
FACIAL RECOGNITION TECHNOLOGY AND THE RIGHT TO PRIVACY

Sanjana Mehta, Student, NMIMS Kirit P. Mehta School of Law

ABSTRACT

Facial Recognition Technology is deployed across governance, law enforcement, and surveillance systems, fundamentally reshaping boundaries between individual privacy and state authority. We examine the intersection of FRT and constitutional right to privacy in India, tracing the evolution of privacy as a fundamental right under Article 21 of Constitution, culminating in the nine-judge bench judgement in the case Justice K.S. Puttaswamy v Union of India(2017). The paper goes on to analyze the three-part constitutional test laid down and evaluates if the current FRT deployment in India satisfies these requirements. Through various case illustrations including drone-based surveillance during 2020 NRC protests in Uttar Pradesh, the paper states that India's adequate legal backing, defined purpose and proportionality. The paper highlights systemic concerns including unconsented data collection, algorithmic biases disproportionately affecting disadvantaged communities, mass surveillance without reasonable suspicion and the effect on dissent and democratic participation. The paper concludes that in the absence of a dedicated legal framework governing FRT, its deployment remains constitutionally vulnerable and risks normalizing surveillance that undermines civil liberties, autonomy, and human dignity.

Key Words: - Facial Recognition Technology (FRT), Right to Privacy, Article 21, K.S. Puttaswamy, Biometric Surveillance, Mass Surveillance, Proportionality, Data Protection, Civil Liberties, Algorithmic Bias, Surveillance State, Fundamental Rights, India, Constitutional Law

I. INTRODUCTION

Artificial Intelligence has become more and more integrated in sectors such as governance, security and surveillance systems. Today a candid photo or spontaneous video is no longer merely a record of a moment instead it becomes a data point within a much larger digital repository. Each image or video becomes a part of a larger digital depository. Somewhere, in a place filled with data centers buzzing with machines, a facial recognition algorithm or software processes these images by scanning expressions, comparing facial features and matches this against various records or databases. The outcome of this ends up to be a highly organized, searchable archive with a catalogue of human existence preserved frame by frame. This has become today's reality.

Facial recognition technology (FRT) is already embedded in our world. One can enter an airport and the camera scans your face or your phone unlocks at the sight of your face. It can simplify, accelerate and protect. However, it also has some cons and concerns. As every image becomes a part of a larger digital identity or digital record, the boundary between personal and public is increasingly hazy and blurred. What was earlier a private moment now having the potential to be universally misused and accessed.

India in particular has seen a massive rise in the deployment of facial recognition systems over the last couple of years. On December 22, 2019 Delhi Police used the "automated facial recognition" computer software to identify and screen masses during Prime Minister Narendra Modi's rally giving rise to several concerns about privacy and mass surveillance

II. UNDERSTANDING FRT

Facial Recognition technology operates as a biometric identification method which is similar to technologies like fingerprint recognition or iris recognition. It essentially analyses specific features of your face like contour of jawline or shape of nose or distance between eyes. These features are transformed into a mathematical model which is termed as facial template which corresponds to an individual. It enables identification without direct contact or interaction with the individual, making it particularly useful for law enforcement and large-scale surveillance. It functions using both standard light and infrared imaging enabling the detection and identification of faces from still images, video recording or real time camera feeds.

There are multiple technical stages with regards to the functioning of this technology. The first step is facial data being collected from cameras or digital images which can be captured in real time or can be drawn out from existing databases such as social media. The algorithm will then detect a face and identify and memorize distinct facial features and then they will be converted into a mathematical representation using algorithm which shall be known as a faceprint. This will then be stored in a repository and compared with other such facial features to establish a match. The correctness of this technology depends on factors like camera quality and training dataset quality. This technology does not merely record images but it also stores and processes personal biometric data and sensitive data. Once breached, it cannot be altered like passwords, making the risks associated with such misuse or data breaches severe in nature.

III. RIGHT TO PRIVACY AND FRT

The Right to privacy in India has evolved tremendously over the past few years. What was once included within the protections of life and personal liberty now is a part of an independent and recognized fundamental right under article 21. The Supreme Court laid this down in Justice K.S. Puttaswamy v Union of India and stated that it is innate to human dignity, autonomy, and the enjoyment of all freedoms provided by the constitution that are fundamental in nature.

Article 21 states that “No person shall be deprived of his life or personal liberty except according to the procedure established by law.” Through out decades, it was interpreted narrowly, equating liberty with physical restraint. Decisions such as Kharak Singh v State of UP rejected the status of this right as a fundamental freedom. These rulings highlighted a constitutional era that prioritized governmental power and formal legal procedure rather than individual liberty. Subsequent jurisdiction expanded the scope of this article especially after Maneka Gandhi v Union of India which stated that life and liberty must be interpreted broadly and all restrictions shall be fair, just and reasonable. Privacy still remained largely unaddressed till the time it was addressed in K.S. Puttaswamy v Union of India. In the Puttaswamy judgement, nine judges held that privacy is not a statutory or common law right but a fundamental right seen in the constitution. The court held that it was a right emerging from rights given in Part III. It was basically stated to be a cluster of interlinked protections such as bodily privacy, spatial privacy and sexual freedoms. The infringement must meet strict constitutional standards. The court established that right to privacy can also be restricted when three conditions are satisfied: legality, legitimate aim and proportionality. It protects people from unnecessary state intrusion.

The doctrine is predominant with modern surveillance technologies such as facial recognition, biometric databases, and automated data analytics which enable large scale and often invisible monitoring of individuals.

In the case of Justice K.S. Puttaswamy (Retd) v. Union of India (2017 10 SCC 1, the Supreme Court of India developed a very important framework for the State to interfere with the right to privacy of a person, which is a fundamental right conferred by Article 21 of the Indian Constitution. The Supreme Court held that the infringement of the right to privacy by the State must conform to the constitutional regulations, and the right to privacy cannot be diminished as a fundamental right. These regulations have been developed to ensure that there is no violation of the right to individual liberty by the State. With every attempt by the State to infringe the right to privacy, the Supreme Court developed a three-fold test.

First, there must be a legitimate basis for the restriction. There must always be a legitimate reason for any infringement of the right to privacy. Article 21 makes it very clear that no one may be deprived of life, liberty, or any other personal freedom unless the process of law has been followed. An important requirement, therefore, is that there must exist a law that allows for such an incursion into an individual's right to privacy. Any incursion into an individual's right to privacy would, therefore, be arbitrary and unconstitutional in the absence of a law.

Second, there must exist a legitimate state objective that is being pursued by the law that allows for such an incursion into an individual's right to privacy. There must exist a legitimate state objective such as national security, public safety, prevention of crimes, and the maintenance of public order. Furthermore, the intent and content of such a law must conform to the reasonableness test under Article 14, which protects an individual from arbitrary state actions.

Third, the proportionality principle must be satisfied by the restriction. This means that the strategies employed by the State must be proportionate to the goal that the law seeks to achieve. The level and nature of privacy intrusion should not be more than what is needed to achieve the desired end. In other words, the State must choose strategies that are both least invasive and appropriately balanced, yet effective in achieving the legitimate goal. In other words, proportionality acts as an important check against over-reach by the state .

The constitutional norm that controls any state activity impacting the right to privacy in India is made up of these three principles: proportionality, legitimate objective, and legality. They

guarantee the preservation of individual liberty while permitting the State to pursue justifiable public interests within well-defined legal bounds.

As seen from these three threshold requirements put forward by the Supreme court in the judgement, the usage of Facial Recognition Technology does not satisfy the requirements given. There are no legal basis surrounding FRT and governmental discretion is not enough as there should be a legal backing to defend such intrusion of privacy. Second, it should be used for clear and specific purposes such as identification of missing persons and other such purposes. Third, these methods have to be minimally intrusive and should not be disproportionate to the purpose of law.

There are various privacy concerns regarding FRT. One of them being that many facial recognition systems are collated from photographs sourced online from social media or other websites without obtaining consent from the required individuals. This was seen in the case of Clearview AI which built an online repository by collating pictures from public platforms. While this approach enabled fast database expansion, it also led to serious concerns about individual privacy rights and the overall quality and fairness of such datasets. Also, real time image capture for identification of individuals introduces challenges. Such practices also raise critical legal and ethical questions about the extent to which such information can be retrieved and used by the government.

It also poses certain challenges across privacy, civil liberties and equity. Not being captured by FRT is simply not an option and hence this technology has been termed as invasive in nature. When used for real time surveillance, FRT allows authorities to track a person's movements, acts and social and societal interactions on a much larger scale and at a lower cost. Without adequate regulation, this technology can lead to the mass collection and storage of facial data even when there is no specific suspect or incident being investigated for a crime or offence.

Another concern is equity and discrimination. Historically suppressed communities are often subjected to greater levels of surveillance and the widespread use of FRT may worsen this imbalance between poor and rich individuals. Police used aerial surveillance and drones to monitor and track individuals during the protest regarding Citizenship Amendment Act and proposed National Register of Citizens of Uttar Pradesh in 2020. Reports suggested that more than 1000 people were detained after being identified through drone footage.

Likewise, the Delhi police used FRT technology in 2019 to identify individuals who were deemed to be political threats or troublemakers during a political rally. This technology captured the images of the people present at the rally as they entered the venue. These images were then matched with a pre-existing database of images of people taken from footage of previous protests.

The use of FRT technology, if unchecked, would enable the government to keep a close eye on its citizens, especially during times of protests or political activities. This could, in turn, deter people from voicing their dissent and taking part in the democratic process .

There is presently no comprehensive legislation that particularly regulates the use of face recognition technology by law enforcement authorities in India, despite the technology's growing adoption. Although the Digital Personal Data Protection Act, 2023 was passed in India, it does not specifically address the special difficulties presented by biometric surveillance technology like facial recognition software. Concerns regarding responsibility, oversight, and transparency in the use of these technologies are raised by the lack of a specific regulatory framework. The possibility of misuse and widespread surveillance persists in the absence of explicit legislative guidelines controlling data collection, storage, and use.

IV.RECOMMENDATIONS

1. Promote explicit legislation on FRT: India should develop a comprehensive law that clearly defines the parameters, objectives, and limitations of facial recognition technology used by law enforcement agencies.
2. Ensure transparency on data usage: To avoid abuse and unauthorized surveillance, law enforcement agencies should be transparent on the collection, storage, processing, and dissemination of facial data.
3. Develop mechanisms for independent oversight: To ensure compliance with constitutional provisions, the use of facial recognition technology should be monitored by independent agencies or judicial authorities.
4. Ensure compliance with constitutional provisions: As per the Supreme Court's judgment on 'Justice K.S. Puttaswamy v. Union of India', the use of facial recognition technology should comply with the principles of legality, legitimate state purpose, and proportionality.

5. Strengthen data protection mechanisms: To protect biometric data, law enforcement agencies should develop effective security measures, such as imposing restrictions on data retention and ensuring non-breaches or unauthorized access.
6. Prevent Algorithmic Bias and Discrimination: In order to ensure that facial recognition technology does not end up being discriminatory towards certain communities, it should be periodically tested.
6. Encourage Accountability and Public Awareness: In order to enable people to raise their voices against incorrect identification and the misuse of their biometric data, accountability mechanisms need to be put in place.

V. CONCLUSION

One of the important technical tools that holds promise in assisting law and order and improving public safety is facial recognition technology. However, the use of facial recognition technology also raises important constitutional concerns in regard to the infringement of civil rights, privacy, and surveillance. The Puttaswamy ruling on the importance of privacy as an essential right under Article 21 of the Constitution requires that any state action should be in accordance with the principles of proportionality, legitimacy, and legality. The widespread use of facial recognition technology threatens the very foundations of democratic rights and freedoms without specific legislation and regulations in place. So, in the case of India, there is an immediate need to develop an equitable system that balances the rights of citizens and their fundamental rights.

References

1. Prachilekha Sahoo, “Facial Recognition Technology and Privacy: A Legal and Ethical Inquiry”, 8 International Journal of Law Management & Humanities
2. Editorial, “Privacy Fears as India Police Use Facial Recognition at Rally” Al Jazeera, December 30, 2019.
3. Editorial, “The Landscape of Facial Recognition Technologies in India” Tech Policy Press, April 1, 2024.
4. Justice K S Puttaswamy (Retd) v. Union of India 2017 10 SCC 1 (SC)
5. Editorial, “Clearview AI fined for illegal facial recognition database” Forbes, September 3, 2024.
6. K Reddemma Choudary, “Facial Recognition and the Right to Privacy: Legal and Ethical Concerns in India”, Volume VII, Issue III, Indian Journal of Law and Legal Research,(2025)
7. Viddhi Uppal, Pragya Narang, Harshita Gera, Kartik Upadhyay and Keshav Mittal, “Right to Privacy Under Article 21 Versus AI Surveillance : Constitutional Validity of Facial Recognition Technologies in India”, Volume 14, Issue 1, International Journal of Engineering development and research, (2026).
8. Mohita Yadav and Arti Sharma, “Facial Recognition Technology in India: Socio-Legal Debates on Privacy and Human Rights”,International Journal of Science, Engineering and Technology,(2025).