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

Sritrisha S, BBA LLB (Hons.), School of Excellence in Law, TNDALU.

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 deferred to the limb of a sovereign police, a municipal surveillance net, or an undisclosed vendor of removably authorised algorithms, 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 'binomal 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 digitised 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 vs. Union of India (2017), where the Supreme Court squarely held that the right to privacy is a fundamental right safeguarded by Article 21 of the Constitution. 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. Notwithstanding this authoritative command, India now faces a complete legislative void on data protection one that is glaringly apparent when biometric data, and specifically facial-recognition systems, are concerned. 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.

01. 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 (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 authorisation 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 spectre of unchecked tracking, the spectre of vulnerability to profiling, and a glaring absence of transparent oversight and grievance channels. Final figures are sobering: more than 170 city-wide systems are up and running in Maharashtra, Delhi, Telangana and selected districts, with central and local budgets channeling over ₹15,000 crore into installations, annual contracts, and sprawling databases. The spending and the stakes clearly position FRT as a non-negotiable fixture in the nation's digital posture.[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

[1] Ameen, J., & Vipra, J. (2022). Addressing constitutional challenges in use of facial recognition technology by Indian law enforcement. Jurist Commentary.

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 posture[2].

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 operationalises granular data protection norms through the General Data Protection Regulation, and in the United States, where 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, 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 marginalised 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 characterised 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]

[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.

In closing, facial recognition technology serves India as both potential enabler and profound risk, promise for improving governance and commerce tightly interwoven with threats to privacy and human dignity. To secure the fundamental rights of the individual, Indian constitutional and regulatory frameworks must mature in an integrated and anticipatory manner, calibrating the power of any technology to the ongoing moral and democratic proposition that the dignity and autonomy of each citizen is its foremost obligation.

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

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 crucial 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 authorisation, the risks posed by indefinite data retention, creeping illicit mission expansion, and the broader spectre of discriminatory targeting. The glide path that the Indian government has set driving the

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

technology under the twin rubrics of governance efficiency and crime deterrence trades on the promise of speed and efficiency, but stands at a watershed where the technocratic drive must reconcile itself, at each step, to deeply held constitutional and human rights norms.[5]

Across the world, urgent conversations are centring on the ethics and governance of biometric surveillance, reflecting the acute complexity that these technologies introduce. The European Union, through the General Data Protection Regulation, has established a demanding privacy regime for the processing of biometric data, signalling that any such activity must meet a stringent consent and proportionality standard. Parallelly, the United States has pursued a piecemeal and often contradictory regulatory strategy, leaving some jurisdictions to enact outright bans while others merely institute temporary stop-gaps. India, still formulating a coherent data protection and surveillance governance framework, can learn from these markedly distinctive global tapestries in order to create a legislative and institutional architecture that reconciles the imperative to protect sensitive biometric information with the equally pressing imperative to foster technological growth.

The present study therefore situates the deployment of facial recognition technology within India in relation to the country's distinctive technological capacity, constitutional embedding of privacy and dignity rights, and prevailing regulatory infrastructure. The paper charts the pace and componential architecture of adoption, interrogates the evolving privacy risks and the analytical boundaries of the Indian judiciary's privacy jurisprudence, and finally explains how the absence of a dedicated, coherent legislative template aggravates the danger that fundamental rights are rendered precariously contingent. The resulting analysis reinforces the central proposition that without deliberate statutory codification, supplemented by ethical assessment institutions, the technology is all but certain to ameliorate constitutional entitlements asymmetrically, privileging surveillance and undermining accountability.

03. CONSTITUTIONAL RIGHT TO PRIVACY IN INDIA

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

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

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 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.

[6] Lawful Legal. (2025). Supreme Court's perspective on privacy in the era of AI and facial recognition. Lawful Legal Journal.

04. OVERVIEW OF FACIAL RECOGNITION TECHNOLOGY (FRT)

Facial Recognition Technology (FRT) denotes an automated framework for ascertaining or confirming an individual's identity through the quantitative analysis of facial characteristics derived from still or dynamic image data. The 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 FRT 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 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.

FRT 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 programmes.

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 harmonising rapid technological advancement with guarantee of foundational rights.

05. 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 FRT 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 FRT.

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.

Various state governments have implemented facial recognition projects without comprehensive privacy impact assessments or public consultations, raising concerns over transparency and accountability. The Ministry of Home Affairs has proposed guidelines for biometric data handling in police investigations, but these are advisory and lack enforceability.

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.

06. 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 about how the right to privacy should breathe and grow today came from the Puttaswamy judgment, and it is that lens we must use to check the risks FRT brings us.

The intrusive power of FRT 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, FRT multiplies that once-private gaze a million times. The surveillance freedom FRT 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 FRT 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 FRT 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.

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 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.

07. CASE LAWS

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 Aadhaar case, Justice K.S. Puttaswamy (Retd.) v. Union of India, in which the Supreme Court ruled that 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 FRT.

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 FRT without guardrails could run head-on with the right to due process. Put that same FRT 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, FRT included, critics say the same law is too vague on how long the data stays, 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.

08. 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. Gapwatchers 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.

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's 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 crates 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.

09. 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, FRT 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-not-happening 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. FRT shines a bright-ish 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 merryangana 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 FRT, 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. Purshouse, J. (2019). Privacy, crime control and police use of automated facial recognition. Journal of Law and Society, 46(4), 581-610.
8. Mustafa, F. (2021). On facial recognition and fundamental rights in India: A law and technology perspective. SSRN Electronic Journal.
9. Raji, A. (2023). Facial recognition technology (FRT) through the lens of privacy: A comparative analysis between India and the UK. SSRN Electronic Journal.
10. Smith, M. (2021). Facial recognition and privacy rights. In Digital Surveillance and Society (pp. 135-158). CSU Research Output.
11. Wang, X. (2024). Beyond surveillance: Privacy, ethics, and regulations in facial recognition. Frontiers in Artificial Intelligence, 7, Article 1125605.
12. Al-Dabbas, H. M. (2024). Two proposed models for face recognition: Achieving privacy and efficiency. Engineering, Technology & Applied Science Research, 14(2), 8343-8351.
13. Lawful Legal. (2025). Supreme Court's perspective on privacy in the era of AI and facial recognition. Lawful Legal Journal.
14. Panjab University Law Magazine. (2025). AI-driven facial recognition: Human rights concerns and regulatory challenges. MagLaw, 4(1).
15. SFLC.in. (2024). Analysis of the facial recognition technology-enabled surveillance landscape in India.

16. NLSIJLT. (2021). Facing up to the risks of automated facial-recognition technology in India. Indian Journal of Law and Technology, 17(2).
17. Lipsa, S. (2023). Facial recognition devices: Developments and regulation in India. DSNLU Law & Technology Review, 2(1), 12-29.
18. Ghosh, R., & Suri, M. (2023). Legal challenges in biometric data usage in India. FreeLaw, 5(1), 40-54.
19. S. S. Rana & Co. (2025). Facial recognition technology: A growing challenge for privacy. Mondaq (India).
20. Engineering, Technology & Applied Science Research. (2024). Two proposed models for face recognition: Achieving privacy and efficiency. 14(2), 8343-8351.
21. MagLaw. (2025). AI-driven facial recognition: Human rights concerns and regulatory challenges. 4(1).
22. Queen Mary University of London. (2022). Facial recognition technology vs privacy: The case of Clearview AI. Queen Mary Law Journal.
23. DePaul Law Review. (2022). The legal and ethical considerations of facial recognition technology in the business sector. 71(3), 731-763.
24. SSRN. (2025). Facial recognition technology and fundamental right to privacy. SSRN Electronic Journal.
25. SSRN. (2023). Facial recognition technology (FRT) through the lens of privacy: A comparative analysis between India and the UK. SSRN Electronic Journal.
26. Panjab University. (2025). AI-driven facial recognition: Human rights concerns and regulatory challenges. MagLaw, 4(1).
27. Lawful Legal. (2025). Facial recognition technology and the right to privacy in India. Lawful Legal Journal.
28. Kugler, M. (2024). Public perceptions can guide regulation of public facial recognition. Science and Technology Law Review.
29. Purshouse, J. (2019). Privacy, crime control and police use of automated facial recognition. Journal of Law and Society.
30. Thales Group. (2023). Facial recognition history. In Digital Identity and Security.