for state intervention. Under this framework, law enforcement can only bypass these prohibitions for strictly defined objectives, such as searching for a victim of abduction or preventing a specific, substantial, and imminent

terrorist threat, and even then, only with prior judicial or administrative authorization. On a domestic level, nations are increasingly developing specialized legislation to fill the gaps left by general data protection rules (Luiz; Pires; Lisboa, 2026). In the United Kingdom, the governance of FRT has historically relied on a patchwork of the Data Protection Act 2018 and the guidelines issued by the Biometrics and Surveillance Camera Commissioner. These guidelines emphasize that the "policing by consent" model requires clear, accessible legal codes rather than internal police policies. Conversely, in India, the Digital Personal Data Protection (DPDP) Act of 2023 provides a different approach, focusing on the processing of digital personal data and providing certain exemptions for state agencies in the interest of national security and public order. The challenge for these domestic laws remains the "function creep", where technology introduced for extreme circumstances slowly becomes a tool for routine surveillance.

The practical boundaries of these laws are often defined not in parliaments, but in the courtroom through landmark Judicial Precedents. One of the most influential cases globally is Bridges v. South Wales Police. In this instance, the Court of Appeal in the UK ruled that the police force's use of automated facial recognition was unlawful because there was "too much discretion" left to individual officers regarding who could be put on a watchlist and where the technology could be deployed. This ruling established a critical legal principle: for FRT use to be "in accordance with the law," the legal framework must be specific enough to give citizens an indication of the circumstances in which they might be scanned. Ultimately, these frameworks are moving toward a "Privacy by Design" requirement, where technical safeguards are mandated by law before a single camera is switched on. This includes requirements for Data Protection Impact Assessments (DPIAs) and mandatory sunset clauses that require the deletion of biometric data after a set period if no match is found. By synthesizing international regulations like the EU AI Act with domestic statutes and judicial oversight, the goal is to create a predictable legal environment where the "Security Mandate" can coexist with the "Right to Privacy" without one completely eclipsing the other.

Proposed Safeguards

To bridge the gap between state security and individual liberty, a "Gold Standard" framework for Facial Recognition Technology (FRT) must move beyond vague promises of ethical use toward concrete, enforceable safeguards. The first pillar of this balance is the Strict Necessity Test. This principle dictates that FRT is not a general-purpose tool for

routine policing but a specialized instrument reserved for the most “high-stakes” scenarios. By legally restricting its application to serious crimes, such as counter-terrorism, human trafficking, or the search for missing children, authorities can prevent the “mission creep” that leads to the surveillance of petty crimes like jaywalking or minor vandalism. This ensures that the intrusion into public privacy is always commensurate with the gravity of the threat. The second essential safeguard is the requirement for Independent Oversight, specifically through a judicial warrant process. As of 2026, many legal scholars argue that the deployment of live facial recognition should be treated with the same legal scrutiny as a wiretap or a physical search of a home (Jawahitha, 2022). Mandating that law enforcement obtain a warrant from an independent judge before activating FRT in a public space provides a critical check on executive power. This process forces agencies to demonstrate “probable cause” or a specific investigative need, ensuring that mass surveillance is not conducted on a whim or for generalized monitoring without a targeted objective.

A “Gold Standard” framework must eliminate the risk of “automation bias” through a mandatory Human-in-the-Loop requirement. This is a legal safeguard ensuring that no arrest, detention, or formal accusation can be made based solely on an algorithmic “match.” AI is a tool of suggestion, not a final arbiter of truth. By requiring a human officer, trained in forensic facial identification, to manually verify and sign off on a match before any action is taken, the system preserves human accountability. This layer of verification acts as a vital safety net against technical glitches or the demographic biases that often plague biometric software. Finally, the framework is anchored by Transparency and Auditing. To maintain public trust, law enforcement agencies should maintain publicly accessible logs detailing when, where, and why FRT was deployed, as well as the outcomes of those deployments. This transparency is bolstered by periodic, mandatory third-party audits of the algorithms themselves. These audits test for accuracy and bias across different ethnicities and genders, ensuring that the technology remains “fit for purpose” and does not violate the Right to Equality. By making the “black box” of biometric policing visible to the public and the courts, the state can demonstrate that its search for security does not come at the hidden cost of fundamental human rights.

Conclusion

The evolution of Facial Recognition Technology represents one of the most significant shifts in the history of criminal justice, marking the transition from traditional reactive policing to a proactive, data-driven era. As we have explored, the “Security

Mandate" offers undeniable benefits in identifying fugitives and protecting the vulnerable. However, these gains cannot be viewed in isolation from the "Privacy Challenge," where the risks of systemic bias, the erosion of anonymous assembly, and the permanence of biometric data pose a legitimate threat to the democratic social contract. The tension between these two poles is not a problem to be solved once, but a balance that must be constantly recalibrated as technology advances. The path forward lies in the transition from "possibility" to "proportionality." The mere fact that a technology can scan a crowd does not mean the law should permit it without rigorous justification (Monika; Giulia, 2025). The emerging global consensus, led by frameworks like the EU AI Act and reinforced by judicial precedents, suggests that the future of FRT is not in mass surveillance, but in targeted, transparent, and judicially overseen applications. By embedding "Human-in-the-Loop" requirements and strict necessity tests into the heart of penal codes, society can harness the investigative power of biometrics while insulating citizens from the specter of digital authoritarianism.

Ultimately, the goal of modern criminal law is to ensure that the tools used to protect the public do not inadvertently dismantle the very freedoms they are meant to defend. As we move deeper into 2026 and beyond, the success of FRT in law enforcement will not be measured by the number of matches it generates, but by the strength of the safeguards that govern it. True security in a digital age is found only when the state's "eye" is matched by the citizen's "shield," ensuring that the right to walk through a public square remains a free and private act.

How to cite this article:

ABNT

SAYYED, Hifajatali. Facial recognition technology in law enforcement: balancing security and the right to privacy. *Passagens rev. int. hist. pol. e cult. jur.*, Niterói, v. 18, n. 3, p. 471-482, Sept.-Dec. 2026. https://doi.org/10.15175/dcmy3d24

APA

Sayyed, H. (2026). Facial recognition technology in law enforcement: balancing security and the right to privacy. *Passagens rev. int. hist. pol. e cult. jur.*, *18*(3), 471-482. https://doi.org/10.15175/dcmy3d24

Copyright:

Copyright © 2026 Author. This is an open access article distributed under the Creative Commons Attribution License which permits unrestricted use, distribution, and reproduction in any medium, provided the original article is properly cited.

Publisher responsible for the evaluation process:

Gizlene Neder

References

GATES, Kelly A. *Our biometric future*: facial recognition technology and the culture of surveillance. New York: NYU Press, 2011. https://www.jstor.org/stable/j.ctt9qg8xd

JENSEN, Benjamin M.; WHYTE, Christopher; CUOMO, Scott. Algorithms at war: the promise, peril, and limits of artificial intelligence. *International Studies Review*, v. 22, n. 3, p. 526-550, 2020. https://www.jstor.org/stable/48590664. Accessed on: 21 Mar. 2026.

PAIK, Sejin *et al*. Who benefits from AI? Examining different demographics' fairness perceptions across personal, work, and public life. *Discov Artif Intell*, v. 5, art. 39, 2025. https://doi.org/10.1007/s44163-025-00235-7

REEDY, Paul. Interpol review of digital evidence for 2019-2022. *Forensic Sci Int Synerg*., v. 6, 100313, 2023. https://doi.org/10.1016/j.fsisyn.2022.100313

LEVINE, Kate. Police Suspects. *Columbia Law Review*, v. 116, n. 5, p. 1197-1258, 2016. http://www.jstor.org/stable/43783403. Accessed on: 12 Apr. 2026.

JONES, Colin Clemente. Systematizing discrimination: AI vendors & Title VII enforcement. *University of Pennsylvania Law Review*, v. 171, n. 1, p. 235-266, 2022. http://www.jstor.org/stable/45476496. Accessed on: 28 Apr. 2026.

LUIZ, Stephany Holanda-Filho, PIRES, João Pedro Prado Benevides; LISBOA, Rafaela Ponte. Similarities and singularities of the data protection laws of the south American countries. *Computer Law & Security Review*, v 61, 106308, 2026. https://doi.org/10.1016/j.clsr.2026.106308.

JAWAHITHA, Sarabdeen. Protection of the rights of the individual when using facial recognition technology. *Heliyon*, v. 8, n. 3, e09086, 2022. https://doi.org/10.1016/j.heliyon.2022.e09086.

MONIKA Simmler, GIULIA Canova. Facial recognition technology in law enforcement: regulating data analysis of another kind. *Computer Law & Security Review*, v. 56, 106092, 2025. https://doi.org/10.1016/j.clsr.2024.106092.