



ISSN: 2583-7753

LAWFOYER INTERNATIONAL JOURNAL OF DOCTRINAL LEGAL RESEARCH

[ISSN: 2583-7753]



Volume IV | Special Issue I

2026

Special Issue on the International E-Conference on

“Law in the Age of Artificial Intelligence: A Fundamental Perspective”

Organised by KES’ Shri J. H. Patel College of Law, Mumbai, on 24 January 2026

Official Publication Partner: LawFoyer International Journal of Doctrinal Legal Research

DOI: <https://doi.org/10.70183/lijdlr.2026.v4si1.09>

© 2026 LawFoyer International Journal of Doctrinal Legal Research

Follow this and additional research works at: www.lijdlr.com

Under the Platform of LawFoyer – www.lawfoyer.in

After careful consideration, the editorial board of LawFoyer International Journal of Doctrinal Legal Research has decided to publish this submission as part of the publication.

In case of any suggestions or complaints, kindly contact (info.lijdlr@gmail.com)

To submit your Manuscript for Publication in the LawFoyer International Journal of Doctrinal Legal Research, To submit your Manuscript [Click here](#)

KES' SHRI. JAYANTILAL H. PATEL LAW COLLEGE

About the College



KES' Shri. Jayantilal H. Patel Law College is committed to nurturing and empowering students through quality legal education. The college provides an inclusive and academically enriching environment that encourages students to excel in their studies, participate in co-curricular activities, engage in research, and develop a strong sense of civic responsibility.

The college is affiliated to the University of Mumbai, approved by the Bar Council of India, NAAC accredited with 'B++' grade, and ISO 9001:2015 certified. It offers programmes including B.A. LL.B., LL.B., LL.M., and specialised diploma courses.

With qualified and experienced faculty, a strong academic environment, moot court training, research activities and modern infrastructure, the institution seeks to prepare responsible, skilled and socially conscious legal professionals equipped to meet the challenges of a rapidly changing world.

The college functions under the aegis of Kandivli Education Society (KES), an institution established in 1936 with a long-standing commitment to quality, inclusivity and value-based education.

Affiliation	University of Mumbai
Recognition	Approved by the Bar Council of India
Accreditation	NAAC accredited 'B++'
Certification	ISO 9001:2015 certified

KANDIVLI EDUCATION SOCIETY

Established 1936



Kandivli Education Society (KES), established in 1936, has grown from a small educational initiative into a dynamic educational institution serving thousands of students.

With a legacy of quality, inclusivity and value-based learning, KES has expanded its academic presence across various disciplines. Its educational institutions are committed to providing meaningful learning opportunities and fostering academic, professional and personal development among students.

KES' Shri. Jayantilal H. Patel Law College is one of its prominent institutions dedicated to legal education. Through academic excellence, research, practical learning and co-curricular engagement, the college seeks to empower students with the knowledge, skills and values necessary to contribute meaningfully to society.

EDUCATIONAL COMMITMENT

- Quality and inclusive education
- Value-based learning
- Academic and professional development
- Research and practical learning
- Holistic and future-ready education

LAW IN THE AGE OF ARTIFICIAL INTELLIGENCE

A Fundamental Perspective



ABOUT THE INTERNATIONAL CONFERENCE

The International Conference on “Law in the Age of Artificial Intelligence: A Fundamental Perspective” provided an academic platform to examine the transformative impact of Artificial Intelligence on law, legal systems, governance and society.

The conference explored emerging legal and ethical questions relating to Artificial Intelligence, including intellectual property, authorship and ownership, liability, data privacy, cybersecurity, criminal justice, evidence law, human rights, ethics and accountability. It addressed the implications of Artificial Intelligence for legal education, commercial law, regulatory frameworks, policy development, research and scholarly communication.

The conference brought together academicians, research scholars, legal professionals and students to present research, exchange ideas and engage in interdisciplinary discussions. It encouraged meaningful academic dialogue and contributed towards the development of effective, ethical and inclusive legal responses to the rapidly evolving Artificial Intelligence landscape.

Conference	International Conference
Theme	Law in the Age of Artificial Intelligence: A Fundamental Perspective
Date	24 January 2026
Time	10:00 AM onwards
Mode	Online
Organised by	IQAC, Student Research Society and Library Committee
Publication Partner	LawFoyer International Journal of Doctrinal Legal Research [ISSN: 2583-7753]

PRINCIPAL'S MESSAGE

KES' Shri. Jayantilal H. Patel Law College



It gives me immense pleasure to welcome all academicians, research scholars, legal professionals and students to the International Conference on “Law in the Age of Artificial Intelligence: A Fundamental Perspective.”

Artificial Intelligence is transforming the way societies function and is increasingly influencing legal systems, governance, professional practices and education. These developments bring significant opportunities as well as complex legal, ethical and social challenges.

This conference provided a valuable platform for intellectual exchange and interdisciplinary dialogue on emerging issues such as data privacy, intellectual property, liability, criminal justice, human rights, ethics and the governance of Artificial Intelligence. The scholarly contributions and discussions during the conference encouraged deeper understanding and promoted responsible approaches to the use of Artificial Intelligence.

I extend my best wishes to all the speakers, researchers, presenters, participants and members of the organising team for a meaningful and intellectually enriching conference.

DR. VIRAL DAVE

I/c. Principal

KES' Shri. Jayantilal H. Patel Law College

ORGANISING COMMITTEE

International Conference on Law in the Age of Artificial Intelligence



I/c. Principal

Dr. Viral Dave

Convenor

Mr. Mahavir Mandot

Co-Convenors

Dr. Shweta Vijendra Pathak

Ms. Priyanka Khakhadia

Ms. Deepanshi Chandarana

Organised by IQAC, Student Research Society and Library Committee

KES' Shri. Jayantilal H. Patel Law College, Mumbai

*Papers presented at the conference are published in the Special Issue of the LawFoyer International Journal of
Doctrinal Legal Research [Volume IV, Special Issue I, 2026]*

PUBLIC-SECTOR AI FACE SURVEILLANCE AND FUNDAMENTAL RIGHTS: INDIA IN COMPARATIVE PERSPECTIVE

Priyanshu Upadhyay¹

I. ABSTRACT

Facial Recognition Technology (FRT) is rapidly transforming surveillance and law-enforcement practices by converting the human face from a biological attribute into a searchable digital identifier. This paper examines the legal tension between public-sector use of FRT and the protection of fundamental rights in India, where identification capacities have developed faster than the legal framework governing them. Adopting a doctrinal-comparative methodology, the study analyses Article 21 of the Constitution of India, the Information Technology Act 2000, the Digital Personal Data Protection Act 2023, the proposed Facial Recognition Technology (Regulation of Police Powers) Bill 2023, and leading judicial authorities including Justice K.S. Puttaswamy (Retd.) v Union of India. It also considers comparative materials from the European human-rights system, the GDPR, the EU AI Act 2024, United States biometric privacy approaches, and relevant policy scholarship. The analysis finds that India lacks a dedicated statutory framework regulating state deployment of FRT, despite privacy being constitutionally protected under Article 21 and subject to legality, necessity, proportionality, and procedural safeguards. Comparative jurisdictions increasingly treat biometric surveillance as a high-risk practice: the GDPR classifies biometric data used for unique identification as special-category data, while the EU AI Act restricts real-time remote biometric identification in publicly accessible spaces, subject to narrow law-enforcement exceptions and authorisation safeguards. These developments reflect growing concern that FRT may undermine privacy, free expression, equality, and democratic participation, particularly because of risks of mass surveillance, function creep, and algorithmic bias. The paper concludes that India's present reliance on executive practice creates a serious regulatory vacuum between constitutional guarantees and administrative deployment, requiring a rights-

¹ 10th Semester B.A.LL.B Student at CMP Degree College (University Of Allahabad), Prayagraj (India).Email: priyanshu121upadhyay@gmail.com

based statute grounded in transparency, judicial oversight, purpose limitation, and effective redress.

II. KEYWORDS

Biometric Surveillance, Proportionality Doctrine, Digital Personal Data Protection Act 2023, EU AI Act 2024, Algorithmic Bias.

III. INTRODUCTION

Facial Recognition Technology (FRT) - the technology that automates the process of identifying persons based on their facial features is experiencing an exponential growth in its use by governments and non-governmental entities all over the world². Supporters believe that FRT will improve security and efficiency which will help in preventing crime and in access control.³ Nevertheless, FRT creates the capacity of ubiquitous surveillance, which provokes acute human rights issues. Specifically, FRT may violate the right to privacy and smother free speech, assembly and equality. Significantly, the key human rights organizations (e.g. UN Special Rapporteurs) and the Non-Governmental Organizations (Amnesty, ARTICLE 19) have cautioned that uncontrolled FRT is equivalent to mass surveillance which is incompatible with fundamental rights.

The decision of the Supreme Court (2017) to claim privacy as inherent in Article 21 of the Constitution places stringent restrictions on any surveillance, though no further statute regulates FRT directly. This brings about a regulatory vacuum at the junction of technology and rights. On the international level, the methods are different: the European Union has implemented very strong data protection regulations (GDPR) and is reinventing an AI Act to limit FRT, whereas the United States is divided (no federal legislation, although certain states such as Illinois are implementing biometric privacy laws). This paper will provide a comparative legal discussion between FRT

² RC Bajpai and S Yadav, 'Use of Facial Recognition Technology in India: A Function Creep Breaching Privacy' (Oxford Human Rights Hub, 11 January 2021) <https://ohrh.law.ox.ac.uk/use-of-facial-recognition-technology-in-india-a-function-creep-breaching-privacy/> accessed 9 March 2026.

³ S Sritrisha, 'Facial Recognition Technology and the Right to Privacy in India: A Constitutional and Regulatory Analysis' (2025) Indian Journal of Law and Legal Research <https://www.ijllr.com/post/facial-recognition-technology-and-the-right-to-privacy-in-india-a-constitutional-and-regulatory-ana> accessed 9 March 2026.

and human rights protection with reference to the cases of India and international norms. The primary analysis compares the constitutional and statutory environment (and recent bills) in India to that of the international sphere, including jurisprudence and policy initiatives in the EU, US and the human rights arena.

A. Research Objectives

1. To compare Indian deployment of FRT in the public sector with the constitutional doctrine of proportionality determined in K.S. Puttaswamy Judgment.
2. To Compare the regulatory void in India with the international deregios-based regimes namely the European Union risk-management policy.
3. To Investigate the chilling effect of automated monitoring on Article 19 freedoms and democratic dissent.
4. To Introduce a rights-based legislative roadmap that meets the "procedure established by law" requirement of Article 21 of the Indian Constitution.

B. Research Questions

1. Is an unregulated use of FRT by the state agencies a contravention of the Article 21 constitutional obligation?
2. Are the wide state exemptions of the DPDP Act 2023 consistent with the positive privacy requirements?
3. What are the legal protections on the Glukhin v. Russia precedence require the use of highly intrusive tech?
4. Is a moratorium on the use of FRT needed because of systemic algorithmic biases against marginalized groups?
5. Does the Facial Recognition Bill 2023 place enough judicial checks and balances on individual liberties?

C. Research Methodology

This paper uses purely doctrinal approach to examine the intersection between the Facial Recognition Technology (FRT) and the basic human rights. The study is a critical analysis of main legal tools, such as Article 21 of the Indian Constitution, the Puttaswamy judgment, the Digital Personal Data Protection (DPDP) Act 2023, and the

draft Facial Recognition Technology Bill, 2023. In order to frame the regulatory environment, it analyses international laws (e.g., GDPR and AI Act of the European Union), United States laws on privacy (e.g., BIPA), and international human rights law (e.g., *Glukhin v. Russia*). Moreover, the research incorporates the secondary sources, such as policy documents and reports by the UN and the NGOs (Amnesty International, ARTICLE 19) to evaluate the empirical consequences, i.e. algorithmic bias and the chilling effect on the freedom of expression.

IV. RESEARCH & ANALYSIS

A. Constitutional Privacy in India

Any rights analysis relating to state surveillance should commence with the constitution of India. In its landmark case of 2017, *KS Puttaswamy v Union of India*,⁴ the Court of nine judges categorically acknowledged the right to privacy as an inherent and inalienable aspect of the right to life and personal liberty under Article 21, and that any state intrusion into individual privacy must be supported by a legitimate, fair, and reasonable law, and must pass a stringent proportionality test. This test holds that any state encroachment on individual privacy must meet the following conditions:

1. it must be supported by a statute;
2. the state action must serve a legitimate overarching purpose, such as maintaining national security or public order;
3. the means adopted must have a rational nexus to the objective and be the least intrusive method available; and
4. the law must incorporate adequate procedural safeguards to prevent arbitrary application and protect against the abuse of state power.

In the absence of these requisite threshold conditions the right to privacy cannot be legally restrained. Moreover, the Court pointed out that privacy rights are applicable to informational and personal autonomy, which will be implemented even in open areas.

⁴ *Justice KS Puttaswamy (Retd) v Union of India* (2017) 10 SCC 1.

In the case of Facial Recognition Technology (FRT), the bar that is set by the Puttaswamy framework is very high. FRT itself implies the extraction, processing, and tracking of biometric facial data a highly personal and irreversible physical trait. According to the Puttaswamy doctrine, the State is categorically forbidden to engage in any kind of surveillance unless it expressly predates a particular piece of legislative enactment, which has solid procedural checks and is substantially justified.

Legal critics are therefore of the view that any FRT implementation by a state should comply with these constitutional requirements. As an example of this basic condition, the petitioners in the current case of *SQ Masood v State of Telangana* have submitted that the use of FRT by the state is not accompanied by the necessary legislative sanction and the procedural protection and is thus a failure in the prongs of legality and procedure in the Puttaswamy test.⁵

B. Current Indian Legal Framework

Indeed, there is currently no statute specifically on FRT or digital surveillance more generally, even though it is mandated by the constitution. The rules of Data Protection (2011), which are part of the Information Technology Act 2000 (as amended) and which categorizes the biometric data as sensitive personal data in the hands of a private actor, only apply to body corporates and service providers, but not to a government agency.

Practically, it implies that FRT (e.g. by police or municipal authorities) use by the government is outside the scope of the IT Act. Aadhaar Act 2016 has few privacy protections (it restricts the use of biometric data of the ID system) but only on the Aadhaar context. Besides this patchwork, India enacted the Digital Personal Data Protection Act, 2023 (DPDP Act) that was aimed at establishing a minimum level of data protection. Although the DPDP Act deems consent in the personal data processing in principle, it grants wide exemptions to State (Section 17).

With this in mind, the Parliament has recently brought up the Facial Recognition (Regulation of Police Powers) Bill, 2023. This draft legislation would make it illegal to use FRT by police to conduct routine criminal investigations (Sec.3(1)) with the

⁵ *SQ Masood v State of Telangana* WP (PIL) No 44 of 2021 (Telangana HC).

exceptions of criminal activities that occur to national security or integrity. Section 43A of the IT Act and the SPDI Rules 2011 do not apply to government bodies, but other provisions such as Section 69 (lawful interception) and Section 69B (monitoring of traffic data) may still govern government surveillance. In other situations, a police officer would require an order of a Magistrate using FRT. Interestingly, the Bill goes further to prohibit the identification of persons on forbidden grounds (e.g. race, caste, religion, or gender) by a facial match.⁶

Although the Digital Personal Data Protection Act, 2023 was enacted to establish a baseline framework for personal data protection, it also preserves a significant regulatory gap in relation to state surveillance. While the Act is generally premised on consent and lawful processing of personal data, Section 17(2)(a) empowers the Central Government to exempt notified instrumentalities of the State from the application of the Act in the interests of the sovereignty and integrity of India, security of the State, friendly relations with foreign States, maintenance of public order, or prevention of incitement to related cognizable offences.

This broad exemption may substantially shield public-sector deployments of Facial Recognition Technology (FRT) from core privacy safeguards, including purpose limitation, data minimization, and meaningful oversight. By contrast, Section 17(2)(b) concerns a distinct exemption for processing necessary for research, archiving, or statistical purposes, provided such data is not used to make decisions specific to a Data Principal and the processing complies with prescribed standards. Accordingly, conflating Section 17(2)(b) with the state-instrumentality exemption would be legally inaccurate. The breadth of Section 17(2)(a), if applied without independent oversight and proportionality safeguards, risks leaving biometric surveillance insufficiently regulated and may conflict with the privacy principles recognised in *K.S. Puttaswamy v Union of India*.

The position must also be read in light of the Digital Personal Data Protection Rules, 2025, which operationalise several provisions of the parent Act. The Rules introduce

⁶ ARTICLE 19, 'European Court of Human Rights: Groundbreaking Ruling on Facial Recognition' (ARTICLE 19, 2023) <https://www.article19.org/resources/european-court-of-human-rights-groundbreaking-ruling-on-facial-recognition/> accessed 9 March 2026.

implementation-level obligations relating to clear consent notices, consent managers, breach notification, grievance-handling timelines, Data Principal rights, and the functioning of the Data Protection Board. They also reinforce principles such as purpose limitation, data minimisation, storage limitation, security safeguards, and accountability.

However, these procedural mechanisms do not materially narrow the exemption created by Section 17(2)(a) for notified State instrumentalities. Consequently, while the Rules improve the general compliance architecture of Indian data protection law, they leave largely untouched the core concern relevant to public-sector FRT: biometric surveillance by exempted State agencies may still operate outside ordinary consent, retention, and accountability controls unless separate statutory safeguards, independent oversight, and proportionality-based authorisation requirements are imposed.

C. Judicial and Regulatory Gaps

No Indian Court has so far adjudicated a case on FRT alone but only the Court of Puttaswamy. The concepts of Puttaswamy are, however, general. Since India continues to rely on executive action (e.g. police circulars, inter-departmental guidelines) to enforce FRT, any Court attack would most probably be put to test insofar as Article 21 is concerned. The limited numbers of high-profile cases (such as the Telangana petition) highlight the weakness: activists believe that the use of FRT is not proportionate and not transparent.

As an example, the petition observes that Telangana police rolled out FRT networks and mobile matching apps without reporting their accuracies and legality. This is non-transparency and accountability, which implies a creep of functions - surveillance well beyond any original intention.

Conclusively, India is experiencing regulatory vacuum on FRT. Privacy in the one hand is a basic constitutional right whereas on the other hand no binding legislation controls FRT. As a matter of fact, police have been utilizing FRT through executive

orders or informal guidelines instead of statute.⁷ This is in sharp contrast to the *lex materia* in other jurisdictions (see further), which have either data protection legislation or the legislation outlining biometrics legislation which directly limits FRT. The application of FRT in the Indian state is based on precarious legal principles in its absence - a scenario that commentators have termed as a total legislative vacuum⁸.

The *S.Q. Masood v. State of Telangana* petition has become a pivotal point in the legal discussion of biometric mass surveillance in India, as it is one of the limited high-profile cases against executive-led policing technologies. The petitioners claim that the use of Facial Recognition Technology (FRT) networks and mobile matching applications by the Telangana police is not specially authorized in the legislature. They, therefore, argue that this unregulated surveillance does not pass the high constitutional proportionality test developed by the Supreme Court in *K.S. Puttaswamy v. Union of India*. Moreover, the petition points to the extreme absence of transparency and accountability in the matter of the accuracy and legality of such biometric systems. This current case reveals the regulatory vacuum at the core of Indian society, in which police use technology that is highly intrusive based on ad hoc standards and not legal frameworks.⁹

D. International Human Rights Frameworks

In the entire world, the right to privacy is declared as basic by international human rights law. Article 12 of the Universal Declaration of Human Rights and Article 17 of the International Covenant on Civil and Political Rights (ICCPR) forbid an arbitrary or unlawful interference with privacy¹⁰. These instruments do not specifically refer to biometric surveillance, but UN experts perceive mass data-driven identification (such as FRT) as a preservation of privacy. As an illustration, the UN High Commissioner and special rapporteurs have included that the application of FRT in identification is

⁷ Amnesty International, 'The Right to Privacy in the Digital Age (Submission to OHCHR)' (Amnesty International, 14 June 2022)

<https://www.ohchr.org/sites/default/files/documents/issues/digitalage/reportprivindigage2022/submissions/2022-09-06/CFI-RTP-Amnesty-International.pdf> accessed 9 March 2026.

⁸ Srikrishna (n 5).

⁹ Bapat (n 2).

¹⁰ M Simmler and G Canova, 'Facial Recognition Technology in Law Enforcement: Regulating Data Analysis of Another Kind' (2025) 56 Computer Law & Security Review 106092.

equivalent to mass surveillance without discrimination that is contrary to privacy and democratic rights. In fact, a conducive statement encouraged states to prohibit technologies that facilitate the mass and discriminatory targeted surveillance.

Other human rights are also implicated by the deployment of FRT. In *Glukhin v. Russia*, decided on 4 July 2023, the European Court of Human Rights held that the use of facial-recognition technology to identify a peaceful protester violated Article 8, concerning privacy, and Article 10, concerning freedom of expression, of the European Convention on Human Rights. The jurisdictional position must be stated with precision: Russia was expelled from the Council of Europe on 16 March 2022, but it ceased to be a High Contracting Party to the European Convention on Human Rights only on 16 September 2022, following the six-month period contemplated under Article 58 of the Convention.

The Court therefore retained competence to examine alleged violations attributable to Russia that occurred before 16 September 2022, including the 2019 events in *Glukhin*. The Court treated the use of FRT in this context as highly intrusive, particularly because the applicant's conduct did not involve any threat to public safety. According to advocacy groups, a high chilling effect on the freedom of assembly and speech is the result of this type of surveillance: ARTICLE 19 states that people who know they are being spied upon will be less willing to exercise their rights.

FRT misidentifies minorities, which is an empirical issue that makes equality a concern. As invariably discovered in the research, commercial FRT is less accurate in women and people of color¹¹, i.e. minority populations are disproportionately misrecognized (and could be wrongly police). In conclusion, it can be suggested that the international human rights language views FRT through the prism of privacy, non-discrimination, and democratic freedoms.

E. Regulatory Approaches Abroad

- 1. European Union (EU):** EU has been keeping a low profile. The facial images and other biometric identifiers under the GDPR (Regulation 2016/679) fall

¹¹ Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 [2024] OJ L1689/1.

under the category of special-category data. In the GDPR, Article 9 of Regulation (EU) 2016/679 (GDPR) expressly forbids the use of biometric data (to identify something uniquely) without express permission or under restricted purposes that are legally identified. Practically, it implies that FRT scanning by a private company requires an informed consent of an individual, and police use has to be justified by high-quality data protection requirements (e.g. necessity tests, DPAs). At the policy level, the EU Artificial Intelligence Act reflects a risk-based regulatory approach to biometric surveillance. Political agreement on the Act was reached between the European Parliament and the Council in December 2023; formal adoption by the European Parliament followed in March 2024, and the Regulation entered into force on 1 August 2024 as Regulation (EU) 2024/1689. The Act subjects real-time remote biometric identification in publicly accessible spaces to strict limitations, permitting law-enforcement use only in narrowly defined circumstances and subject to authorisation and necessity-based safeguards. This framework preserves the paper's central comparative point: unlike India's largely executive-led approach to FRT deployment, the EU has moved toward an express statutory model that treats biometric identification as a high-risk rights-sensitive technology.

2. **United States:** There is no national policy concerning federal privacy, and the state legislation forms a patchwork in the U.S. The Biometric Information Privacy Act (BIPA, 2008) of Illinois is the remarkable one: according to this law, the private organizations must get a written agreement to use biometric identifiers (faceprints) prior to gathering biometric data. There have been a number of lawsuits against companies and police under FRT as required by BIPA. A ban has been implemented on law enforcement use of FRT in some cities within the U.S. (e.g. San Francisco, Boston). Privacy activists still demand tougher legislation at the federal level, however; a recent report by the U.S. Commission cautions that unregulated FRT is a significant threat to civil rights. Therefore, the U.S. is developing an uneven FRT regulation.

F. Human Rights Implications of FRT

The FRT implications to rights have been adequately recorded across jurisdictions. The main problem is privacy: FRT allows one to identify (match the face of the individual against a database) without his or her knowledge or permission. This is way above conventional surveillance (such as CCTV) as it can be able to automatically identify identities in bulk. Amnesty International claims that the application of real-time facial recognition in a public is a flagrant breach of privacy that cannot be considered a necessary or proportionate interference¹². Even post hoc (detecting it post-factum) compromises anonymity.

FRT also affects the freedom of expression and assembly. When the protesters or the reporters fear to be caught by the cameras, they can self-censor. ARTICLE 19 reports that the Russian government has already deployed FRT to monitor demonstrators, and the decision of the ECtHR in Glukhin admitted this very intrusive. One of the fundamental issues that human rights experts bring up is the so-called chilling effect, through which individuals do not speak or even demonstrate because they are afraid of being monitored.

In addition to this the FRT may become discriminatory. Algorithms which are trained on biased data may be biased in their misidentification or inability to identify some demographic groups systematically. This, along with the past prejudices of governments, makes some warning necessary that FRT will only enhance racial or social profiling. Therefore, most of the proposals clearly outlaw identification based on such sensitive attributes as caste, religion or race.

Lastly, the use of FRT also creates the problem of due process and accountability. When governments store facial templates indefinitely, then there is a possibility of function creep - the use of the data to other purposes. The level of transparency is usually low: people are usually not aware whether they are scanned or not and the reason. To ensure human rights are strong and well-protected, a number of scholars

¹² R Yadav and A Pundir, 'India's Digital Dilemma: Reconciling Facial Recognition Security with the Constitutional Right to Privacy' (NLIU-CLT, n.d.) <https://clt.nliu.ac.in/?p=1276> accessed 9 March 2026.

and UN organizations recommend that deployments of FRT should have algorithmic impact evaluation, transparency, and effective redress against abuses.

Together these considerations highlight the point that FRT is not a technical problem per se, but a legal one that is so deep rooted in law. It directly involves the fundamental rights - privacy, liberty, equality - and, therefore, it should be seriously reviewed by law.

V. KEY FINDINGS

- 1. Legal Vacuum in India:** The present Indian position reveals a significant gap between constitutional rights and administrative practice. Although the Supreme Court has imposed a high threshold for privacy-intrusive state action, India does not yet have a dedicated statute regulating FRT. In practice, law-enforcement authorities deploy FRT through executive instructions or ad hoc arrangements, without clearly defined purposes, safeguards, or accountability mechanisms. This raises serious concerns under the *Puttaswamy* proportionality framework, particularly on the requirements of legality, necessity, and procedural safeguards.
- 2. International Contrast:** Comparative jurisdictions increasingly recognise the need for express regulation of biometric surveillance. The GDPR and the EU AI Act reflect a precautionary and risk-based approach by subjecting biometric identification to stricter legality, necessity, consent, and authorisation standards. Similar safeguards proposed in the Indian Facial Recognition Technology Bill 2023, including judicial authorisation and restrictions on sensitive profiling, indicate a rights-based legislative direction. However, until such safeguards are enacted and implemented, India remains structurally behind comparative regulatory models and international human-rights expectations.

VI. SUGGESTIONS AND RECOMMENDATIONS

To develop a rights-based legislative roadmap consistent with the *Puttaswamy* proportionality framework and comparative data-protection standards, India should

consolidate its approach to public-sector Facial Recognition Technology through the following measures:

1. **Enact a specialised law on biometric surveillance by law-enforcement agencies:** India should move beyond broad state exemptions under the DPDP Act, 2023 and adopt a dedicated statutory framework governing the collection, processing, retention, sharing, and deletion of facial biometric data. Such a law must require every FRT deployment to satisfy legality, necessity, proportionality, and procedural-safeguard requirements.
2. **Establish an independent oversight authority:** A specialised authority, comparable in function to the European AI Office or an independent data-protection regulator, should be empowered to review public-sector FRT deployments, approve high-risk uses, conduct bias audits, prescribe technical standards, and prohibit unlawful or discriminatory surveillance practices.
3. **Mandate Fundamental Rights Impact Assessments:** Before any police, municipal, or administrative authority deploys FRT, a Fundamental Rights Impact Assessment should be conducted and, subject to narrowly tailored security exceptions, made publicly available. The assessment should disclose the purpose, necessity, scope, duration, affected groups, retention period, and safeguards attached to the proposed deployment.
4. **Create a public registry of FRT deployments:** All public-sector FRT systems should be recorded in a user-friendly and machine-readable public registry, drawing guidance from the transparency model reflected in Article 71 of the EU AI Act. Such a registry would enable citizens, courts, regulators, and civil-society organisations to monitor the scale and legality of state biometric surveillance.
5. **Require technical transparency and independent benchmarking:** No FRT system should be used by law-enforcement agencies unless it has undergone independent accuracy testing, demographic bias assessment, and security certification. Accuracy rates, false-positive risks, false-negative risks, and known limitations should be disclosed in a manner compatible with operational security.

6. **Strengthen Data Principal rights and human review:** The proposed Indian framework should recognise a right to contest adverse outcomes caused by FRT, including misidentification, wrongful investigation, exclusion from public services, or unlawful profiling. Individuals should have access to human review, reasons for adverse action, correction mechanisms, and an effective grievance-redress process.
7. **Provide compensation for unlawful processing and misidentification:** The statute should expressly provide compensation for harm caused by unauthorised processing, negligent retention, wrongful identification, or discriminatory use of facial biometric data. This would align Indian law with comparative rights-based models, including the remedial principle reflected in GDPR Article 82.
8. **Prohibit sensitive profiling and function creep:** FRT should not be used to classify, track, or profile persons on grounds such as caste, religion, race, gender, political opinion, or participation in lawful protest. Any use beyond the originally authorised purpose should require fresh legal authorisation, independent review, and strict necessity justification.

VII. CONCLUSION

The fact that facial recognition technology is spreading rapidly and, in most cases, covertly in the Indian public sector is an indication of a paradigm shift in the dynamics between the citizen and state. The face turns into a digital signature, thus the traditional demands of anonymity in the street are being destroyed in a systematic manner. This study has proved that the judiciary in *Justice K.S. Puttaswamy v. Union of India* has given a strong constitutional protection to the right to privacy, the executive-led use of FRT is currently being conducted in the state of a legislative vacuum, which does not meet the required proportionality and legality requirement. The comparative indicators of the analysis of the European Union AI Act indicate that India is still focused on administrative efficiency by providing extensive state exemptions under the DPDP Act 2023, whereas other jurisdictions are moving towards a risk-based, precaution approach of requiring the judiciary to supervise the effectiveness of the law.

In addition, the threats of algorithmic bias, as well as the chilling effect on democratic dissent, were recorded and are such examples as the case of *Glukhin v. Russia*. It emphasized that FRT is not a neutral technology but rather a very intrusive technology that can radically change the exercise of fundamental rights. The research concludes that such an invasive surveillance is currently resting on a thin thread due to the use of police circulars and executive orders. It is, thus, necessary that the Indian Parliament passes a rights-focused, statutory framework, including the proposed Facial Recognition Technology (Regulation of Police Powers) Bill, 2023, to have biometric identification regulated in accordance with the principles of necessity, purpose limitation and judicial authorization.

The promise of Article 21 can only be maintained in the digital age through a transparent, accountable and legally based approach that will ensure that technology is used as a means of providing safety to people and not as an instrument of uncontrolled state power. The growing gap between the technological potential and the discipline of the constitution should be bridged before the process of the normalization of surveillance will finally consume the very fabric of human dignity and democratic liberty.

VIII. REFERENCES

1. Amnesty International, 'Ban the Scan: Inside the NYPD's Surveillance Machine' (Amnesty International, 2022) <https://banthescan.amnesty.org/decode/> accessed 9 March 2026.
2. ARTICLE 19, 'Russia: Expansive Use of Facial Recognition Threatens Anonymity' (ARTICLE 19, 2022) <https://www.article19.org/resources/russia-facial-recognition-endangers-anonymity/> accessed 9 March 2026.
3. Biometric Information Privacy Act 2008, 740 ILCS 14 (US).
4. J Buolamwini and T Gebru, 'Gender Shades: Intersectional Accuracy Disparities in Commercial Gender Classification' (2018) 81 Proceedings of Machine Learning Research 77-91.
5. Digital Personal Data Protection Act 2023.

6. Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation) [2016] OJ L119/1.
7. 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 L1689/1.
8. Facial Recognition Technology (Regulation of Police Powers) Bill 2023.
9. *Glukhin v Russia* App no 11519/20 (ECtHR, 4 July 2023).
10. Information Technology Act 2000.
11. Internet Freedom Foundation, 'Project Panoptic: Mapping India's Facial Recognition Deployments' (Internet Freedom Foundation, 2021).
12. *Justice KS Puttaswamy (Retd) v Union of India* (2017) 10 SCC 1.
13. *SQ Masood v State of Telangana*, PIL challenging deployment of Facial Recognition Technology by Telangana authorities, Telangana High Court, notice issued January 2022.
14. MAM Qandeel, 'Facial Recognition Technology: Regulations, Rights and the Rule of Law' (2024) 7 *Frontiers in Big Data* <https://doi.org/10.3389/fdata.2024.1354659> accessed 9 March 2026.
15. Aadhaar (Targeted Delivery of Financial and Other Subsidies, Benefits and Services) Act 2016.
16. Universal Declaration of Human Rights (adopted 10 December 1948) UNGA Res 217 A(III) (UDHR).
17. International Covenant on Civil and Political Rights (adopted 16 December 1966, entered into force 23 March 1976) 999 UNTS 171 (ICCPR).
18. UN Human Rights Council, 'Report of the Special Rapporteur on the Promotion and Protection of Human Rights and Fundamental Freedoms while Countering Terrorism' (2023) UN Doc A/HRC/52/39.
19. US Commission on Civil Rights, 'The Civil Rights Implications of the Federal Use of Facial Recognition Technology' (US Commission on Civil Rights, 2024) <https://www.usccr.gov/reports/2024/civil-rights-implications-federal-use-facial-recognition-technology> accessed 9 March 2026.