

**FACIAL RECOGNITION TECHNOLOGY AND THE RIGHT
TO PRIVACY IN INDIA: A CONSTITUTIONAL AND REGULATORY
ANALYSIS**

by

M. RAGA ROSHINI

S. THANGAPAZHAM LAW COLLEGE, TAMILNADU

ABSTRACT

Ripe at the confluence of Indian State jurisprudential discourse lies the at once closed-presence and beleaguered occupant of the right to the individual, Privacy, now sewn to the relentless advance of Facial Recognition Technology (FRT). Whether deployed by sovereign police, a municipal surveillance net, the doctrinal stitch seems to unravel further as rolls, performs, and repositions the individual profile of every domestic dweller. The surveillance apparatus burgeons beyond the premises of ‘binomial consent’ or ‘security necessity’ as magnitudes of biometric detail relax into both vendor engine and State archive, fastening the broader tableau of data-handling, earlier drawn only from handwriting and testimony, to a permanence once accorded sacred relic. The pursuit offered here entwines what the law adroitly terms ‘intrinsic spin-offs’ of the jurisprudential oeuvre since 1950, obliges the text to process every dash of precedential script upon the disguised visage, and re-examines article sovereign lies re-constructed in such casually minted permanence of facial tiles. This paper home in on the constitutional foundations of privacy as elaborated in the landmark judgment of Justice K.S. Puttaswamy (Retd.) V. Union of India (2017), where the Supreme Court squarely held that the primarily on constitutional right to privacy: the Aadhaar validity case was decided separately

in 2018. The ruling requires that any encroachment on privacy must be justified by a law that is just, fair and reasonable, underlining the necessity of strict safeguards when deploying intrusive technologies such as facial recognition. The absence of binding and coherent legislation has created a regulatory vacuum, further complicated by the fragmented schema of the Information Technology Act, the narrow provisions of the Aadhaar Act, and various advisory frameworks that government bodies have offered on a non-mandatory basis.

Keywords: Face Recognition, technology, privacy, digital, fundamental rights, regulatory framework.

INTRODUCTION

The accelerated spread of facial recognition technology has reshaped the way identification and surveillance functions both in India and abroad. Within India, the technology is being pressed into service for public order, police investigations, and any number of routine administrative tasks, yet none of these deployments is matched by a dedicated privacy law. Such a discrepancy invites considerable doubt about safeguarding the privacy afforded, absent explicit limitations, by the Constitution's Article 21. The Court's authoritative ruling in *K.S. Puttaswamy (Retd.)* (2017) asserts privacy as an unequivocal constitutional entitlement, establishing an obligatory threshold any surveillance method must respect. Yet a continuing absence of any statutory scheme applying specifically to facial recognition has invited vague authorization and consequential rights risks.

Facial recognition technology has become a cornerstone biometric tool driving identity proofing, crime deterrence, and administrative efficiency on a global scale. In India, integration is broad, encompassing police archives, immigration desks, public-space safety cameras, online banking checks, and a swift onward march into retail and app-based services. The pace, while disruptive, has also prompted loud societal pushback, spotlighting encroaching privacy limits, the specter of unchecked tracking, the specter of vulnerability to profiling, and a glaring absence of transparent oversight and grievance channels. Final figures are sobering: more than "170 city-wide systems" and ₹15,000 crore expenditure. The spending and the stakes clearly position of facial recognition technology as a nonnegotiable fixture in the nation's digital posture.

The Internet Freedom Foundation's Project Panoptic initiative, launched in 2020, had by 2024 documented more than 120 government contracts for facial recognition technology across India, constituting the most comprehensive public database of such deployments in the country. A 2024 analysis published by the Software Freedom Law Centre India (SFLC.in) recorded 126 operational and tendered FRT systems as of June 2023, with a combined government outlay of INR 1,499.41 crore, illustrating the pace at which public resources are being committed to biometric surveillance infrastructure in the absence of any dedicated statutory framework to govern collection, use, or long-term storage of the facial data so acquired.¹

This Article undertakes a thorough constitutional and regulatory examination of Face Recognition Technologies as deployed within the Indian state. The analysis opens by mapping the privacy right as construed by the Court, and then chronicles the technology's nature, capability, and the latent societal shifts it produces. Next, it critiques the present regulatory mosaic, (part statutory, part administrative, and part informal) and appraises whether fragmentary modules, absent explicit direction, furnish adequate privacy shielding. The Article then skirts domestic precedent to test lessons emerging elsewhere, reflecting comparative regimes that likewise confront biometrically-enabled surveillance. The discourse completes by exposing normative and ethical contingencies that the technology raises and by identification of concrete legal and administrative advances inscribed within applicable constitutional norms that the state ought to pursue to orient the persistent and domestic evolving deployment towards a privacy centric posture².

Beyond a close review of domestic statutes, this study situates India's regulatory profile within the unfolding global conversation on facial recognition technology by cross-examining more mature approaches in the European Union, which operationalizes granular data protection norms through the General Data Protection Regulation, and in the United States, lively and mosaic debates on facial recognition regulation advance in patchwork state legislation. The comparative perspective demonstrates that, despite commendable pronouncements on the sanctity of privacy, India's legislative apparatus remains deficient in tethering facial recognition operations through precise,

Internet Freedom Foundation, 'Project Panoptic' (panoptic.in, 2024) <<https://panoptic.in/about>> accessed 28 August 2026; SFLC.in, 'Deployment of Facial Recognition Technology for State Surveillance and Monitoring' (sflc.in, November 2024) <<https://sflc.in/deployment-of-facial-recognition-technology-for-state-surveillance-and-monitoring/>> accessed 28 August 2026.

enforceable, and transparent prescriptions governing collection, retention, onward sharing, and final deletion of biometric records.

The present analysis also interrogates layered ethical and socio-political dilemmas generated by facial recognition technologies. Addressing algorithmic disadvantage, heightened error rates for marginalized demographics, systemic deficits in meaningful consent, and the insidious fog over civic freedoms, the scrutiny reveals the amplification of harm when vast state-sponsored scrutiny is conducted in the name of national security and public order. The section concludes by cautioning that the deployment of facial recognition technology, when characterized by opacity and lack of legitimate oversight, risks sidestepping the proportionality required to protect rights and the rule of law.

This analysis therefore urges the Indian legislature and relevant regulators to act without delay. Key actions include enacting a standalone law on biometric data, expressly covering facial recognition and related systems; stipulating mandatory privacy and risk impact assessments, followed by systematic audits; creating genuinely independent oversight bodies to enforce accountability; and requiring adoption of strict purpose limitation, data minimization, and clear informed-consent norms. Beyond the statutory measures, enhanced public literacy programs and authentic participatory governance forums are essential to prevent emergent technologies from undermining constitutional guarantees.³

1.METHODOLOGY

Methodology synthesizes principles from artificial intelligence, computer vision, and machine learning, constructing a biometric template by mapping distinctive landmarks such as interocular distance, nasal morphology, and mandible contour into a numerically encoded representation.

Current implementations of facial recognition technology proceed through a sequence of stages: detection, geometric alignment, feature extraction, and comparative matching. Initially, the detection algorithm identifies one or more face candidates within the visual data; subsequent

² Hodge, S. D. Jr. (2022). The legal and ethical considerations of facial recognition technology in the business sector. *DePaul Law Review*, 71(3), 731-763.

³ Dul, C. (2022). Facial recognition technology vs privacy: The case of Clearview AI. *Queen Mary Law Journal*, 2022, 1-24.

alignment rectifies angular deviation, spatial scale, and aspect ratio. During feature extraction, these rectified images are translated into a high-dimensional numerical vector; the matching component then conducts a rapid query against a reference gallery to yield an identity or confirmation of a subject. Notable enhancements in accuracy have emerged from the application of convolutional and recurrent deep neural networks, which exhibit robustness to heterogeneous lighting, non-frontal head poses, and obstructive elements.

Facial recognition technology deployment encompasses diverse domains, including mobile device authentication, financial transaction approval, and tactical operations within policing, immigration control, and urban surveillance. In the Indian context, the technology is frequently coupled with complementary biometric modalities such as fingerprint and iris data within the expansive biometric infrastructure of the Aadhaar initiative and concurrent public safety programmed.

Nonetheless, face recognition technology remains constrained by inherent technical deficiencies, famously manifesting as elevated rates of error and systematic bias. Empirical research consistently shows that prevailing recognition algorithms underperform with respect to female subjects, racial and ethnic minorities, and pediatric populations, thereby amplifying anxieties surrounding procedural fairness and discriminatory harm. Concurrently, the architecture of these systems remains exposed to spoofing—whereby photographed or video images deceive sensors—and to adversarial perturbations engineered to mislead classifiers, undermining the expected reliability of output. Motivated by the pressing imperatives of state and commercial surveillance, the diffusion of face recognition persists, generating continuing, contentious discourse surrounding the ordeal of harmonizing rapid technological advancement with guarantee of foundational rights.

2. BACKGROUND AND CONTEXT

Facial Recognition Technology (FRT) serves as a rapidly evolving biometric method by which individuals can be automatically identified or verified through analysis of their distinctive facial traits. Tracing its origins to early experiments in the 1960s, the discipline has, since the early 2000s, reached maturity evidenced by widespread global deployment, a leap made possible by breakthroughs in artificial intelligence, machine learning, and computer vision. Today, its uses extend to diverse domains including public safety, financial services, immigration, healthcare administration, and a wide array of commercial operations.

In the Indian context, robust large-scale deployment of face recognition technology commenced in the latter part of the 2010s and tracked closely with the comprehensive introduction of Aadhaar, the biometric universal identification framework. While second-generation Aadhaar architecture predominantly centre on fingerprint and iris biometric capture, the Unique Identification Authority of India (UIDAI) in 2018 convened stakeholder discussions aimed at integrating facial-recognition capability as an additional authentication tier. The stated objective was to mitigate instances of biometric failure or mismatch. Beyond government circles, Indian telecom companies quickly began evaluating face recognition technology for identity assurance in SIM activation and consumer onboarding, underscoring the technology's emergent utility for identity verification and regulatory Know Your Customer (KYC) obligations.

From 2019 onward, government uptake of facial recognition technology accelerated, beginning when the National Crime Records Bureau (NCRB) revealed plans for a national, centralized Automated Facial Recognition System (AFRS). Designed as an analytical lever for police, the AFRS sought to assemble a uniform national photo bank by pooling images from civil-service records – passports, criminal justice, and child-nutrition files – to quicken the pace of criminal identification. The scheme initially promised to curtail real-time monitoring by asserting limits on CCTV linkage. Yet civil society probes and public discourse soon exposed fears of an uncharted trajectory toward virtual monitoring on a national scale and the attendant hazards of an all-encompassing data architecture. Privacy, consent, and surveillance architecture inherited from indefinite state oversight now converged in one algorithmic thread.⁴

Regional and municipal administrations did not linger. Telangana, Punjab, Uttar Pradesh, Delhi, Maharashtra, and Tamil Nadu were prominent among a wider cohort that layered facial recognition tools onto police mobile and desktop systems. In fact, these efforts are not standalone ventures; they nest inside expansive digital policing reform bundles such as the Crime and Criminal Tracking Network and Systems (CCTNS), which continuously furnish a scaffolding for biometric data among the nation's 38,000-strong police-import infrastructure. Despite the rapid rollout, the technology grapples with hurdles of admissible accuracy and systemic fairness: reports show a precarious rise in misidentifications, the reckless amplification of algorithmic prejudice, and an

4Jauhar, A., & Vipra, J. (2022). Addressing constitutional challenges in use of facial recognition technology by Indian law enforcement. *Jurist Commentary*.

inequitable dragnet effect on poor, marginalized, and youth populations yet still crowded out of protective legal infrastructures.

The vulnerability of unregulated biometric archives to security failures is not merely hypothetical. On 3 May 2024, the Tamil Nadu Police Facial Recognition Portal was breached by a threat actor, resulting in the exposure of more than 800,000 lines of data, including the facial biometric profiles, FIR details, and personal contact information of approximately 50,000 accused and suspected persons, with the stolen data subsequently offered for sale on dark web forums. The Internet Freedom Foundation noted that the breach exposed the absence of mandatory security audits and any enforceable data-handling standards governing police-operated facial recognition systems, calling for an immediate cessation of unregulated police use of the technology pending the introduction of proper legislative safeguards.⁵

India's shifting landscape of facial recognition technology unfolds against a legal and regulatory backcloth that remains riddled with unanswered questions. The 2017 Puttaswamy judgment from the Supreme Court confirmed, with finality, that the right to privacy sits squarely within the contours of Article 21, thus conferring a robust constitutional guarantee against unwarranted intrusions. Nevertheless, the country still proceeds without a cohesive data-protection law that explicitly enunciates obligations tied to the peculiar risks posed by facial recognition systems. Respective statutes the Information Technology Act, the 2016 Aadhaar Act, and a variety of prescriptive notes scattered across criminal sectors contain imprecise provisions on consent, governance of biometric archives, and limitations on data repurposing, collectively leaving the legal architecture the equivalent of a jigsaw with missing pieces.

The resultant deficiency has sparked sustained agitation surrounding the thresholds of legality, necessity, and oversight that are constitutionally mandated whenever the State, or indeed a private actor, resorts to facial recognition. Advocacy groups, privacy scholars, and informed jurists repeatedly highlight the operational dangers of concealed authorization, the risks posed by indefinite data retention, creeping illicit mission expansion, and the broader specter of

Medianama, 'Tamil Nadu Police Facial Recognition Portal Data Breach Exposes Over 50,000 Users' Details' (Medianama, 6 May 2024) <<https://www.medianama.com/2024/05/223-tamil-nadu-police-facial-recognition-portal-data-breach-exposes-over-50000-users-details/>> accessed 28 August 2026; Internet Freedom Foundation, 'Why a Massive Leak in Tamil Nadu Police's FRT Database Must Herald the End of Police Use of Surveillance Technologies' (internetfreedom.in, 17 May 2024) <<https://internetfreedom.in/leak-in-tamil-nadu-polices-frt-database/>> accessed 28 August 2026.

discriminatory targeting. The Indian jurisprudential recognition of a constitutional right to privacy attained definitive clarity with the unanimous exposition of the Supreme Court in Justice

K.S. Puttaswamy (Retd.) vs. Union of India (2017). By vacating its erstwhile stance which categorically denied privacy the status of a fundamental right the Court fortified the position that privacy is embedded within

the right to life and personal liberty articulated in Article 21. Delivered by a nine-judge constitutional bench, the ruling elucidated that the reach of privacy extends to a spectrum of constituent liberties: informational privacy, decisional autonomy, corporeal integrity, and the safeguarding of the individual against ad hoc, unwarranted incursions by state agents.

Beyond substantive categorization, the Puttaswamy exposition animated privacy with an intrinsic link to the constitutional concept of human dignity, individual autonomy, and the expansive capacity to make free, inviolable life choices. The bench proclaimed that no encroachment upon the right to privacy shall survive unless the challenged measure satisfies the tripartite benchmarks of legality, necessity, and proportionality innovation in terms of which any lesser standard seriatim renders the encroachment unconstitutional. By institutionalizing that precise metric, the Court erected a structured bulwark against arbitrary surrenders of personal liberty and against expansive, falling intrusion by state power.

The litigation concerned the Aadhaar biometric identification initiative, where applicants contest mass data capture, absence of informed consent, and surveillance dangers. The constitutional bench, in the Puttaswamy verdict, reaffirmed the imperative of protecting informational privacy, asserting that privacy entitlements encompass digital artefacts and new technology scenarios.⁶

The judgment now constitutes a reference point for privacy jurisprudence and for framing data governance in the country. Subsequent bench rulings on issues of sexual orientation, reproductive freedoms, and free expression have invoked the judgment as a guarantee of dignity. Nevertheless, a comprehensive data protection statute remains absent, and the legal and institutional framework

Purshouse, J. (2019). Privacy, crime control and police use of automated facial recognition. *Journal of Law and Society*, 46(4), 581-610.

for regulating biometric instruments especially Facial Recognition Technologies—continues to be incomplete and inadequately enforced.

The Puttaswamy ruling therefore offers a constitutional lens for assessing and contesting facial recognition claims, marking the decisive need for a binding legislative and doctrinal apparatus that reconciles the iteration of automated surveillance with established privacy entitlements. Enactment of these measures will avert the incremental, unchecked enclosure of privacy under the justified categorical of the public, and will re-establish privacy as a positive, actionable, and uplifted normative requirement.

4. LEGAL AND REGULATORY FRAMEWORK GOVERNING FRT IN INDIA

The deployment and regulation of Facial Recognition Technology (FRT) in India occur amidst a piecemeal and fragmented legislative environment. While the Supreme Court recognized privacy as a fundamental right in the Puttaswamy (2017) case, India lacks a dedicated, comprehensive data protection framework explicitly addressing biometric data and facial recognition technologies.

The principal laws and policies that implicitly govern aspects of face recognition technology use include the Information Technology Act, 2000 and its associated Rules, the Aadhaar (Targeted Delivery of Financial and other Subsidies, Benefits and Services) Act, 2016, and voluntary guidelines issued by various government agencies. The Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011, define biometric data as sensitive personal data, necessitating certain safeguards. However, these rules often fall short in providing clear procedural mechanisms for consent, purpose limitation, and data minimization pertinent to face recognition technology.

Aadhaar, India's biometric identity system, is the single largest biometric database, incorporating fingerprints, iris scans, and facial images. The Aadhaar Act provides biometric data protection norms, but the Supreme Court has imposed strict limits on the use of Aadhaar data, particularly ensuring it cannot be used for mass surveillance or unauthorized profiling. The use of facial recognition beyond Aadhaar, such as by police departments or private entities, remains far less regulated.

In 2023, India enacted the Digital Personal Data Protection (DPDP) Act, which introduces safeguards around personal data processing aligned with constitutional privacy rights. Although

this law marks progress, it currently does not explicitly address biometric data or specify detailed norms for FRT systems. Consequently, ambiguity and regulatory gaps persist.

A structural gap in the Digital Personal Data Protection Act, 2023 that directly affects the regulation of facial recognition systems is its departure from the tiered model adopted by the European Union's General Data Protection Regulation, which designates biometric data used for the purpose of uniquely identifying individuals as 'special category data' subject to a presumptive processing prohibition. The DPDP Act instead applies a uniform, single-tier consent framework to all personal data regardless of its sensitivity, without recognising biometric information as a distinct category warranting heightened protection. Legal commentators have further noted that the Act's broad exemptions for government processing related to national security and public order effectively insulate police-operated facial recognition systems from the statute's consent and purpose-limitation requirements, leaving such deployments subject only to the constitutional proportionality standard articulated in *Puttaswamy*, with no dedicated statutory rules to operationalise that standard in the biometric context.⁷

India is also a signatory to international human rights conventions which bolster the normative framework for privacy and data protection, influencing domestic discourse. Overall, India's regulatory framework is characterized by sectoral rules, judicial pronouncements, and policy guidelines but lacks a unified statute expressly regulating facial recognition technology necessitating urgent legislative reforms.

5. ANALYSIS OF PRIVACY CONCERNS AND CONSTITUTIONAL ISSUES

The fast-spreading use of Facial Recognition Technology (FRT) across India poses huge worries about privacy. Its design enables constant, large-scale watching of citizens, threatening both the danger of personal information falling into the wrong hands and the boundaries that the Indian Constitution carefully sets around personal rights. Guidance on how the right to privacy should breathe and grow today came from the *Puttaswamy* judgment, and it is that lens we must use to

AZB and Partners, 'Biometric Data Regulation in India: Legal Landscape and Risks' (azbpartners.com, August 2025) <<https://www.azbpartners.com/bank/biometric-data-regulation-in-india-legal-landscape-and-risks/>> accessed 28 August 2026; SFLC.in, 'Analysis of the Facial Recognition Technology-Enabled Surveillance Landscape in India' (sflc.in, November 2024) <<https://sflc.in/analysis-of-the-facial-recognition-technology-enabled-surveillance-landscape-in-india/>> accessed 28 August 2026.

check the risks face recognition technology brings us. Constitution carefully sets around personal rights. Guidance about how the right to privacy should breathe and grow today came from the

Digital Personal Data Protection Act, 2023, Act No. 22 of 2023, Government of India. The Act provides a statutory framework for processing digital personal data.

Puttaswamy judgment, and it is that lens we must use to check the risks face recognition technology brings us.

The intrusive power of face recognition technology today gives it a head start over older forms of watching people. Cameras can now silently collect our faces, link them to a crowd index, and compare the matches all the while we remain unaware, and none of us have given clear agreement. While older forms of spying depended on a person's eyes and memory, face recognition technology multiplies that once private gaze a million times. The surveillance freedom face recognition technology hands to the state gives way, step by step, to what looks, feels, and sometimes operates as a surveillance state. Because our faces are our most basic biometrics, the billion face-prints that can be uploaded change the rules for what our autonomy and our informational privacy once protected.

The risks multiply when we see how quietly and vigorously face recognition technology cameras have entered streets and rooms. Very few official records tell us how long Brazil's face-stamp will remain on the books, how long the cameras will clean it, and how police will hold, use, or share it. Key national research and promise warnings about how to map face recognition technology onto the country's older privacy promises. Without official notice, without a public debate, without the formal warnings on timing or scope or rights that defined older privacy rules, the data protection and the protection of everyone's choices in this country are the reminder.

The limits of face recognition technology together with its known flaws turn privacy into an urgent problem. Bias in the algorithms raises the chance of wrongly flagging or missing facial prints in communities already facing systemic neglect, which undercuts the equal status guaranteed by Articles 14 and 15 of our Constitution. Being misidentified can open the door to undue questioning, mistaken detentions, and the freezing of access to necessary services.

The scale of this demographic disparity is empirically documented in the research literature. In December 2019, the United States National Institute of Standards and Technology published the most comprehensive evaluation to date of 189 facial recognition algorithms across racial and gender demographic groups, finding that most systems produced false positive rates for Asian and African-American individuals that were between 10 and 100 times higher than those recorded for Caucasian subjects. Applied to India's exceptionally diverse population, which encompasses a wide range of skin tones, facial structures, and ethnic profiles not adequately represented in the predominantly Western-sourced training datasets used by many commercial vendors, these documented disparities are likely to be amplified, compounding the risk of wrongful biometric identification for communities that already face systemic disadvantages in their interactions with the criminal justice system.⁸

When the State employs face recognition, it must meet the tripartite criteria of legality, necessity, and proportionality that the protection of privacy courts imposed. Yet, most current programs ignore this benchmark: poorly defined or absent laws, weak safety procedures, and an expansion of the technology beyond what the stated juice of safety can justify.

Consequences for freedom of peaceful and lawful assembly and for nurture expression, enshrined in Articles 19(1)(a) and (b), also loom large. If activists and ordinary citizens know that surveillance governs every gathering, the natural reluctance to be recorded can chill street protests, open debates, and even spontaneous street celebrations.

When face recognition is rolled out with no tight laws, strong hardware guidance, and regular check-ins by independents, the whole fundament of freedom to move and speak freely, of which

Justice K.S. Puttaswamy (Retd.) v. Union of India, (2017) 10 SCC 1 — privacy restrictions must satisfy the requirements of legality, necessity and proportionality.

Patrick Grother, Mei Ngan and Kayee Hanaoka, 'NISTIR 8280: Face Recognition Vendor Test Part 3: Demographic Effects' (National Institute of Standards and Technology, December 2019) <<https://doi.org/10.6028/NIST.IR.8280>> accessed 28 August 2026; Intifada P Basheer, 'Bias in the Algorithm: Issues Raised Due to Use of Facial Recognition in India' (2025) *Surveillance and Society* <<https://journals.sagepub.com/doi/10.1177/24551333241283992>> accessed 28 August 2026.

the Constitution is the benchmark. What is now needed is a reinvention, not a facelift, of rules, boxes, and spirits that not only curbs the technology but also at the same time, creates the space for technology that affirms constitutional dignities.

6. COMPARATIVE REGULATORY APPROACHES

Around the world, countries are rolling out their own rules for facial recognition technology (FRT), and the difference isn't just red tape, it's a difference in what societies care about most, whether that's privacy, the latest gadgets, or laws that protect citizens from overreach. The European Union has taken the most detailed stance to date, mainly through the General Data Protection Regulation, or GDPR. Under this rule, facial scans fall into the "sensitive personal data" category, which means the least amount of data the system can use, the better. If it has to use the data, it must be locked up behind a set of strict doors think of them as vaults with several levers. The Union is also drawing up a new law, the Artificial Intelligence Act, that would slap the "danger" or "don't even think about it" labels on real-time facial recognition in public areas. The technology could peek out for a moment only in specific police efforts that absolutely can't carry on without it. Even then, cops would have to prove that the tech won't bust up basic rights and can't hog more data or power than it really needs. Requirements on the law books would ask questions like, "Is this the only way to do it?" or "Is the risk in line with the task?" or "Will the public ever find out how this went down?" The result is a rules package that's already read by privacy experts beyond the EU and is getting tweaked again and again until the balance feels just right, soaking in the lesson that even chipboards deciding guilt for the most outrageous crimes must be set in a brisk air of respect and fairness.

Unlike Europe's unified stance, oversight of facial-recognition technology in the U.S. is cluttered and shifting. No single federal rule governs these powerful systems, but a handful of states have started filling the gap. The Illinois Biometric Information Privacy Act widely known as BIPA demands that companies secure written consent from individuals before capturing, labeling, or storing a single biometric image. The law imposes strict limits on how long companies can keep records and on whom they can share them with. People harmed by violations can sue for damages and win substantial payments. In a softer but still significant way, cities like San Francisco and Portland have pursued the strictest limits of all: outright bans or long freezes on police use of facial-recognition algorithms, spurred by worries about biases that mistreat racial minorities and

immigrants. Across towns and states, the rules look like a patchwork quilt, loudly advertising the tension between pushing forward the latest technology and protecting personal liberties. Gap watchers warn that vulnerable citizens can easily be skipped over by companies, since nothing stops them from relocating their servers or switching their pipelines to a gaping-state with more permissive law.

European Union, General Data Protection Regulation (GDPR), Regulation (EU) 2016/679, Art. 9 — biometric data used for identification is classified as sensitive personal data and is subject to strict protection

In marked contrast, every aspect of facial-recognition practice in China is orchestrated from the center. The technology is woven into a vast apparatus of social scoring, biometric border control, and constant public-monitoring cameras on the rung. Far from being a remedial backup, the government operations fill the void that U.S. advocates usually expect to find in standards: a *sine-qua-non* for citizens, cleansed of effective avenues for appeal. China legal landscape, offering meager hints of privacy law, holds no clauses even remotely similar to Europe's GDPR or U.S. BIPA provisions. Without restrictions that balance authenticity with oversight, the system fully imports reflexive panic into public safety, as state authorities routinely inspect, share, and repurpose images without warrant or oversight.

Countries like Canada and Australia take a mix-and-match approach to rule book facial recognition tech. Canada's Privacy Commissioner thinks it's time to re-write the playbook. Their pitch? Extra rules since the tech sneaks up on identity and reveals a lot of personal data.

They want agencies to stick to the three golden rules: be clear about why you're watching, let someone check the logs later, and then earn the people's trust. Australia's Office of the Australian Information Commissioner also creates a tiny secret rulebook. Anyone using the tech whether cops or the corner grocery store has to explain what's going on and get a yes before the face-matching starts.

These lessons serve a bigger purpose for India. Let's not wait for a fix-it-after-the-fact moment. India should sketch a rule book that can grow sideways as the market of apps and databases races ahead. That means starting with plain words that name facial recognition, spelling out what counts

as “play with face data,” and planting citizens’ agency in the driver’s seat so that even new data rules can’t trample the country’s promise of privacy. For India’s speedy market to trust itself, lawmakers should borrow a few headlights keep watching what’s working in Canada, Australia, and the U.S. To chop unseen biases and possible abuses during the rollout, it’s wiser to learn early than to bed-in privacy later.

7. CRIMINAL PROCEDURE (IDENTIFICATION) ACT, 2022

Objective of the Criminal Procedure (Identification) Act, 2022

The British colonial government enacted the Identification of Prisoners Act in 1920. The I.P. Act, instituted shortly after Gandhi’s non-cooperation movement amidst a swirling surge of nationalism, was indeed an attempt by the colonial government to strengthen its authority by broadening the vigilance scope. It empowered law-enforcement agencies to take and store photos, footprints, and fingerprints of convicted and non-convicted (only in specific circumstances) individuals and established provisions for their storage and disposal. A century later, the government of independent India replaced the I.P. Act, whose scope was limited, with vaguely drafted legislation that leaves no stone unturned to acquire more sensitive personal data and offers

Criminal Procedure (Identification) Act, 2022, Statement of Objects and Reasons.

fewer safeguards as compared to the colonial legislation.

The term “measurements” used in the said Act authorized only the taking of fingerprints and footprints of a limited category of convicted and non-convicted individuals and photos on the Magistrate’s order.

The ruling by the Supreme Court in the *State of U.P. vs. Ram Babu Misra* case and the 87th Report of the Law Commission of India called for amendments to the legislation in the 1980s. The 1920 Act received criticism and had to be amended mainly due to its narrow definition of “measurements”. Hence, one of the primary goals of the 2022 legislation appears to resolve this issue.

According to its Statement of Objects and Reasons, the Criminal Procedure (Identification) Act, 2022 declares its goal as modernizing the law to take into account the latest techniques of

identification and measurement that have emerged over the past century, especially in developed nations, which produce highly reliable and trustworthy results that are acknowledged around the world. The new Act of 2022 allows for more efficient and expedient criminal investigations, resulting in a higher conviction rate.

Features of the Criminal Procedure (Identification) Act, 2022

The Act expands the types of data that can be gathered, the people from whom such data can be in a centralized database. In accordance with section 6(2) of the 2022 Act, resistance or refusal to provide information or data will be considered to hinder a public worker from carrying out his duties.

The legislation makes it legal for police and prison officials to collect, store, and analyze physical and biological samples, including retina and iris scans of individuals who have been convicted. According to the Act, the record of measurements will be kept for 75 years from the date of collection. The people who have not been convicted or arrested for crimes against women or children or in detention for an offense that is punishable for less than seven years can refuse to give their biological samples. The National Crime Records Bureau (NCRB) will serve as the organization that keeps track of the data.

The 75-year biometric data retention period prescribed under the 2022 Act is exceptional by comparative standards and has attracted sustained criticism from privacy scholars and civil liberties organisations. A 2024 analysis by the Software Freedom Law Centre India found that tender documents for police-operated facial recognition systems routinely omit any retention schedule, deletion mechanism, or data minimisation requirement, thereby enabling the indefinite accumulation of biometric records irrespective of whether the person concerned is ultimately charged, convicted, or exonerated. The absence of a mandatory deletion obligation for records of persons who are acquitted or whose cases are discharged stands in stark contrast to the position taken by the European Court of Human Rights, which has held that the indefinite retention of biometric data of individuals not convicted of any offence constitutes a disproportionate interference with the right to private life.⁹

SFLC.in, 'Analysis of the Facial Recognition Technology-Enabled Surveillance Landscape in India' (sflc.in, November 2024) <<https://sflc.in/analysis-of-the-facial-recognition-technology-enabled-surveillance-landscape-in-india/>> accessed 28 August 2026.

Analysis of the Criminal Procedure (Identification) Act, 2022

In particular, the Act impacts Indian citizens who are under trial, arrested, in jail, or detained under a preventive custody law, which will be enacted to cover everyone who is arrested in a case. It principally violates the fundamental rights under Article 14, 20(3), and 21. It gives the police and magistrates considerable power. They have the power to compel the accused to testify, which is ludicrous and might lead to abuse of authority and rampant corruption.

Criminal Procedure (Identification) Act, 2022, Section 2(1)(b) and Section 4, relating to the taking and recording of measurements.

The Act's provisions allow the police to forcibly take "measurements" of convicts, arrestees, detainees, undertrials, and anyone else who may be remotely involved with the connection of an offense without first establishing their involvement or the evidentiary value of such "measurements." "Measurements" also include "biological samples", "analysis", and can be seized forcefully in the event of resistance or refusal. These phrases can be interpreted to include "measurements" of a testimonial kind obtained through a coerced mental assessment. As a result, this coercive clause violates the right against self-incrimination a well-established element of our criminal justice system stipulated by Article 20 (3).

8.A COMPARATIVE ANALYSIS OF THE EUROPEAN UNION, UNITED STATES, AND AUSTRALIA

Biometric Data Protection in the European Union

The European Union (EU) has been a pioneer in the development of robust data protection laws, with the General Data Protection Regulation serving as a model for many other jurisdictions. Under the General Data Protection Regulation, biometric data is classified as "special category data," which requires enhanced protection due to its potential to uniquely identify an individual. Article 9 of the General Data Protection Regulation specifically prohibits the processing of biometric data for the purpose of uniquely identifying an individual, unless one of several exceptions applies, such as explicit consent, necessity for employment, or reasons of substantial public interest.

The European Union has further supplemented the GDPR with the Artificial Intelligence Act (Regulation (EU) 2024/1689), which entered into force on 1 August 2024, with its prohibitions on unacceptable AI practices taking effect from 2 February 2025. The AI Act adopts a risk-based architecture that classifies the real-time remote biometric identification of individuals in publicly accessible spaces for law enforcement purposes as an unacceptable risk, and generally prohibits such systems subject to narrow, judicially authorised exceptions covering searches for missing persons, the prevention of imminent and serious threats to life, and the identification of serious criminal offenders. The Act also expressly prohibits the untargeted scraping of the internet or CCTV footage to create or expand facial recognition databases, thereby addressing the concern that retrospective biometric archives can be assembled at scale without the knowledge or consent of those whose data is captured: a practice that India's current regulatory framework does not explicitly prohibit.¹⁰

The General Data Protection Regulations approach to biometric data is grounded in several key principles, including transparency, purpose limitation, data minimization, and the right to data portability. These principles are designed to ensure that individuals have control over their biometric data and that organizations processing such data do so in a manner that respects individuals' privacy rights.

Transparency: The GDPR requires organizations to be transparent about their collection, use, and storage of biometric data. This includes providing clear and accessible information to individuals about the purposes for which their biometric data is being processed, the legal basis for such processing, and the rights available to them under the GDPR about the purposes for which their biometric data is being processed, the legal basis for such processing, and the rights available to them under the GDPR.

Purpose Limitation: The principle of purpose limitation mandates that biometric data must only be collected for specific, explicit, and legitimate purposes. Once collected, the data cannot be further

Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonised rules on artificial intelligence (Artificial Intelligence Act) [2024] OJ L 1689, Arts 5(1)(h) and 5(1)(e); European Commission, 'AI Act' (digital-strategy.ec.europa.eu, 2024) <<https://digital-strategy.ec.europa.eu/en/policies/regulatory-framework-ai>> accessed 28 August 2026.

processed in a manner that is incompatible with these purposes unless additional consent is

Regulation (EU) 2016/679 (General Data Protection Regulation), Article 9, concerning the processing of biometric data for uniquely identifying an individual. Regulation (EU) 2016/679 (General Data Protection Regulation), Article 9, concerning the processing of biometric data for uniquely identifying an individual.

Data Minimization: The GDPR requires that organizations collect only the minimum amount of biometric data necessary for the specified purposes. This principle is particularly important in the context of biometric data, given its sensitivity and the potential risks associated with its misuse.

Data Portability: The right to data portability allows individuals to obtain and reuse their biometric data across different services. This right is intended to enhance individuals' control over their data and facilitate greater interoperability between different biometric systems.

The GDPR also imposes strict security requirements on organizations processing biometric data. These requirements include the implementation of appropriate technical and organizational measures to protect the data from unauthorized access, alteration, or disclosure. Organizations are also required to conduct regular security assessments and implement measures such as encryption and anonymization to mitigate the risks associated with biometric data processing.

In addition to the General Data Protection Regulation, the European Court of Human Rights (ECHR) has played a significant role in shaping the jurisprudence on biometric data protection. the ECHR has emphasized the importance of balancing public security interests with individual privacy rights. This landmark case involved the retention of DNA profiles and fingerprints of individuals who had been acquitted of crimes. The ECHR ruled that the indefinite retention of such biometric data constituted a violation of the right to privacy under Article 8 of the European Convention on Human Rights. This decision set an important precedent for the regulation of biometric data, underscoring the need for proportionate and justified use of such data by public authorities.

Biometric Data Protection in the United States

The United States adopts a more fragmented approach to data protection, with a patchwork of federal and state laws governing the regulation of biometric data. Unlike the EU, the US does not have a comprehensive federal data protection law. Instead, biometric privacy laws in the US are governed by a combination of sector-specific regulations and state-level legislation.

Accountability Act (HIPAA) and the Gramm-Leach-Bliley Act (GLBA) provide some protection for biometric data in specific contexts, such as healthcare and financial services. HIPAA, for example, imposes strict requirements on the collection, use, and disclosure of biometric data in the healthcare sector. However, these laws do not provide broad protection for biometric data across all sectors.

State-Level Legislation: Illinois has been a pioneer in biometric data protection with the enactment of the Biometric Information Privacy Act (BIPA) in 2008. BIPA imposes strict requirements on private entities that collect biometric data, including obtaining written consent, informing individuals of the purpose and duration of data collection, and implementing safeguards to protect

Regulation (EU) 2016/679 (General Data Protection Regulation), Arts. 5 & 9.

the data. BIPA also provides a private right of action, allowing individuals to sue for violations, which has led to a significant amount of litigation and has influenced other states to consider similar legislation. The effectiveness of BIPA lies in its enforcement mechanism, which empowers individuals to hold organizations accountable for non-compliance.

California's Consumer Privacy Act (CCPA), which took effect in 2020, also includes provisions related to biometric data, classifying it as a category of personal information that is subject to enhanced privacy rights and protections. The CCPA grants consumers the right to access, delete, and opt out of the sale of their biometric data, reflecting the growing importance of biometric data in the broader landscape of data privacy law. However, unlike BIPA, the CCPA does not provide a private right of action for biometric data breaches, limiting its enforceability to actions by the Attorney General.

Biometric Data Protection in Australia

Australia's approach to biometric data protection is primarily governed by the Privacy Act, 1988, which regulates the handling of personal information by government agencies and private organizations. Under the Privacy Act, biometric data is classified as "sensitive information," which is subject to higher levels of protection than other types of personal information.

The Australian Privacy Principles (APPs): The Australian Privacy Principles (APPs), which are set out in the Privacy Act, provide the framework for the collection, use, and disclosure of biometric data. APP 3, for example, requires organizations to obtain consent before collecting biometric data, unless an exception applies, such as where the collection is required by law. APP 11 requires organizations to take reasonable steps to protect biometric data from misuse, interference, and loss, as well as unauthorized access, modification, or disclosure.

The APPs emphasize the importance of transparency, accountability, and individual rights in the handling of biometric data. Organizations are required to have a clear and publicly available privacy policy that outlines their practices regarding the collection and use of biometric data. **Federal Regulations:** At the federal level, laws such as the Health Insurance Portability and Individuals also have the right to access and correct their biometric data, as well as to lodge complaints if they believe their data has been mishandled.

Enforcement and Guidance by the OAIC: Australia's Office of the Australian Information Commissioner (OAIC) plays a key role in enforcing the Privacy Act and ensuring compliance with the APPs. The OAIC has issued guidance on the use of biometric data, emphasizing the importance of transparency, consent, and data security. The OAIC also has the power to investigate complaints and take enforcement action against organizations that breach the Privacy Act, including the imposition of fines and other penalties.

Privacy Act 1988, Australian Privacy Principles (APPs) 3 and 11, concerning the collection and security of biometric and personal information.

9. CASE LAWS

K.S. Puttaswamy (Retd.) v. Union of India

In India, the debate over how the law treats Facial Recognition Technology (FRT) is still new, and the Supreme Court has not yet given a clear answer about whether using it broadly is allowed under the Constitution. Even so, some important legal principles and trends from past judgments provide a useful compass. The key starting place is the landmark decision in the 2017 right to privacy case, Justice K.S. Puttaswamy (Retd.) v. Union of India, in which the Supreme Court ruled that

Illinois Biometric Information Privacy Act, 740 ILCS 14/1 et seq.— regulating the collection, use and storage of biometric information.

the right to privacy is a fundamental right under Article 21 of the Constitution. This decision laid down a “three-fold test” that requires any government action that invades the privacy of individuals to be legal, necessary for a valid public purpose, and not more intrusive than the situation requires. This test now serves as the first hurdle for any public authority that wishes to deploy face recognition technology.

Since the Puttaswamy Judgment, the courts have reiterated this privacy framework in cases dealing with the collection of biometric data. In a 2018 decision, for example, the Court accepted the Aadhaar scheme but banned the use of Aadhaar data for surveillance or for any purpose other than welfare and tax. This guardrail shows the judiciary’s concern about “function creep”—the worry that data once collected for one purpose will be used for another more intrusive purpose—while protecting privacy as well as basic legal principles of fair procedure.

Indian lower and High Courts have looked at facial recognition tech (FRT) on only a narrow front. A Delhi High Court-led project used FRT to reunite lost kids and was praised for the service to child welfare. Yet judges and rights watchdogs worry that the same tech can track protesters or other vulnerable folks without checks, point to the absence of clear rules, and flag the harm caused

when faces get wrongly matched. Smart lawyers and academics point out that letting police use face recognition technology without guardrails could run head-on with the right to due process. Put that same face recognition technology proof before a judge, and doubts pile up: the Indian Evidence Act says the system must be trustworthy and capable of being checked, and when tech

makes big mistakes, the cost isn't just a wrong mugshot—it's somebody's freedom and name on the line.

Though the Criminal Identification Act, 2022 opens the door for lots more biometric grabs, face recognition technology included, critics say the same law is too vague on how long the data stays.

Justice K.S. Puttaswamy (Retd.) v. Union of India, (2017) 10 SCC 1, recognize privacy as a fundamental right under Article 21 of the Constitution of India.

how a judge watches each step, and how a person says yes to the match. Those gaps sound new alarms under the Constitution.

Looking abroad, the European Court of Human Rights said it best: the justices said letting the state keep the biometric record of someone never charged with a crime is a poor, over-the-top trade for safety. That verdict, at least, helps above average Indian folks of data.

People's Union for Civil Liberties (PUCL) v. Union of India (1997)

The case can be traced back to the growing concerns about the unfettered and arbitrary use of Telephone tapping power under Section 5(2) of the Indian Telegraph Act, 1885. In the 1990s numerous public disclosures and media reports revealed that the phones of several well-known journalists, activists, and political figures were tapped illegally. This practice was viewed

as a breach of an individual's privacy and a direct threat to civil liberties and democratic accountability. PUCL, a human rights organization, filed a petition under Article 32 of the Indian Constitution and challenged the constitutional validity of Section 5(2) of the Indian Telegraph Act, 1885, which allows telephone interception in certain situations, such as in the interest of public emergency or in the interest of public safety.

PUCL contended that the provision lacked procedural safeguards and was broad in nature, which makes it prone to misuse by government authorities. In the absence of stringent regulatory control, phone tapping breaches the fundamental rights, especially the right to privacy, which is an indispensable part of the right to life and personal liberty guaranteed under Article 21, and freedom of speech and expression under Article 19(1)(a) of the Indian Constitution. The case raised

a significant constitutional issue regarding the extent and limitations of state power in relation to an individual's fundamental rights. It has also highlighted the need for a robust legal framework to govern surveillance practices and guarantee accountability.

In this case, the main issue before the court was whether Section 5(2) of the Indian Telegraph Act, 1885, which allows telephone tapping under certain situations in the absence of sufficient procedural safeguards, violates the fundamental rights, especially the right to freedom of speech

People's Union for Civil Liberties (PUCL) v. Union of India, (1997) 1 SCC 301, concerning telephone tapping, privacy, and procedural safeguards under Articles 19 and 21 of the Constitution.

and expression guaranteed under Article 19(1)(a) and the right to life and personal liberty under Article 21?

The court held that in this case, concerning the right to privacy and validity of telephone tapping under Section 5(2) of the Indian Telegraph Act, 1885, the Supreme Court delivered a historic judgement.

1. The court held that telephone tapping without proper safeguards is a violation of an individual's right to privacy. The right to privacy, though not explicitly, is a component of Article 21 (Right to life and personal liberty).

2. Article 19(1)(a), which guaranteed the right to freedom of speech and expression, is also impacted because of telephone tapping because of the constant fear of being under surveillance.

3. The court also held that Section 5(2) of the Indian Telegraph Act, 1885, is not unconstitutional, and hence it was not struck down, but it was read down to make the provisions align with individual's fundamental rights. The provisions remain valid only used for strict procedural safeguards.

Selvi v. State of Karnataka (2010)

According to the facts of the case, appellant Selvi's daughter married a man from a different caste against her family's wishes. In 2004, the man was brutally killed by Selvi and two other people,

who became the prime suspect in the murder. In this case, the prosecution requested brain mapping and polygraphy examination of all three accused and received the authorization from regarding the same. The result of these tests showed the deception, the prosecution requested to perform the narcoanalysis on the three individuals which was approved by the magistrate. It was then challenged in the Karnataka High court which was later on denied. The appellant then approached the Supreme Court. The first appeal was filed by the appellant in 2004. Subsequently, they filed the appeal in 2005, 2006, 2007, and 2010, which was collectively taken up through a Special Leave

People's Union for Civil Liberties v. Union of India, (1997) 1 SCC 301, on telephone tapping, privacy, and procedural safeguards under Articles 19 and 21.

Petition on 5th May 2010. The main contention of the accused was to undergo the neuroscientific investigative techniques without obtaining consent.

Several constitutional and legal issue was raised, primarily revolving around the admissibility of evidence through certain scientific techniques without the consent of the accused. The key issues include:

1. The primary constitutional issue was whether subjecting an individual to narco-analysis, brain-mapping, and polygraph tests without their consent violated their right against self-incrimination as enshrined in Article 20(3) of the Indian Constitution. This article protects individuals from being compelled to be witnesses against themselves the case also raised questions about the violation of the right to life and personal liberty guaranteed under Article 21 of the Constitution. The court had to consider whether the involuntary administration of these tests amounted to an infringement of the accused person's fundamental rights.

2. The court examined the voluntariness of confessions obtained through these scientific techniques. It considered whether the use of such methods without the accused's consent undermined the voluntariness of any statements or information obtained during the tests.

The court acknowledged the fact that narcoanalysis, brain mapping, and polygraphy tests are invasive procedures in themselves that may infringe on someone's mental privacy. These tests are involuntary in nature so as to raise concern about the reliability of the information obtained. the

Supreme Court ruled that the prohibition against self-incrimination found in Article 20(3) applies to criminal investigation as well. It was held that compulsory administration of neuroscientific techniques should be viewed as a clear violation of Article 20(3) of the accused. It is due to the fact, that the emphasis during the investigative techniques was on the veracity and the voluntariness of the statement made by the accused. Compelling the accused to undergo these tests without their consent is a violation of fundamental rights and any information, if forcibly extracted from an individual is unconstitutional. Article 20(3) read with Section 161(2) of the Code of Criminal Procedure, 1973, protects the accused persons, suspects as well as

Selvi v. State of Karnataka, (2010) 7 SCC 263, concerning narco-analysis, polygraph tests, brain-mapping, and the right against self-incrimination under Article 20(3).

witnesses to be examined during the investigation. “*Article 20(3) safeguards a person’s right to choose to speak or to keep quiet, regardless of whether the ensuing testimony turns out to be exculpatory or inculpatory.*” The court ruled that the forced application of these procedures is an invasion of mental privacy and a violation of an individual’s fundamental human rights. It will subsequently violate the standard of substantive due process as given in Article 21.

The court recommended that a comprehensive legal framework be established to regulate the use of these tests, ensuring that they are conducted with the utmost care and respect for individual rights. It suggested that such a framework should include guidelines on the voluntary nature of consent, the presence of legal representatives, and the prohibition of any form of physical or mental coercion.

10. SUGGESTIONS

India should encourage technological approaches that achieve legitimate identification or security objectives while minimizing the collection of personal information. Encryption, anonymization where technically feasible, access controls, secure deletion, and privacy-by-design principles should be incorporated into system architecture. Technological innovation

should therefore proceed alongside constitutional protection rather than treating privacy as an afterthought.

Promote Privacy-Preserving Technology and Responsible Innovation

Government authorities should publicly disclose the purpose, legal authority, responsible agency, categories of data collected, retention period, sharing arrangements, and general safeguards applicable to facial recognition systems. Public consultation and participatory governance should be encouraged before large-scale or high-risk deployments. Greater transparency would improve accountability and public trust while allowing constitutional concerns to be considered before harm occurs.

Strengthen Transparency and Public Participation

The use of facial recognition at demonstrations, public meetings, and other lawful assemblies requires particular caution because surveillance may discourage citizens from exercising Articles 19(1)(a) and 19(1)(b). Deployment in such contexts should therefore require heightened justification, narrowly defined objectives, and safeguards against identification, tracking, or profiling of persons merely because they participate in lawful civic activity.

Protect Freedom of Speech and Peaceful Assembly

Before and during operational use, facial recognition systems should undergo independent testing for accuracy, false matches, demographic bias, spoofing risks, and cybersecurity vulnerabilities. Systems that demonstrate unacceptable error or discriminatory outcomes should not be deployed until the identified deficiencies are addressed. Audit results should be periodically reviewed rather than treating accuracy as a one-time certification.

Require Accuracy, Bias and Security Audits

An independent supervisory mechanism should be empowered to review governmental and, where appropriate, high-risk private uses of facial recognition. Regular audits, compliance inspections, transparency reports, and accessible grievance mechanisms should be made mandatory. Individuals who are wrongly identified or whose biometric information is unlawfully processed should have an effective avenue for correction, complaint, and appropriate legal remedy.

Establish Independent Oversight and Effective Remedies

Facial data should be collected only for a specified and legitimate purpose and should not subsequently be repurposed without a fresh lawful basis. Clear retention periods should be prescribed, with mandatory deletion or anonymization when the purpose for which the data was collected has ended. These safeguards are particularly important in preventing function creep and indefinite biometric surveillance.

Introduce Strict Purpose Limitation and Data Retention Rules

Every governmental deployment of facial recognition should be preceded by a documented assessment of legality, necessity, and proportionality in accordance with the constitutional principles developed in Justice K.S. Puttaswamy (Retd.) v. Union of India. Facial recognition should not be used merely because it is technologically available; the authority should demonstrate a lawful basis, a legitimate and necessary objective, and that no less intrusive method can reasonably achieve the same purpose.

Apply Mandatory Legality, Necessity and Proportionality Tests

India should consider a dedicated statutory framework specifically regulating facial recognition technology and other biometric surveillance systems. Such legislation should clearly define facial recognition, identify permissible public and private uses, prescribe lawful purposes, and establish enforceable safeguards for collection, processing, retention, sharing, and deletion of facial data. This would reduce the regulatory uncertainty identified in this research and ensure that technological deployment remains consistent with the constitutional right to privacy under Article 21.

Enact a Dedicated Legal Framework for Facial Recognition

11. CONCLUSION

Bringing facial recognition technology (FRT) into India's digital landscape is like flying a glitzy flag launching a new age while also lifting a floodlight that shows cracks in our traditions of privacy, freedom, and public control. These past few years, face recognition technology has mushroomed across every space we used to think of as separate police, crime-solving, buses, vaccines, banks, you name it. The dazzling claims of faster queue-moving, better locking doors,

and crime prevention make it easy to cheer. Still, that cheer grows soft under the weight of the same technology slipping in without rules, like letting guests walk through your locked gate just because they ringed the bell nicely. A key riddle blinking through the report is the standoff between our instinct to feel safe and our need to feel free. Facial Recognition Technology shines a bright light finding lost children, tightening border checks yet this gain casts darker shadows, too: whole populations in search light, mistaken marks, tilted race fractions, and hand-losing no one is safe from. When the gadget is used too widely, too aggressively, it chips away at the public ink we name “trust,” that ink public Internet government and nice dinner. It scares not just voices on the microphone, not just merrymaking choruses, because freedoms that the crowd no longer expects it name aloud, too, no one keeps it from the firebase.

When you look at it through the lens of the constitution, the right to privacy that the Supreme Court granted us in the Puttaswamy case acts like a safety net for any facial recognition technology, or face recognition technology, that the government wants to use. To give that right real muscle, officials must prove that collecting our biometric data meets a strict three-part rule: the system must be allowed by law, it must be absolutely necessary, and the way it collects and uses our data must not stretch the rules more than absolutely needed. Still, if you check the law books, you will find that the toolkit the Indian government currently has falls far short. There is no clear and detailed law that tells officials how to treat our biometric everything, and the more complex problems that come from automated facial recognition still float around without a framework at all. The Digital Personal Data Protection Act, 2023 is a step forward, no doubt, but it is not the finish line especially in the case of facial recognition technology, where the grey areas still outnumber the clear rules by too wide a margin.

Right now, facial-recognition tech is racing ahead while the law is stuck in the slow lane. Schools, cops, and even some store managers roll out cameras without telling us, holding no community meetings and skipping the privacy checks that should happen first. If you look globally, this is the messy outlier, since places like the European Union see people’s faces as private in the first place. Their rules, the GDPR, are strict about consent and the way the tech is explained. Meanwhile, the U.S. state of Illinois says, “nope, get consent first,” and some cities just ban the tech completely. India, on the other hand, doesn’t yet have a nationwide blueprint that you could actually enforce.

The tech itself, of course, creates even more headaches. Brought to life by machine learning, the cameras are trained on mostly white and male faces, so when they see someone else, they get it wrong more often in the dark and dynamic street. For women, minorities, and especially kids, the wrong scan can land someone in handcuffs overnight. If there are no strict rules telling how long data can be stored, the footage might get sold to a private retailer, left on a school server, or leaked online. That drifting permission called function creep isn't just a worry, it's a predictable pattern in every tech debacle. We'd be smarter to hit the brakes and put real, enforceable standards in place first.

To wrap this up, India is at a point where the future could go one of two ways. If the country chooses to widely use facial recognition software for safety and services, everyone—from the Parliament to the college student must also insist on laws that guard people's dignity, personal freedoms, and the spirit of the Constitution. Backing this roadmap would renew the promise that the right to be left alone still matters. Then, India could proudly show other nations the calm, principled way to innovate. Only when strong, clear laws are on the books, and people are always put first, can facial recognition go from a potential danger to a useful tool keeping roads safer, services faster, and the spirit of democratic India still shining bright.

References

1. Ameen, J., & Vipra, J. (2022). Addressing constitutional challenges in use of facial recognition technology by Indian law enforcement. *Jurist Commentary*.
2. Dul, C. (2022). Facial recognition technology vs privacy: The case of Clearview AI. *Queen Mary Law Journal*, 2022, 1-24.
3. Gültekin-Várkonyi, G. (2024). Navigating data governance risks: Facial recognition in law enforcement. *Policy Review*, 24(3), 175-197.
4. Hodge, S. D. Jr. (2022). The legal and ethical considerations of facial recognition technology in the business sector. *DePaul Law Review*, 71(3), 731-763.
5. Jauhar, A., & Vipra, J. (2022). Addressing constitutional challenges in use of facial recognition technology by Indian law enforcement. *Jurist Commentary*.
6. Kugler, M. (2024). Public perceptions can guide regulation of public facial recognition. *Science and Technology Law Review*, 25(1), 1–14.

7. Mustafa, F. (2021). On facial recognition and fundamental rights in India: A law and technology perspective. SSRN Electronic Journal.
8. Raji, A. (2023). Facial recognition technology (FRT) through the lens of privacy: A comparative analysis between India and the UK. SSRN Electronic Journal.
9. Smith, M. (2021). Facial recognition and privacy rights. In *Digital Surveillance and Society* (pp. 135-158). CSU Research Output.
10. Wang, X. (2024). Beyond surveillance: Privacy, ethics, and regulations in facial recognition. *Frontiers in Artificial Intelligence*, 7, Article 1125605.
11. Al-Dabbas, H. M. (2024). Two proposed models for face recognition: Achieving privacy and efficiency. *Engineering, Technology & Applied Science Research*, 14(2), 8343-8351.
12. Lawful Legal. (2025). Supreme Court's perspective on privacy in the era of AI and facial recognition. *Lawful Legal Journal*.
13. Panjab University Law Magazine. (2025). AI-driven facial recognition: Human rights concerns and regulatory challenges. *Mag Law*, 4(1).
14. SFLC.in. (2024). Analysis of the facial recognition technology-enabled surveillance landscape in India.
15. NLSIJLT. (2021). Facing up to the risks of automated facial-recognition technology in India. *Indian Journal of Law and Technology*, 17(2).
16. Ghosh, R., & Suri, M. (2023). Legal challenges in biometric data usage in India. *Free Law*, 5(1), 40-54.
17. S. S. Rana & Co. (2025). Facial recognition technology: A growing challenge for privacy. *Mondaq (India)*.
18. Engineering, Technology & Applied Science Research. (2024). Two proposed models for face recognition: Achieving privacy and efficiency. 14(2), 8343-8351.
19. Mag Law. (2025). AI-driven facial recognition: Human rights concerns and regulatory challenges. 4(1).
20. Queen Mary University of London. (2022). Facial recognition technology vs privacy: The case of Clearview AI. *Queen Mary Law Journal*.
21. DePaul Law Review. (2022). The legal and ethical considerations of facial recognition technology in the business sector. 71(3), 731-763.

22. SSRN. (2025). Facial recognition technology and fundamental right to privacy. SSRN Electronic Journal.
23. SSRN. (2023). Facial recognition technology (FRT) through the lens of privacy: A comparative analysis between India and the UK. SSRN Electronic Journal.
24. Panjab University. (2025). AI-driven facial recognition: Human rights concerns and regulatory challenges. *Mag Law*, 4(1).
25. Lawful Legal. (2025). Facial recognition technology and the right to privacy in India. *Lawful Legal Journal*.
26. Kugler, M. (2024). Public perceptions can guide regulation of public facial recognition. *Science and Technology Law Review*.
27. Thales Group. (2023). Facial recognition history. In *Digital Identity and Security*.



Journal of Multi-Disciplinary
Legal Research