ILE MULTIDISCIPLINARY JOURNAL [IF SCORE – 7.58]

VOLUME 4 AND ISSUE 2 OF 2025

APIS – 3920 – 0007 | ISSN - 2583-7230

Published by

Institute of Legal Education

https://iledu.in

BALANCING SECURITY AND PRIVACY: THE IMPERATIVE FOR AN EFFECTIVE LEGAL FRAMEWORK FOR FACIAL RECOGNITION TECHNOLOGY IN INDIA

AUTHOR – YUSRA KHAN, STUDENT AT AMITY LAW SCHOOL, NOIDA

BEST CITATION - YUSRA KHAN, BALANCING SECURITY AND PRIVACY: THE IMPERATIVE FOR AN EFFECTIVE LEGAL FRAMEWORK FOR FACIAL RECOGNITION TECHNOLOGY IN INDIA, ILE MULTIDISCIPLINARY JOURNAL, 4 (2) OF 2025, PG. 41-43, APIS – 3920-0007 | ISSN - 2583-7230.

Abstract

Facial recognition technology (FRT) is a potent tool for law enforcement and business use that has the ability to improve security, streamline verification, and increase efficiency. Nevertheless, its use is subject to serious privacy and ethical issues, especially in a democracy such as India where data protection regulations are in the early stages of development. Lack of appropriate safeguards in FRT may generate mass surveillance, identity thefts, and assaults on basic freedoms. This report critically analyzes India's legal and regulatory framework around FRT for its benefits, drawbacks, and hazards. The report also enunciates that an overarching statutory regime is called for to juxtapose security considerations with privacy freedoms. Through analysis of current laws, international best practices, and principles of law, this study offers policy guidance to ensure the proper application of FRT in India.

Introduction

National security needs, corporate motives, and administrative convenience have fueled India's rapid growth and deployment of facial recognition technology. The government has deployed FRT in policing, airport security, and border control, while private companies use it for customer authentication, targeted marketing, and workplace surveillance. Although this technology offers convenience and security benefits, its unregulated use poses severe privacy risks. Without proper legal safeguards, FRT can lead to mass surveillance, function creep, and breaches of individual rights. The Indian Supreme Court, in *Justice K.S. Puttaswamy v. Union of India (2017)*, identified the right to privacy as a constitutional right, but India does not yet have a definite legal framework for the collection and use of biometric data. This paper discusses the implications of FRT, evaluates the current legal framework, and considers the need for regulatory measures to ensure privacy while permitting responsible use of the technology.

Facial Recognition Technology: An Overview

Facial recognition technology is an artificial intelligence-based system that recognizes or authenticates individuals by processing facial features from images or video recordings. The technology works through three primary processes: data collection, feature extraction, and pattern matching. An image or video recording of an individual's face is first gathered from databases, surveillance cameras, or digital devices. Then, the software captures and maps distinctive facial features, including eye distance and jaw shape, to form a biometric template. Lastly, the features that are extracted are matched against stored databases to confirm the identity of the individual.

The uses of FRT are diverse in nature. In law enforcement, FRT is utilized for crime detection, missing persons' tracking, and monitoring national security. The business world uses FRT for attendance management of employees, customer profiling, and targeted marketing. Public administration implements FRT in

Aadhaar authentication, smart city surveillance, and border patrol. Though these applications bring about security and convenience, they also pose extensive risks in terms of violation of privacy, data security, and chances of abuse of authority.

Legal and Regulatory Environment in India

India lacks a specific legal framework for the regulation of FRT. The Information Technology Act, 2000, and the Personal Data Protection Bill, 2019, are the major laws that protect data. The IT Act mainly deals with cybersecurity and protection of data online but does not have any specific provisions regarding FRT and processing of biometric data. The Personal Data Protection Bill, pending, aims to govern the collection, processing, and storage of personal data, including biometric data. Yet, its delay in passing leaves FRT use mostly unregulated. Judicial precedents like the Puttaswamy judgment have prioritized privacy rights, but their enforcement in FRT regulation is weak.

India's FRT deployment regulatory loopholes are seen in the absence of clear laws regulating its use and monitoring. The authorities have installed FRT systems without consulting the public or disclosing information, posing a risk to the misuse of mass surveillance technologies. India further lacks independent institutions with the power to monitor and ensure compliance with data protection and privacy standards.

Ethical and Privacy Concerns

One of the earliest concerns regarding FRT is interference with the right to privacy. Application of FRT in broad surveillance contexts like protests or warrantless tracking on a large scale is a profound threat to citizens' liberties. Unsanctioned collection and storage of such data by official bodies or by private companies give rise to targeted profiling and prejudice. Algorithmic bias in the FRT application also threatens truth and justice in its results. Research suggests that facial recognition technologies tend to be racially, gender-wise, and ethnically biased, and hence lead to wrongful identifications and discriminatory treatments. These biases can be disproportionately done to marginalized populations and thus devalue the reliability of FRT in sensitive applications.Data protection is another urgent concern related to FRT. Large-scale biometric databases, when stored, raise the threat of data breaches and identity theft. Poor cybersecurity practices in biometric data handling can put individuals at risk of fraud and covert surveillance. Without robust data protection systems, abuse of FRT can have devastating effects on personal privacy and security.

Comparative Legal Analysis

A survey of international regulatory strategies towards FRT offers useful lessons for India. The General Data Protection Regulation (GDPR) of the European Union has stringent data protection norms, mandating express consent for biometric data gathering. It requires that people be given the right to access, edit, and erase their data. The United States takes a patchwork approach, with state-level laws like the Illinois Biometric Information Privacy Act (BIPA), requiring informed consent and data retention durations. China, however, uses FRT heavily for public monitoring with little protection of privacy. India will have to follow a hybrid model using aspects of the EU's privacy-oriented model while keeping in view national security imperatives.

Need for a Strong Legal Framework

An effective legal framework needs to be established to regulate the application of FRT in India while ensuring security as well as privacy interests. The principles upon which regulation needs to be based are consent and transparency, accountability and oversight, data minimization, and proportionality. Consent and transparency are particularly important in allowing individuals to know of the gathering and use of their biometric information. There should be a regulatory body that ensures compliance and enforces accountability requirements. Data minimization principles

must restrict data collection to necessary and lawful purposes, preventing excessive data retention. The proportionality principle ensures that FRT deployment is justified and minimally invasive, preventing its use in indiscriminate surveillance.To meet these concerns, India must implement a specific Facial Recognition Regulation Act with defined compliance pathways. There should be a National Data Protection Authority governing FRT deployments and guaranteeing respect for privacy legislation. Privacy-by-design principles must also be included in the development and deployment of FRT, with robust data security practices and fairness checks.

Conclusion and Policy Recommendations

Rising applications of facial recognition technology in India require a proper legal framework to reconcile national security interests with privacy rights of citizens. This study emphasizes the pressing need for well-defined legislation, greater transparency, and regulation to deal with this technology. Policymakers need to ensure that FRT is utilized responsibly and its risks are addressed through robust privacy protection. Some of the major recommendations are the passage of a specific FRT regulation law, the creation of a data protection authority with enforcement capabilities, increasing public awareness of biometric data rights, and periodic audits to determine the accuracy and fairness of FRT systems. With these steps, India can reap the advantages of facial recognition technology while safeguarding the basic rights of its citizens.