
HUMAN RIGHTS IMPLICATIONS OF FACIAL RECOGNITION TECHNOLOGY IN INDIA: LEGAL, ETHICAL AND POLICY PERSPECTIVES

Ms Muskan Grover, Assistant Professor, Gitarattan International Business School, Rohini,
Affiliated to GGSIPU, Delhi

ABSTRACT

Facial Recognition Technology (FRT) has become a rapidly-growing instrument of policy-making, peace-keeping and commercial purposes all over the globe, and in India, too. The use of FRT in India is diverse, as being seen at the biometric boarding of passengers under the DigiYatra program at airports or police usage of the technology during public protests. The article focuses on the impact of the application of FRT on human rights in India using the doctrinal, normative and comparative methodology. The article reviews the literature related to artificial intelligence and human rights, biometric surveillance and privacy law; analyzes the rights enshrined in the Articles No. 14, 19 and 21 of the Constitution of India and the Supreme Court doctrine in Justice K.S. Puttaswamy v. Union of India and related cases; and puts the Indian experience into perspective of the global regulatory practices such as the regulations of the European Union, the laws analyzed in *Bridges v. South Wales Police* case and legal development in the USA, China and Canada. The analysis finds that while the Digital Personal Data Protection Act, 2023 marks a significant step forward, the absence of a purpose-built law governing biometric surveillance, weak independent oversight, and the risk of algorithmic bias leave critical human rights gaps unaddressed in the Indian context. The paper concludes with legislative, institutional, technical and participatory recommendations for a human rights-centred regulatory framework for FRT in India.

Keywords: Facial Recognition Technology, Human Rights, Privacy, Artificial Intelligence, Surveillance, Digital Rights, Data Protection, India.

1. Introduction

1.1 Background

The past twenty years has seen rapid proliferation of Artificial Intelligence (AI) in governance. Different governments around the world have increasingly adopted AI-based technology to enhance service delivery, safeguard security and efficiently manage large populations. Biometric surveillance is probably the most significant application in the domain of algorithmic governance by allowing various state and non-state actors to both identify individuals and monitor and track their movements in real time. Facial recognition technology (FRT) is the protagonist in this use of technology in governance. FRT is different from other biometric means of identification, such as fingerprinting or iris scanning, in that it can work almost undetected, and without any prior information or consent.

In India, its own process of digital transition marked by Digital India Programme, Aadhaar biometric identity platform and development of smart and safe cities -- has led to the widespread acceptance of FRT. As the world's most populous democracy and one of the largest markets for digital public infrastructure, India's experience with FRT carries significance well beyond its own borders, both as a model for other developing economies and as a test case for how constitutional democracies reconcile security imperatives with fundamental rights.

1.2 Meaning and Working of Facial Recognition Technology

Facial Recognition Technology refers to a class of biometric software applications capable of identifying or verifying a person from a digital image or a video frame by analysing and comparing patterns based on the person's facial features. The process typically involves four stages: face detection, in which the system isolates a face within an image; feature extraction, in which unique facial landmarks (the distance between the eyes, the contour of the jawline, the shape of the cheekbones) are converted into a mathematical representation known as a faceprint or template; matching, in which this template is compared against one or more templates stored in a reference database using deep-learning-based convolutional neural networks; and a final decision stage that yields either a verification (a one-to-one match, such as unlocking a phone) or an identification (a one-to-many search across a database, such as scanning a crowd for a wanted person). The distinction between verification and identification is analytically important, because it is the latter particularly when performed in real time on

live camera feeds in public spaces that carries the gravest human rights risks, since it enables the continuous, suspicionless tracking of entire populations rather than the confirmation of a single individual's identity.

1.3 Growth of Facial Recognition Technology in India

Over the last ten years, facial recognition technology (FRT) has been implemented in many areas in India. DigiYatra is a significant FRT-based program in the civil aviation sector that enables passengers to use facial recognition for hassle-free entry and security checks at prominent airports. In law enforcement, the National Crime Records Bureau has been working on creating an Automated Facial Recognition System (AFRS) that would help police with the identification of criminals, missing people and unidentified corpses. Also, various state police departments in India have already implemented FRT-enabled surveillance cameras across their cities. In addition, there have been many projects in Indian cities that utilize FRT for the monitoring and surveillance of the city inhabitants. FRT is also utilized in the railway services or at schools for creating attendance records and also in the banking sector for customer identification and verification during financial transactions.

1.4 Statement of the Problem

India is witnessing the rapid deployment of Facial Recognition Technology by government agencies and private entities without a comprehensive legal framework governing its collection, storage and use. While FRT promises enhanced security and more efficient governance, its widespread and often opaque use raises serious concerns regarding privacy, mass surveillance, discrimination, freedom of expression and due process. The absence of adequate statutory safeguards, independent oversight and accountability mechanisms threatens the fundamental rights guaranteed under the Constitution of India, and creates a governance vacuum in which technological capability has outpaced legal regulation.

1.5 Research Questions

- What is Facial Recognition Technology and how is it currently used in India?
- What human rights are affected by the deployment of FRT?
- Does the existing Indian legal framework adequately regulate FRT?

- What are the constitutional and ethical challenges associated with facial recognition?
- What reforms are necessary to ensure the responsible and rights-compliant use of FRT?

1.6 Research Objectives

- To examine the concept, working mechanism and applications of Facial Recognition Technology.
- To analyse the human rights implications of FRT in India.
- To examine the constitutional and statutory safeguards available under Indian law.
- To compare India's regulatory approach with international practices in the European Union, the United Kingdom, the United States, China and Canada.
- To recommend legal and policy reforms for the responsible governance of FRT in India.

1.7 Significance of the Study

This study is significant for three reasons. First, it responds to the growing use of state surveillance capabilities in the absence of comprehensive legal regulation, a gap that has become more urgent following the enactment of the Digital Personal Data Protection Act, 2023, which does not specifically address biometric surveillance by law enforcement. Second, it contributes to an emerging but still limited body of Indian legal scholarship that integrates constitutional privacy jurisprudence with the technical and ethical dimensions of AI-enabled biometric systems. Third, by situating the Indian experience within a comparative framework, the study offers policy lessons that can inform the design of a rights-respecting regulatory architecture that balances legitimate security interests with the constitutional guarantees of equality, liberty and dignity.

2. Review of Literature

The literature bearing on this study can be organized into six broad strands: (a) foundational scholarship on privacy and the surveillance society; (b) technical and ethical literature on algorithmic bias in facial recognition systems; (c) Indian constitutional privacy jurisprudence; (d) civil-society and empirical documentation of FRT deployment in India; (e) international

human rights and AI governance instruments; and (f) comparative regulatory scholarship. Each is discussed below, followed by an identification of the resulting research gap.

2.1 Privacy, Surveillance and the Information Society

The theoretical foundation of privacy law contains terms useful for the analysis of facial recognition technology (FRT). Solove (2004) proposed a popular classification of privacy violations—surveillance, aggregation, identification, secondary use, and exclusion—which can be seen in biometric data detection systems because in FRT several of these violations take place at the same time, such as ongoing surveillance, aggregation of biometric data with other types of personal data, and identification of an individual without their agreement.

Zuboff (2019) expands this consideration to the economy of data extraction under the term of “surveillance capitalism.” According to the author, biometric and behavioral data has become a raw material extracted from the population for commercial and governmental activity, which makes this framework more relevant in connection with private manufacturers of FRT, who serve both commercial and law enforcement customers with the same technology.

2.2 Algorithmic Bias and Technical Literature

A substantial body of computer-science and policy literature has documented systematic accuracy disparities in facial recognition systems across gender and skin tone, most prominently in the Gender Shades study, which found significantly higher error rates for darker-skinned women than for lighter-skinned men across several commercial facial-analysis systems. Subsequent testing by the U.S. National Institute of Standards and Technology similarly found demographic differentials in the accuracy of many facial recognition algorithms. This literature is critical to the Indian context because it demonstrates that the human rights risk of FRT is not confined to correctly identified individuals being surveilled, but extends to wrongly identified individuals—disproportionately from marginalized groups being subjected to erroneous law-enforcement action.

2.3 Indian Constitutional Privacy Jurisprudence

Indian legal scholarship on privacy has grown substantially since the Supreme Court's recognition of privacy as a fundamental right in *Justice K.S. Puttaswamy (Retd.) v. Union of India* (2017). Scholars such as Bhandari and colleagues have examined the doctrinal contours

of the proportionality standard articulated in that judgment and its subsequent application in the Aadhaar case and in *Anuradha Bhasin v. Union of India* (2020), arguing that Indian courts have accepted a four-fold proportionality test legitimate aim, suitability, necessity and balancing but have applied it inconsistently to specific surveillance technologies. This body of work provides the doctrinal foundation for evaluating FRT deployments against constitutional standards, though it has generally focused on Aadhaar and internet shutdowns rather than facial recognition specifically.

2.4 Civil Society and Empirical Documentation in India

In the absence of comprehensive official disclosure, Indian civil-society organizations have played an important documentary role. The Internet Freedom Foundation's Project Panoptic has tracked and catalogued FRT deployments by central and state police forces, airports and municipal authorities across India, revealing that most systems have been procured and deployed without enabling legislation, published standard operating procedures, or data-protection impact assessments. Internationally, Amnesty International's "Ban the Scan" campaign and reports by Access Now have documented similar patterns of opaque procurement and use of FRT for protest surveillance in multiple jurisdictions, including India, drawing particular attention to the deployment of facial recognition against demonstrators during the 2019–2020 protests against the Citizenship (Amendment) Act.

2.5 International Human Rights and AI Governance Instruments

At the international level, the Office of the United Nations High Commissioner for Human Rights has repeatedly flagged the risks that AI-enabled surveillance, including facial recognition, poses to the rights to privacy, non-discrimination and freedom of expression and assembly, calling for a moratorium on the most invasive applications pending adequate safeguards. The UNESCO Recommendation on the Ethics of Artificial Intelligence (2021) and the OECD AI Principles (2019) articulate soft-law standards of transparency, accountability, human oversight and proportionality that, while not binding, increasingly inform domestic policy discourse, including in India's own NITI Aayog strategy papers on "Responsible AI."

2.6 Comparative Regulatory Scholarship

Ever since the United Kingdom Court of Appeal's ruling in the case of *Bridges v. South Wales*

Police (2020), which ruled the police force's use of automated facial recognition to be unlawful due to the absence of an adequate legislative framework and a thorough analysis of the discriminatory implications of the practice, and the European Union's introduction of the Artificial Intelligence Act that prohibits most real-time remote biometric identification in public areas or classifies it as high-risk, comparative literature in regard to FRT regulation has expanded rapidly. Scholars have compared this right-based, precautionary stance to the fragmented and laissez faire regulation of FRT in the USA, where the responsibility for ensuring the legality of FRT rests mostly with the states and municipalities (like the Illinois Biometric Information Privacy Act and the bans in some cities, including San Francisco) or to the extremely extensive use of facial recognition in government supervision and social management in China, which is often mentioned as an example of unlimited biometric regulation.

2.7 Research Gap

This review reveals that while privacy jurisprudence, technical bias studies, civil-society documentation and comparative regulatory literature each address important dimensions of the FRT debate, few studies integrate constitutional human rights analysis, empirical documentation of Indian deployments, and comparative regulatory design into a single, India-focused framework. In particular, there is limited scholarship that systematically maps specific FRT use-cases in India onto the specific human rights they implicate, and fewer studies still that translate this mapping into concrete legislative and institutional recommendations calibrated to the Indian constitutional and administrative context. This study seeks to address that gap.

3. Research Methodology

3.1 Nature and Design of the Study

This study adopts a doctrinal, analytical and comparative research design. It is doctrinal in that it examines constitutional provisions, statutes, and judicial precedent to determine the existing state of Indian law governing facial recognition and biometric surveillance. It is analytical in that it evaluates the adequacy of this legal framework against the human rights it is meant to protect, applying the proportionality standard developed by the Supreme Court of India as its principal analytical tool. It is comparative in that it juxtaposes the Indian regulatory position

with the approaches adopted in the European Union, the United Kingdom, the United States, China and Canada, in order to identify transferable regulatory lessons.

3.2 Sources of Data

3.2.1 Primary Sources

- The Constitution of India, 1950
- The Digital Personal Data Protection Act, 2023
- The Information Technology Act, 2000 and the Sensitive Personal Data or Information Rules, 2011
- Judgments of the Supreme Court of India and comparative apex/appellate courts
- Government policy documents, tender notices and standard operating procedures relating to FRT deployment

3.2.2 Secondary Sources

- Peer-reviewed journal articles and books on privacy, surveillance and AI governance
- Reports of the Office of the United Nations High Commissioner for Human Rights
- NITI Aayog publications on Responsible AI
- Reports by civil-society organisations, including the Internet Freedom Foundation and Amnesty International
- Comparative legislative instruments, including the GDPR and the EU AI Act

3.3 Method of Analysis

The information obtained from these sources has been interpreted from a thematic viewpoint according to the human rights categories presented in the conceptual framework that covers topics such as privacy, nondiscrimination, freedom of expression, freedom of assembly, due process, children's rights, and the issues related to data protection and other ethical matters,

such as transparency and accountability. Judicial interpretation is performed through a doctrinal technique in order to arrive at the relevant constitutional standard, which is then applied/ compared with the cases involving any deployment of facial recognition technology as indicated in the secondary materials. The comparison is made according to the functional comparison approach considering how the proposed countries would address the same regulatory issues regarding the legal basis for deployment, consent requirements, transparency obligations, independent oversight, and remedies for wrongful identification.

3.4 Scope and Limitations

The study is confined to a legal, ethical and policy analysis of FRT and does not undertake independent empirical or technical testing of any specific facial recognition system. It relies on secondary reporting of deployment instances rather than primary data obtained through right-to-information requests, and it draws comparative material from five jurisdictions selected for their regulatory significance rather than an exhaustive global survey. These limitations are appropriate to a doctrinal and policy-analytical study of this nature but suggest fruitful avenues for future empirical research, discussed in the concluding section.

4. Analysis and Interpretation

4.1 International Human Rights Framework

The global framework on human rights establishes the criteria for evaluating the governance of FRT at a local level. The Universal Declaration of Human Rights talks about the right to equality before law (Articles 3 a, b, and the Preamble), the right to protection from any interference in privacy (Article 12), and the freedom of opinion and expression (Article 19). The International Covenant on Civil and Political Rights provides legally binding provisions on these rights in Articles 17, 19, and 21, covering respectively the protection of private life, expression, and the right of peaceful assembly. The UN Guiding Principles on Business and Human Rights impose the relevant requirements on enterprises selling or deploying FRT. There're also some other documents, e.g. OECD AI Principles or Recommendations of UNESCO on Ethical Artificial Intelligence that specify such requirements.

4.2 Constitutional Framework in India

The Constitution of India furnishes the primary domestic standard for evaluating FRT. Article

14 guarantees equality before the law and equal protection of the laws, and is engaged wherever FRT systems produce differential error rates across gender, skin tone or religious appearance, since such disparities amount to unequal treatment without a rational justification. Article 19(1)(a), (1)(b) and (1)(d) guarantee freedom of speech and expression, the right to assemble peaceably, and the right to move freely throughout Indian territory; each is implicated where FRT enables the identification and tracking of protesters or otherwise chills participation in public life. Article 21, as reinterpreted in *Justice K.S. Puttaswamy v. Union of India* (2017), guarantees the right to life and personal liberty, understood to include the right to privacy, dignity and informational self-determination, and is the principal constitutional lens through which FRT must be assessed. Articles 32 and 226 provide the procedural mechanism direct access to the Supreme Court and the High Courts respectively through which individuals may challenge unconstitutional surveillance.

4.3 Judicial Developments

In *Justice K.S. Puttaswamy (Retd.) v. Union of India* (2017), a nine-judge bench of the Supreme Court unanimously held that the right to privacy is intrinsic to the right to life and personal liberty under Article 21 and is also protected as an incident of the freedoms guaranteed under Part III of the Constitution. Crucially for FRT, the Court held that any state intrusion upon privacy must satisfy a four-fold proportionality test: the action must be backed by law, pursue a legitimate state aim, be necessary and suitable to achieve that aim, and strike a fair balance between the individual's right and the State's interest. This standard was subsequently applied in the Aadhaar judgment, *K.S. Puttaswamy v. Union of India* (2019), where the Constitution Bench upheld the Aadhaar biometric identity scheme for welfare delivery while striking down certain provisions permitting private-sector access to Aadhaar data, holding that mandatory biometric linkage beyond what was necessary for the stated welfare purpose was disproportionate. In *Anuradha Bhasin v. Union of India* (2020), the Court applied the same proportionality framework to internet shutdowns, holding that indefinite restrictions on fundamental freedoms require periodic review and the least restrictive alternative a standard directly transferable to the indefinite or blanket deployment of FRT-enabled surveillance. The earlier decision in *People's Union for Civil Liberties v. Union of India* (1997), concerning telephone tapping under the Indian Telegraph Act, remains foundational, having established that the absence of procedural safeguards renders an otherwise lawful surveillance power constitutionally infirm a precedent squarely applicable to FRT systems deployed without

published protocols or oversight. Public interest litigation by civil-society actors challenging specific FRT deployments, including the Automated Facial Recognition System project of the National Crime Records Bureau, remains pending or has been addressed only partially by courts, leaving the constitutionality of large-scale facial recognition for law enforcement substantially untested by binding precedent.

4.4 Human Rights Implications of FRT in India

4.4.1 Right to Privacy

The most direct human rights implication of FRT is its intrusion upon informational and decisional privacy. Continuous CCTV-linked facial recognition enables the mass, suspicionless monitoring of individuals in public space, converting what was previously anonymous movement through a city into a permanently trackable and searchable biometric trail. Because facial biometric templates cannot be changed in the way a password or PIN can, unauthorised access to or leakage of such data poses an irreversible and lifelong privacy risk. The absence of a data-protection impact assessment requirement specific to biometric surveillance in most current deployments compounds this risk.

4.4.2 Right to Equality and Algorithmic Bias

FRT engages Article 14 wherever its accuracy varies systematically across demographic groups. Empirical testing internationally has repeatedly found higher error rates for women and for individuals with darker skin tones, and India's own demographic and religious diversity raises the additional risk of disproportionate misidentification along religious or caste lines where training data is not representative. Such disparities are not merely technical defects; they translate into unequal exposure to the risk of wrongful law-enforcement action, amounting to indirect discrimination even where no discriminatory intent is present in the design of the system.

4.4.3 Freedom of Expression

The knowledge, or reasonable suspicion, that one's presence at a public gathering may be captured and permanently logged by a facial recognition system produces a well-documented "chilling effect" on the willingness of individuals to attend protests, religious gatherings or political meetings, thereby constraining the free exercise of expression under Article 19(1)(a)

even without any formal legal prohibition on the underlying speech or assembly.

4.4.4 Freedom of Assembly

Directly linked to the chilling effect on expression is the impact on the right to assemble peaceably under Article 19(1)(b). Documented use of FRT to identify individuals present at protests, including the 2019–2020 demonstrations against the Citizenship (Amendment) Act, illustrates how biometric surveillance can be used, or perceived to be used, to enable selective post-facto action against protesters, undermining the practical exercise of assembly rights regardless of whether the assembly itself was lawful.

4.4.5 Due Process

Because facial recognition systems are probabilistic rather than deterministic, they generate false positives instances in which an innocent individual is incorrectly matched to a person of interest. Where police act on such a match without independent corroboration, the result can be wrongful questioning, detention or arrest, implicating the due-process guarantees under Article 21 and the protections against arbitrary state action under Article 14. The absence of a statutory requirement for human verification before a facial-recognition match is acted upon significantly heightens this risk.

4.4.6 Children's Rights

The deployment of FRT-based attendance systems in schools and the incidental capture of minors within general CCTV-linked surveillance networks raise distinct concerns under the framework of children's rights, given children's heightened vulnerability to long-term data misuse, the absence of meaningful consent capacity, and the particular sensitivity of biometric data collected in educational settings.

4.4.7 Data Protection Concerns

Facial biometric data raises acute data-protection concerns relating to the adequacy of consent (particularly where FRT operates covertly or where consent is nominally obtained but practically unavoidable, as at certain airports), the duration and purpose limitation of data retention, the scope of onward sharing between government agencies and private vendors, and the cybersecurity of centralised biometric databases, a single breach of which could expose an

entire population's facial templates without any possibility of remediation.

4.4.8 Ethical Concerns

Beyond strict legal analysis, the deployment of FRT in India raises broader ethical concerns of transparency (the general public is rarely informed which systems are in operation, in which locations, and on what legal basis), accountability (there is often no identifiable authority responsible for redressing a wrongful match), explainability (the deep-learning models underlying most commercial FRT systems are not readily auditable even by the agencies that deploy them), and human oversight (procurement records reviewed by civil-society researchers suggest that several deployments lack any mandated human-in-the-loop verification step before action is taken on a system-generated match).

4.5 Comparative Analysis

A comparative review of five jurisdictions illuminates the range of regulatory choices available to India.

The European Union has adopted the most precautionary approach. The General Data Protection Regulation classifies biometric data used for identification purposes as a special category of personal data under Article 9, requiring explicit consent or another narrowly defined legal basis for its processing. The Artificial Intelligence Act builds on this foundation by classifying real-time remote biometric identification in publicly accessible spaces for law-enforcement purposes as presumptively prohibited, permitting it only in narrowly defined circumstances subject to prior judicial or independent administrative authorization.

In contrast, the United Kingdom has addressed FRT primarily in the form of judicial review instead of specific laws. The Courts of Appeal made a ruling in *Bridges v. South Wales Police* (2020), whereby the Court of Appeal held the police's employment of automated facial recognition had breached the law. It pointed out that the mechanism lawfully in place for the determination of the individuals that may end up on the watch list as well as the areas in which such technology would be employed was unnecessarily controversial. The law ruling that the police failed to conduct their obligation as per the provisions of the Equality Act 2010 is formation of reasoning that directly connects to the Article 14 analysis in India.

The USA does not have federal laws governing FRT. There is a number of regulations

embedded in the state laws, especially Illinois Biometric Information Privacy Act that gives individuals the right to litigate against those using biometric identifiers illegally. The regulation of FRT in the municipalities might be illustrated by an example of San Francisco banning the use of FRT by the state all together.

China represents the opposite pole, having integrated facial recognition extensively into state surveillance, transport, and social-management infrastructure with comparatively limited independent oversight, and is frequently cited in comparative literature as an example of the risks of unconstrained biometric governance for privacy, equality and political freedom.

Canada's approach has developed substantially through the investigative and advisory work of the Office of the Privacy Commissioner, which found the collection of facial images by the firm Clearview AI without consent to constitute unlawful mass surveillance under Canadian privacy law, and has since called for updated federal legislation to explicitly address biometric surveillance technologies. When comparing these five frameworks, India's position today corresponds more to the fragmented US system than to the precautionary European model, although a number of cases based on Puttaswamy's case provide adequate protection comparable to European standards.

4.6 Emerging Issues

Several emerging applications intensify the human rights risks already identified. Real-time facial recognition on live CCTV feeds, as opposed to retrospective matching against recorded footage, removes any practical opportunity for prior judicial or administrative authorisation of a specific search. Predictive policing systems that incorporate facial recognition alongside other behavioural data risk embedding historical patterns of discriminatory policing into ostensibly neutral algorithmic outputs. Emotion-recognition technology, which purports to infer psychological states from facial expressions, rests on contested scientific foundations and raises the prospect of decisions being made about individuals based on unreliable inferences about their internal states. The expansion of smart-city surveillance infrastructure and the growing practice of cross-border data sharing between security agencies further compound the difficulty of establishing clear jurisdictional accountability for any single deployment of FRT.

5. Discussion

The preceding analysis indicates that the gap is persistent between the promise of constitutional

protection India offers concerning privacy, equality, and expression and the practical implementation of facial recognition technology in the real world. The Puttaswamy case law has set the bar for proportionality in principle, but the examiner finds out that the doctrine is rarely, if ever applied by courts with respect to the application of facial recognition technology, hence leaving the constitutionality of implementations such as automated facial recognition systems of the NCRB and several state implementations untested. Such lack is a significant gap in practice as the constitutional principle allows preventing use of excessive surveillance; however, the required institutional mechanisms that could actually enforce it do not exist in the context of biometrics.

The passage of the Digital Personal Data Protection Act, 2023 is certainly a good thing, but this study shows that it is not enough by itself to counter the dangers posed by facial recognition technology. The Act's general consent and purpose-limitation framework is not calibrated to the distinctive features of facial biometric data its immutability, its capacity for covert and remote capture, and its use in law-enforcement contexts where individual consent is neither sought nor practically meaningful. Moreover, the Act's exemptions for processing by government agencies in the interests of security of the State, if broadly construed, could be read to place precisely the highest-risk category of FRT deployment law-enforcement surveillance outside the Act's core safeguards, a concern that parallels criticism levelled at similarly broad security exemptions in comparative data-protection regimes.

The comparative analysis in section 4.5 suggests that the sharpest lesson for India lies in the United Kingdom's Bridges judgment: the finding that a legal power can be rendered unlawful not by the absence of any legal basis at all, but by the excessive discretion left to individual deploying authorities and by the failure to assess discriminatory impact before deployment. This reasoning maps closely onto the Indian constitutional requirement, drawn from Puttaswamy, that a privacy-infringing measure be "backed by law" in a manner that is accessible, foreseeable and not arbitrary a standard that current FRT deployment in India, typically authorised by executive procurement decisions rather than legislation, does not appear to satisfy.

The algorithmic bias literature reviewed in section 2.2 further suggests that the equality dimension of FRT governance has received comparatively less attention in Indian policy discourse than the privacy dimension, despite Article 14 offering an independent and

potentially more readily justiciable basis for challenging specific deployments in the absence of mandatory bias-testing requirements. A regulatory framework for FRT in India that addresses privacy without also mandating algorithmic impact assessments and bias audits would therefore address only part of the constitutional problem.

Taken together, these findings point to the same conclusion reached in the research-gap table below: existing literature and existing law each address particular fragments of the FRT problem—privacy, technical accuracy, data protection, or comparative regulation—but no single framework in the Indian context yet integrates constitutional human-rights analysis, technical bias assessment, and institutional design into a coherent regulatory model specific to biometric surveillance.

5.1 Summary of Research Gaps

Existing Literature	Research Gap
Privacy concerns dominate the discourse	Limited comprehensive human-rights analysis integrating equality, expression and due process
Technical accuracy and bias studies	Lack of a constitutional-law perspective connecting bias findings to Article 14
Data protection discussed generally	Insufficient focus on biometric-specific safeguards distinct from general personal data
AI ethics literature (transparency, accountability)	Limited empirical research situating these principles in the Indian institutional context
International regulations analysed (EU, UK, US)	Lack of systematic comparative evaluation calibrated to Indian constitutional doctrine
Surveillance and protest-monitoring studies	Few studies integrate human rights law, constitutional safeguards and AI governance in one framework
Public-sector FRT use examined	Limited focus on private-sector deployment and cross-sectoral accountability

5.2 Policy and Legislative Recommendations

5.2.1 Legislative Reforms

- Enact a dedicated Facial Recognition Technology Regulation Act, distinct from general data-protection law, defining permissible purposes, prohibited uses and mandatory procedural safeguards.
- Statutorily prohibit indiscriminate, suspicionless, real-time facial recognition on public CCTV networks except in narrowly defined and judicially or independently authorised circumstances.
- Require prior legal authorisation, analogous to a warrant, for any high-risk law-enforcement deployment, following the reasoning of the Supreme Court in *Puttaswamy* and the Court of Appeal in *Bridges*.

5.2.2 Institutional Reforms

- Establish an independent AI and Digital Rights Regulatory Authority empowered to license, audit and, where necessary, suspend FRT deployments.
- Mandate periodic, publicly reportable audits of accuracy and demographic bias for every deployed FRT system.
- Create an accessible grievance-redress mechanism for individuals wrongly identified or adversely affected by an FRT-based decision.

5.2.3 Human Rights Safeguards

- Require documented necessity and proportionality assessments, applying the *Puttaswamy* four-fold test, before any new FRT deployment.
- Ensure meaningful, freely given consent wherever feasible, and prohibit consent architectures that make access to essential services contingent on biometric enrolment.
- Adopt specific protective measures for children and other vulnerable groups, including a presumption against FRT deployment in schools absent compelling justification.

5.2.4 Technical Measures

- Mandate algorithmic impact assessments and independent bias testing prior to procurement and at defined intervals thereafter.
- Require a documented human-in-the-loop verification step before any adverse action is taken on the basis of a system-generated match.
- Enforce data-minimisation and purpose-limitation principles, secure storage standards, and defined retention limits for facial biometric templates.

5.2.5 Public Participation and Oversight

- Conduct public consultation prior to large-scale FRT deployment, particularly in smart-city and safe-city projects.
- Support digital-literacy initiatives to enable informed public engagement with biometric surveillance policy.
- Strengthen parliamentary and civil-society oversight, including regular reporting to Parliament on the scope and outcomes of government FRT deployments.

6. Conclusion and Implications

Facial recognition technology presents significant advantages for enhancing public safety, improving public services as well as optimizing the process of governance, thus, a complete ban on its usage would be neither feasible nor reasonable, according to modifications listed by the author elsewhere. Yet, the research clearly indicates that the application of FRT in India involves numerous and varied dangers to such basic values as privacy, equality, freedom of expression and assembly, legal due process, and children's rights. These risks were intensified by the lack of a legal basis for biometric monitoring. In the Indian legal context, there exists the Puttaswamy doctrine which allows addressing excessive surveillance issues but legal means have been presented only due to high costs of initiating lawsuits.

This study has important implications for policy in that reforms must involve more than simply strengthening existing data protection laws. Instead, government regulation applicable to biometric identification programs must include elements such as prior clearance, independent

oversight, bias auditing, and provision of redress, while being guided by lessons learned from comparative analysis of European precautionary principle approach and UK judiciary that insists on limiting governmental discretion. For lawyers, the study points to the fact that the proportionality principle applicable in the Puttaswamy case is still relevant to challenge certain FRT applications even in the absence of specific legislation. For academics, the study suggests the importance of empirical studies on the mapping of FRT applications and conducting independent assessments of the accuracy of FRT systems in order to check the validity of the theoretical and comparative research findings outlined above. Finally, the study argues that human rights-based regulation founded on constitutional and legal principles should be introduced in order to guarantee that technological innovations do not harm the constitutional and democratic nature of India.

REFERENCES:

Access Now. (2021). Ban biometric surveillance for law enforcement. Access Now.

Amnesty International. (2021). Ban the Scan: Amnesty International's campaign to ban facial recognition. Amnesty International.

Anuradha Bhasin v. Union of India, (2020) 3 SCC 637 (India).

Bridges v. Chief Constable of South Wales Police, [2020] EWCA Civ 1058 (Court of Appeal, England and Wales).

Buolamwini, J., & Gebru, T. (2018). Gender shades: Intersectional accuracy disparities in commercial gender classification. *Proceedings of Machine Learning Research*, 81, 1–15.

Constitution of India, 1950.

Digital Personal Data Protection Act, No. 22 of 2023, India Code (2023).

European Parliament and Council. (2016). Regulation (EU) 2016/679 (General Data Protection Regulation). *Official Journal of the European Union*.

European Parliament and Council. (2024). Regulation (EU) 2024/1689 laying down harmonised rules on artificial intelligence (Artificial Intelligence Act). *Official Journal of the European Union*.

Information Technology Act, No. 21 of 2000, India Code (2000).

Internet Freedom Foundation. (2022). Project Panoptic: Tracking facial recognition technology deployments in India. Internet Freedom Foundation.

Justice K.S. Puttaswamy (Retd.) v. Union of India, (2017) 10 SCC 1 (India).

K.S. Puttaswamy v. Union of India (Aadhaar case), (2019) 1 SCC 1 (India).

National Institute of Standards and Technology. (2019). Face recognition vendor test (FRVT) part 3: Demographic effects (NISTIR 8280). U.S. Department of Commerce.

NITI Aayog. (2021). Responsible AI for all: Adopting the framework a use case approach on facial recognition technology. Government of India.

Office of the Privacy Commissioner of Canada. (2021). Investigation into Clearview AI, Inc. Government of Canada.

Office of the United Nations High Commissioner for Human Rights. (2021). The right to privacy in the digital age (A/HRC/48/31). United Nations.

Organisation for Economic Co-operation and Development. (2019). Recommendation of the Council on Artificial Intelligence, OECD/LEGAL/0449.

People's Union for Civil Liberties v. Union of India, (1997) 1 SCC 301 (India).

Solove, D. J. (2004). The digital person: Technology and privacy in the information age. New York University Press.

UNESCO. (2021). Recommendation on the ethics of artificial intelligence. United Nations Educational, Scientific and Cultural Organization.

United Nations Human Rights Council. (2011). Guiding Principles on Business and Human Rights (A/HRC/17/31). United Nations.

United Nations. (1948). Universal Declaration of Human Rights, G.A. Res. 217A (III).

United Nations. (1966). International Covenant on Civil and Political Rights, 999 U.N.T.S. 171.

Zuboff, S. (2019). The age of surveillance capitalism: The fight for a human future at the new frontier of power. PublicAffairs.