



INDIAN JOURNAL OF LEGAL AFFAIRS AND RESEARCH

VOLUME 3 ISSUE 1

Peer-reviewed, open-access, refereed journal

IJLAR

+91 70421 48991
editor@ijlar.com
www.ijlar.com

DISCLAIMER

The views and opinions expressed in the articles published in the Indian Journal of Legal Affairs and Research are those of the respective authors and do not necessarily reflect the official policy or position of the IJLAR, its editorial board, or its affiliated institutions. The IJLAR assumes no responsibility for any errors or omissions in the content of the journal. The information provided in this journal is for general informational purposes only and should not be construed as legal advice. Readers are encouraged to seek professional legal counsel for specific legal issues. The IJLAR and its affiliates shall not be liable for any loss or damage arising from the use of the information contained in this journal.

Introduction

Welcome to the Indian Journal of Legal Affairs and Research (IJLAR), a distinguished platform dedicated to the dissemination of comprehensive legal scholarship and academic research. Our mission is to foster an environment where legal professionals, academics, and students can collaborate and contribute to the evolving discourse in the field of law. We strive to publish high-quality, peer-reviewed articles that provide insightful analysis, innovative perspectives, and practical solutions to contemporary legal challenges. The IJAR is committed to advancing legal knowledge and practice by bridging the gap between theory and practice.

Preface

The Indian Journal of Legal Affairs and Research is a testament to our unwavering commitment to excellence in legal scholarship. This volume presents a curated selection of articles that reflect the diverse and dynamic nature of legal studies today. Our contributors, ranging from esteemed legal scholars to emerging academics, bring forward a rich tapestry of insights that address critical legal issues and offer novel contributions to the field. We are grateful to our editorial board, reviewers, and authors for their dedication and hard work, which have made this publication possible. It is our hope that this journal will serve as a valuable resource for researchers, practitioners, and policymakers, and will inspire further inquiry and debate within the legal community.

Description

The Indian Journal of Legal Affairs and Research is an academic journal that publishes peer-reviewed articles on a wide range of legal topics. Each issue is designed to provide a platform for legal scholars, practitioners, and students to share their research findings, theoretical explorations, and practical insights. Our journal covers various branches of law, including but not limited to constitutional law, international law, criminal law, commercial law, human rights, and environmental law. We are dedicated to ensuring that the articles published in our journal adhere to the highest standards of academic rigor and contribute meaningfully to the understanding and development of legal theories and practices.

SURVEILLANCE BY DESIGN: EXAMINING INDIA'S FACIAL RECOGNITION BOOM AND ITS IMPACT ON FUNDAMENTAL RIGHTS

AUTHORED BY - HARSHIT TIWARI

NMIMS Kirit P. Mehta School of Law, Mumbai

Abstract

India's unprecedented adoption of facial recognition technology (FRT) is emblematic of a global trend towards technology-centric governance. However, the foundational informed concepts of legality, necessity, and proportionality as recognized in a normative framework of constitutional decision-making are largely absent in the current explosion of surveillance programs in India. This article discusses how FRT is being more and more implemented in public infrastructure and law enforcement and its implications for the right to dissent, the right to privacy, and the right to freedom of movement. It posits that an absence of effective legal constraints and oversight means that FRT can easily morph into a tool of mass surveillance rather than a tool of targeted security. The paper reviews and evaluates current contexts of FRT, legal frameworks, and comparative contexts, and provides detailed recommendations for reforms towards a public policy that supports the advance of technology without inhibiting the democratic liberties of the citizen.

Keywords: Surveillance, Facial Recognition Technology, Privacy, Mass Surveillance, Constitutional Liberties, Digital Governance,

The use of technology in governance and public management is recognized as a 21st century reality, a digital revolution that grounds a growing number of disciplines. Of the many technologies currently being used, none raises more questions and relevant issues than the Facial Recognition Technology (FRT). Being touted as essential for national security, law enforcement or consumer convenience, FRT technologies have found their way into airports, train stations, public surveillance systems, and into many of our everyday police activities, FAST. This

substantial involution has happened without much legislative debate, without holding accountable public bodies or judicial scrutiny, and while serious constitutional and ethical dilemmas remain unabated. The main research question presented in this article focuses on human rights violations specifically in light of the uses of facial recognition technologies, which are being employed without sufficiently stringent positive legal instruments or procedural safeguards. At the heart of the issue is a core contradiction between the ambitions of technological advancement, and the protection of liberty and democracy. More specifically, this article seeks to establish the potential to understand how the integration and imposition of FRT in the current legal and procedural vacuum in India can facilitate practices of mass surveillance that violate the right to privacy, right to due process, and right to equality.

To grasp the ambit of facial recognition-based surveillance in India and the scope of some government/governance programs like DigiYatra, Automated Facial Recognition System (AFRS), and city-specific programs by police forces¹. This is a pressing issue on various counts. First, commercialization of surveillance technology tends to happen prior to legal regulation, i.e., dilution of civil liberties happens insidiously and beyond public discourse. Second, technologies like FRT, once embedded in day-to-day governance and policing systems, are difficult to scale back or revoke. Delhi, Hyderabad, Lucknow, and Bengaluru cities already use FRT for real-time surveillance of citizens in public spaces. The other ongoing project named DigiYatra, a Biometric boarding system at airports, is purported to be voluntary but never clear on data sharing, consent, and monitoring issues.²

In India, in the absence of a strong data protection law, the expanding infrastructure of surveillance becomes systemic threat to democratic theory. The current paper therefore aims to: 1- critically analyze current trends; 2- point out the risks involved in a model of governance through surveillance by design; and 3- make recommendations toward the development of a rights-based regulatory framework.

¹ *Deployment of facial recognition technology for state surveillance and monitoring* • software freedom law center, India (2024) Software Freedom Law Center, India • Defender of Your Digital Freedom. Available at: <https://sfhc.in/deployment-of-facial-recognition-technology-for-state-surveillance-and-monitoring>

² Verma, D. (2024) *Resist Surveillance Tech, reject Digi Yatra*, Internet Freedom Foundation. Available at: <https://internetfreedom.in/reject-digiyaatra>

It is in this process that the paper tries to make its own contribution to the larger debate surrounding the intersection between technological innovation and constitutional responsibility in the era of the digital. The application of facial recognition for purposes of public safety promises to transform India into a surveillance state.

The absence of a general legal framework and independent oversight bodies exacerbates these threats, exposing FRT implementation to possible abuse and violation of the constitution. According to the proportionality test set out in *K.S. Puttaswamy v. Union of India*, state intrusion into privacy must be provided for by law, must be in pursuit of a reasonable purpose, and be proportionate to the purpose. The majority of FRT deployments in India lapse on all of these standards.³

The threats are many:

Chilling Effect on Dissent: Through the arrest of protesters at public protests and cross-checking with criminal databases, FRT can create a chilling effect where individuals are reluctant to use their democratic right of protest. **Presumption of Guilt:** Rather than presuming people to be innocent until they are established as guilty, use of FRT considers every person in public as a suspect, which is contrary to criminal jurisprudence.

Increased Vulnerability for Marginalized Groups: It has been found that the facial recognition algorithm misidentifies Dalit, Adivasi, and Muslim individuals at a higher error rate, adding more chances of wrongful detentions and state overreach. International best practices also offer a contrasting view. Real-time biometric surveillance is considered a "high-risk" application for the EU AI Act, and FRT is subjected to rigorous audit procedures, data security adequacy assessments, and transparency obligations. The use of FRT for public surveillance has been suspended or banned in Amsterdam, Toronto, and San Francisco.

³ *Use of facial recognition technology in India: A function creep breaching privacy* (no date) OHRH. Available at: <https://ohrh.law.ox.ac.uk/use-of-facial-recognition-technology-in-india-a-function-creep-breaching-privacy/>

However, there is no independent monitor or clear regulatory regime in India. Without clear procurement procedures in place, the government procures and uses the FRT tools, making it difficult to ensure accountability or data security. The unchecked expansion of FRT threatens the very core of the Indian Constitution and could result in a legitimate form of surveillance if not addressed immediately.

The use of facial recognition technology (FRT) in India has some pretty red-hot warnings, particularly if we scrutinize the way it's being set up and applied like: 1. Lack of Legal Mandate: Perhaps the most concerning of all is the absence of a concrete legal system. More than 90% of facial recognition initiatives in India are running without a specific law to back them up. A prime instance is the Automated Facial Recognition System (AFRS) operated by the National Crime Records Bureau (NCRB),⁴ which is already operating completely devoid of any regulatory law. This creates a humungous void in determining how the technology is going to be used, who will be answerable, and how abuse will be checked.

2. Scale of Surveillance: The scale on which FRT is being implemented is mind-boggling. During the 2020 anti-CAA protests, the Delhi Police scanned more than 100,000 faces,⁵ according to reports. Hyderabad and Bengaluru have installed elaborate systems of CCTV cameras that are connected to real-time facial recognition systems. This puts in place a situation where any individual walking down a public street may be subject to constant surveillance, without regard to whether they've committed anything unlawful.

3. Transparency and Consent: Projects such as DigiYatra, which purport to offer voluntary facial recognition technology for air travel, raise serious issues of informed consent. Users may in fact have the option to opt-in, but there's no transparency on how their facial information is going to be stored, under what circumstances it will be accessed, and for how long it will be retained. The majority of individuals do not fully understand the dangers or the full extent of what they are committing to.

⁴ Sinha, A. (2024) *The landscape of Facial Recognition Technologies in India*, Tech Policy Press. Available at: <https://www.techpolicy.press/the-landscape-of-facial-recognition-technologies-in-india/>

⁵ Jain, A. (2022) *Delhi Police's claims that FRT is accurate at 80% are 100% scary*, Internet Freedom Foundation. Available at: <https://internetfreedom.in/delhi-polices-frt-use-is-80-accurate-and-100-scary>

4. Accuracy and Bias: RTI replies have indicated that the FRT tools operated by law enforcement agencies are anything but reliable. One such RTI reply has indicated that the Delhi Police's facial recognition technology is less than 1% accurate—a jarring revelation, considering that public authorities had earlier declared a success rate of 80%. ⁶This disparity isn't trivial; it has actual implications.

While in the world of global divergence, India is rapidly accelerating its application of facial recognition technology, other countries are slowing down. Consider the European Union's AI Act (2024), for example; it classifies real-time biometric monitoring as a "high-risk" activity and enforces strict legal safeguards on its use. Even cities such as San Francisco and Toronto have decided to prohibit facial recognition technology for surveillance purposes altogether. This glaring contrast points to the fact that the other democracies are emphasizing civil liberties over and above, while India is moving forward without adequate legal or ethical protection.

Literature Review

International and Indian scholarship continues to be doubtful of the unregulated use of facial recognition, however both Zuboff's "surveillance capitalism" theory shows how existing digital infrastructure commodifies personal information, and Usha Ramanathan and Vrinda Bhandari warn that India's adoption of digital infrastructure, which avoids utilising proper protections for privacy, will set a bad precedent. The Internet Freedom Foundation's (IFF) Project Panoptic reports that as of 2023, there are over 130 FRT projects that are either already operational or in progress across India, and most don't have any privacy protecting assessments of their impact of usage or consultations with the public. Hyderabad has over 600,000 CCTV cameras connected to facial recognition, which raises important issues regarding bulk surveillance. A study published by MIT in 2022 has also revealed that, major FRT algorithms are significantly more inaccurate for darker-skinned individuals, especially women, and increasing the misidentification and wrongful arrests of individuals. Cities across the world, including San Francisco, California, US and Brussels, Belgium have already banned the use of FRT based on similar concerns.

⁶ Anandusuresh (2022b) *Delhi Police in RTI reply: 80% match in facial recognition is deemed positive id*, *The Indian Express*. Available at: <https://indianexpress.com/article/cities/delhi/delhi-police-rti-reply-80-pc-match-facial-recognition-deemed-positive-id-8094324/>

In *K.S. Puttaswamy v. Union of India* (2017), the Supreme Court of India held that the right to privacy is a constitutional right, however frequently FRT systems avoid the proportionality test set out in this case all together.⁷

Methodology

Doctrinal legal analysis is the foundation of this study. Constitutional clauses, court rulings, official government policy documents, and answers to RTI applications are examples of primary sources. Media investigations, NGO reports, and scholarly articles are examples of secondary sources.

The legal frameworks governing FRT in the US, India, and the EU are also examined using comparative jurisprudence. The legality, proportionality, and transparency of current FRT use are evaluated using a rights-based analytical framework.

Conclusion

India is facing a pivotal moment deciding how to integrate new technologies with constitutional imperatives. The unmitigated and widespread use of facial recognition technology across the country signifies an unacceptable absence of advocacy for parliamentary oversight, transparency, and public involvement. Furthermore, facial recognition technology can reinforce existing systemic discrimination if deployed without safeguards. For example, biases embedded in these systems may lead to the disproportionate targeting or misidentification of individuals from historically underprivileged or marginalised communities. This can deepen social and legal inequalities, compounding injustices already faced by these groups.

The Indian Supreme Court unequivocally declared privacy to be a basic right in *K.S. Puttaswamy v. UOI*. However, the continued use of FRT in the absence of a legislative or regulatory framework contradicts this decision. The issue is exacerbated by the absence of a data protection statute that provides genuine consent, a mechanism for redress, and oversight.

⁷ *Fundamental right to privacy* (2025) *Supreme Court Observer*. Available at: <https://www.scobserver.in/cases/puttaswamy-v-union-of-india-fundamental-right-to-privacy-case-background/>

India needs a governance structure that upholds human rights and moral decision-making, not a retreat from technology. This involves:

- An overarching data protection act with international norms
- Independent regulation of all surveillance technologies
- Forced disclosure norms for public FRT implications.
- Effective accountability systems for abuse or false identification.

Recommendations:

1. Enactment of a facial recognition regulation statute: Parliament should adopt a comprehensive law that defines permissible use cases, establishes clear standards for data collection and retention and restricts inter-agent and third-party data sharing. Such a statute should incorporate sunset clauses and periodic legislative review.
2. Mandatory Privacy and Human Rights Impact Assessments: Prior to deployment, all FRT systems should be subject to published assessments evaluating their necessity, proportionality and potential discriminatory effects.
3. Independent Oversight Authority: An autonomous regulatory body, modelled on data protection authorities in comparative jurisdictions

Bibliography:

1. <https://sflc.in/deployment-of-facial-recognition-technology-for-state-surveillance-and-monitoring/>
2. <https://www.scobserver.in/cases/puttaswamy-v-union-of-india-fundamental-right-to-privacy-case-background/>
3. <https://indianexpress.com/article/cities/delhi/delhi-police-rti-reply-80-pc-match-facial-recognition-deemed-positive-id-8094324/>
4. <https://internetfreedom.in/delhi-polices-frt-use-is-80-accurate-and-100-scary>
5. <https://www.techpolicy.press/the-landscape-of-facial-recognition-technologies-in-india>
6. <https://ohrh.law.ox.ac.uk/use-of-facial-recognition-technology-in-india-a-function-creep-breaching-privacy/>
7. <https://internetfreedom.in/reject-digiyatra/>